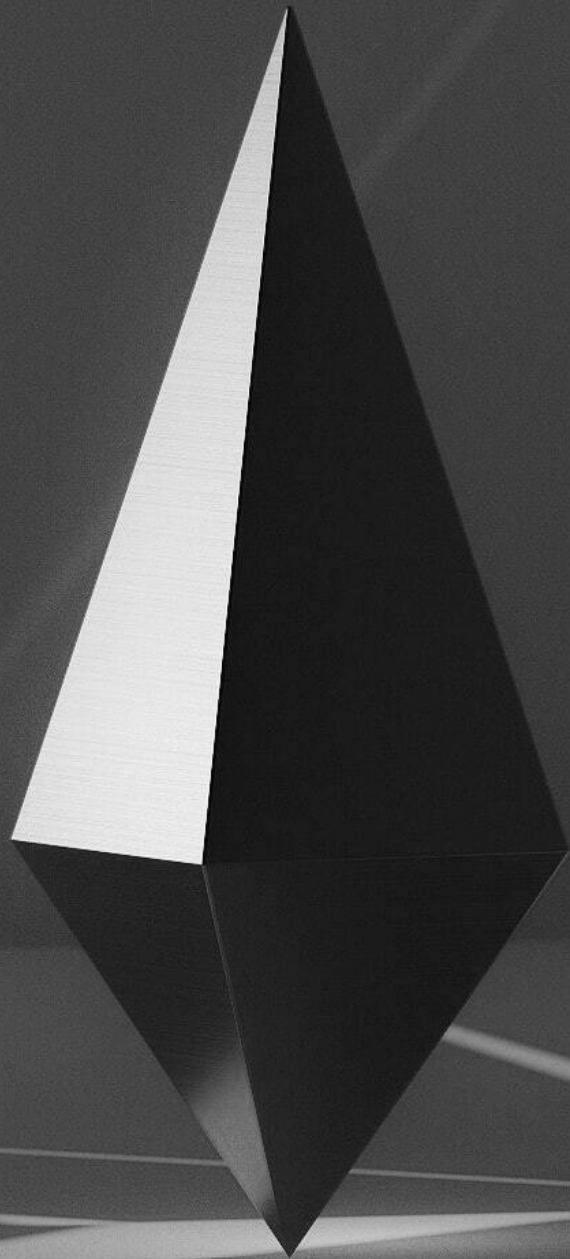


XDR REPORT

Q4 2021



A WORD FROM THE EDITOR

MIRKO ZORZ, EDITOR IN CHIEF, HELP NET SECURITY



What is extended detection and response (XDR)?

The definition varies depending on who you ask. Every vendor in the XDR market segment has their own, usually based on the technologies they provided before deciding to work on an XDR solution. Potential buyers may have their own definition, influenced by their current needs and the technologies they use (or used to use).

Most often, XDR is thought of as evolved endpoint detection and response (EDR) but covering more and diverse “endpoints” than before, or rebranded or augmented security information and event management (SIEM).

Still, there are XDR attributes most can agree on:

- It's cloud-native.
- Detection is based on the collection, normalization, correlation and analysis of endpoint/application/network/cloud logs and telemetry data.
- Investigation and threat hunting capabilities are aided by AI-based security analytics and data correlation.
- Response and remediation capabilities take advantage of automation.
- All of it is available from a single, unified platform

that can be integrated with other security tools.

I expect that a unified definition will only be agreed upon years from now, when a specific approach proves to be more effective than others; in the meantime, cybersecurity practitioners and decision-makers will have to do their research, ask vendors (and peers) incisive questions, and carefully parse the answers.

Choosing the right XDR solution for your organization

Swifter and more accurate threat detection and easier and more effective investigation and response is everybody's desired result, but not every offering will be a good fit for your organization.

Your final choice will depend on many factors: the size of your organization, the technologies already in use, the organization's security maturity and the maturity of its SOC (do you even have one?), the skills of the cybersecurity operators already employed or your organization's ability to employ more of them, the budget at your disposal, and so on.

We hope that this report will serve as a good starting point for this research and will give you an idea of what you can expect from different XDR solutions and vendors.

TABLE OF CONTENTS

- 2** **Impressum**
- 4** **Interview: Gorka Sadowski,
Chief Strategy Officer,
Exabeam**
- 9** **Kognos XDR Hunter: Never
hunt alone**
- 16** **Review: ReliaQuest
GreyMatter**
- 29** **Sophos is shaping the future
of security**
- 36** **User interfaces at a glance**
- 46** **Stellar Cyber Open XDR:
Making security fun again**
- 53** **How do I select an XDR
solution?**
- 68** **Company directory**

Report by Help Net Security
www.helpnetsecurity.com



GORKA SADOWSKI, CHIEF STRATEGY OFFICER, EXABEAM

FOSTERING AN OPEN APPROACH TO XDR



The XDR Alliance is a group of security and information technology providers who have organized to help customers more easily define, implement, and operate effective threat detection, investigation, and response (TDIR) programs and technology stacks.

Mirko Zorz, Editor in Chief, Help Net Security

How does the XDR Alliance define XDR?

At its core, extended detection and response (XDR) is a set of technologies that help organizations with different detection and response needs. However, “investigation” is also a key part of the equation.

There are three dimensions to the “X” which stands for “extended” in XDR. First, it is about detecting, investigating and responding to an extended set of use cases that organizations need to protect against. Second, it is the detection, investigation and response across the extended technology stack that organizations have already deployed – email, cloud, endpoint, network security, etc.

Finally, the focus is on the full extended lifecycle, from detection to response. However, investigation, or threat hunting, is an element that is often overlooked when it comes to XDR technology. As a part of the XDR Alliance we ensure there’s a home for it within our set of best practices.

Organizations need to be more proactive in looking at their use cases and the scenarios individual to their needs. They need to understand the threat detection, investigation and response (TDIR) required, whether this is in defense of compromised credentials, rogue employees, malware or phishing attacks. Once these use cases and scenarios are defined, it then becomes much easier for an organization to navigate. These use cases will depend on the nature of the business –

financial services vs. healthcare vs. retail – or depending on the maturity of an organization. There will be a different set of use cases to consider for each.

The XDR Alliance aims to bring together all types of organizations and cybersecurity and IT teams, from different verticals, to collaborate on building an XDR framework that will make it easier for teams to protect and secure their organizations from adversarial behaviour.

What was the main motivation behind the creation of the XDR Alliance?

While the adversaries are organized, the industry is fragmented at the moment and there is a lack of collaboration.

The conception of the XDR Alliance came from a place of realizing that, right now, SOCs are failing. Effective detection and response is difficult to achieve for a lot of organizations, and the current definition and

approach to XDR is confusing. If you ask 10 people to define XDR, you’ll get 11 different answers.

This is disconcerting for CISOs who are responsible for providing threat detection, investigation and response in their organizations. CISOs are confused and for good reason. No one agrees on what XDR is and no best practices have emerged on how to best deliver it. Providing extended detection and response requires many components working together. It’s like the saying, “it takes a village”... so we thought, why not get the village together to determine the best approach?

At the heart of the XDR Alliance is education and awareness for XDR best practices. We plan to publish case studies and content, and host field events for vendors, customers and prospects. For us, a big part of success is in education.

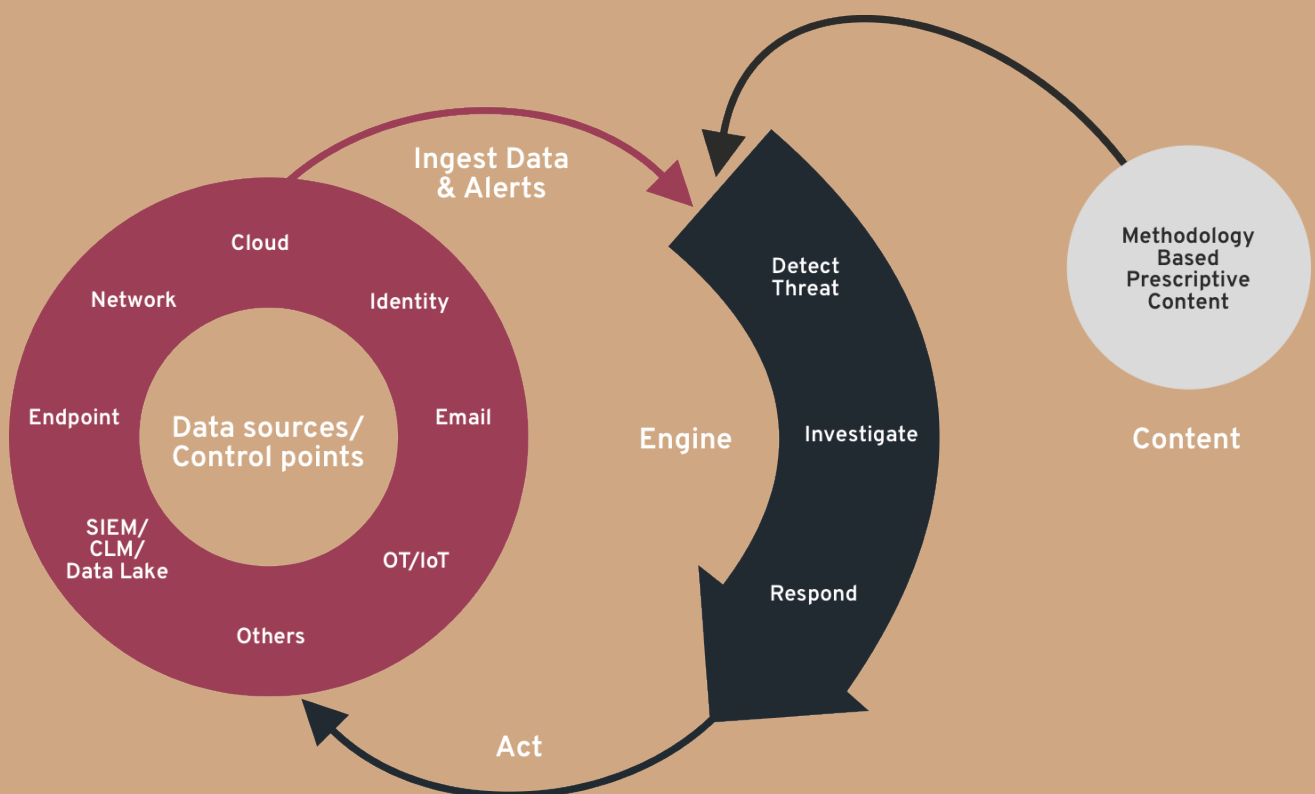
While the adversaries are organized, the industry is fragmented at the moment and there is a lack of collaboration.

The XDR Alliance brings together thought leading vendors in cybersecurity to clean up the industry disconnect, and also to create opportunities to better educate the market and build awareness around XDR. It's also an opportunity to bring together vendors in the

same space to collaborate and build better solutions.

What is your main mission? What do you plan to accomplish and how?

The main mission of the XDR Alliance is to foster an open approach to XDR that enables organizations everywhere to protect themselves against the growing number of



THE XDR THREE-TIER MODEL

cyberattacks, breaches, and intrusions. Ultimately, we want to help the end-user. I put myself in the shoes of the CISO trying to navigate their way through the disjointed layers of security – that’s not a great place to be right now. I think about what we can be doing to help them and how we can make their jobs – and lives – easier. The mission of the alliance is about offering an XDR definition and framework, and a collaborative ecosystem of leading security and IT providers who are committed to working together to achieve the same goal: making it easier for the end-users to protect their organizations.

What vendors have joined so far and what is each member bringing to the table?

Each of the founding members represents a key element in the XDR equation. Our members all typically have something to do with the technology stack that most organizations have deployed, whether that’s associated with endpoint security, cloud, email, TDIR, network vendor or service provider, for example. It is a set of thought-


leading organizations that believe XDR should be open, inclusive and collaborative.

They bring two things to the table. First, they are used as amazing sources of telemetry and data, capable of generating raw logs all the way to rich alerts. These data points are critical for the detection, investigation and response engine to perform high fidelity detection, efficient investigation and decide on response steps.

Second, the vendors and their solutions are used to activate and implement the “response” in XDR. In this case, they are also used as control points to enforce the decisions that the engine has made.

Do you plan to offer content and education for infosec professionals interested in XDR technology?

At the heart of the XDR Alliance is education and awareness for XDR best practices. We plan to publish case studies and content, and host field events for vendors, customers and prospects. For us, a big part of success is in education.



Our vision is for the XDR Alliance to become a standalone framework, prevalent in the industry, and become the centre of expertise for all-things-XDR, and beyond that, all-things-threat detection, investigation and response (TDIR).

We've recently hosted LinkedIn live sessions with members of the alliance taking customer problems and giving tangible examples on how organizations can solve them. What is truly great about the initiative is that every vendor has good intentions, and there is a common willingness to help each other and build a better industry.

Everywhere you look right now is bad news, so we are hoping that by banding together we can help.

How do you expect XDR to evolve in the near future?

We would like to see the XDR Alliance take on a life of its own. Exabeam became the driving force behind the alliance, but we'd like to see it evolve to become more of a distributed peer-to-peer organization.

We'd like to see the alliance become known as the go-to for XDR best practice and for our framework to become the norm, helping to promote a high-level approach in XDR excellence across the industry.

What do you see as the most significant obstacles to XDR adoption?

One of the most significant obstacles to XDR adoption is vendor competition, and those who prioritize competition over collaboration.

Now is the time for the vendor community to come together and be collaborative on how to take the industry forward. Unless we have an XDR approach that is open, collaborative and inclusive, the cyber space will fail.

For XDR to succeed, we all need to collaborate, become a collective voice of reason, and put cooperation above competition.

What's your vision for the XDR Alliance five years from now?

Our vision is for the XDR Alliance to become a standalone framework, prevalent in the industry, and become the centre of expertise for all-things-XDR, and beyond that, all-things-threat detection, investigation and response (TDIR). One of the key components that XDR is missing is "investigation", but in reality, investigation and security triage accounts for an excessive amount of the workload in the SOC. Investigation must become a focal part of the equation.

To conclude, I want to thank all the inaugural members of the alliance for their support and collaboration. Your participation demonstrates your thought leadership, vision, and customer-first mindset, and I am proud to count you as partners in helping security operations teams improve threat detection and response. Let's collectively win the battle against the adversaries. We are just getting started.



KOGNOS XDR HUNTER: NEVER HUNT ALONE

Zeljka Zorz, Managing Editor, Help Net Security

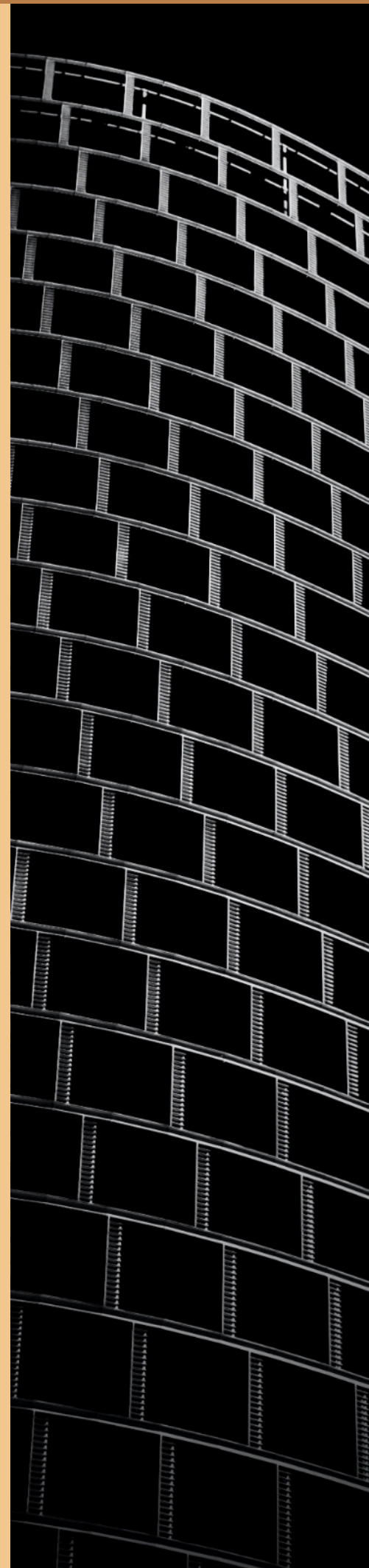
Cyber intruders are becoming increasingly brazen in their choice of targets and no organization seems to be spared.

Recent reports by [Microsoft](#) and [VMware Carbon Black](#) confirm what most security professionals have already realized: Cyber attack volume and sophistication have been on the rise, especially in the last few years. The reasons for this are many, but to enterprise defenders ultimately unimportant – they have no option but to accept the state of play and respond to it.

The thing that matters to them is what they can do to stop their organization from being victimized or to minimize the fallout of successful intrusions.

Uncover attackers in your company's networks

Threat hunting's goal is to find the threats in your enterprise environment that have dodged the security solutions you already have in place.



According to the 2020 VMware Carbon Black Global Threat Report, which is based on the responses of 3,000+ IT leaders from 13 different countries, 86% of the respondents who engage in threat hunting said it had strengthened their company's defenses, and 36% said they had found significant evidence of malicious activity thanks to their threat hunting program.

"Many of the recent successful cyber attacks happening across the US happened despite those organizations having a variety of security products in place and employing skilled defenders. It's becoming obvious that, with the rising attacker sophistication, passive monitoring is not enough, and companies should think about doing proactive threat hunting (if they aren't doing it already)," says Rakesh Nair, CEO of Kognos, a California-based startup that develops cybersecurity industry's first autonomous XDR hunting platform.

That's easier said than done, though. Threat hunting takes a lot of diverse skills and, generally, a lot of time, which

Nothing out there can do what Kognos is able to do: generate interactive stories with extreme fidelity from a hunter's perspective.

is a precious commodity that's usually in low supply in overworked security teams. The activity requires posing a lot of questions, getting a lot of answers, and having a way to extract from those answers enough relevant information to create valuable context to enable speedy mitigation.

Precisely because all of that, autonomous threat hunting has become Kognos's main goal.

"Nothing out there can do what Kognos is able to do: generate interactive stories with extreme fidelity from a hunter's perspective," Nair notes.

"Starting with a hypothesis and by asking all the relevant questions on behalf of the threat hunter, the system traces the whole attack path in real-time and tells the hunter what really happened and how, allowing security teams to respond quickly and drastically reduce attackers' dwell time."

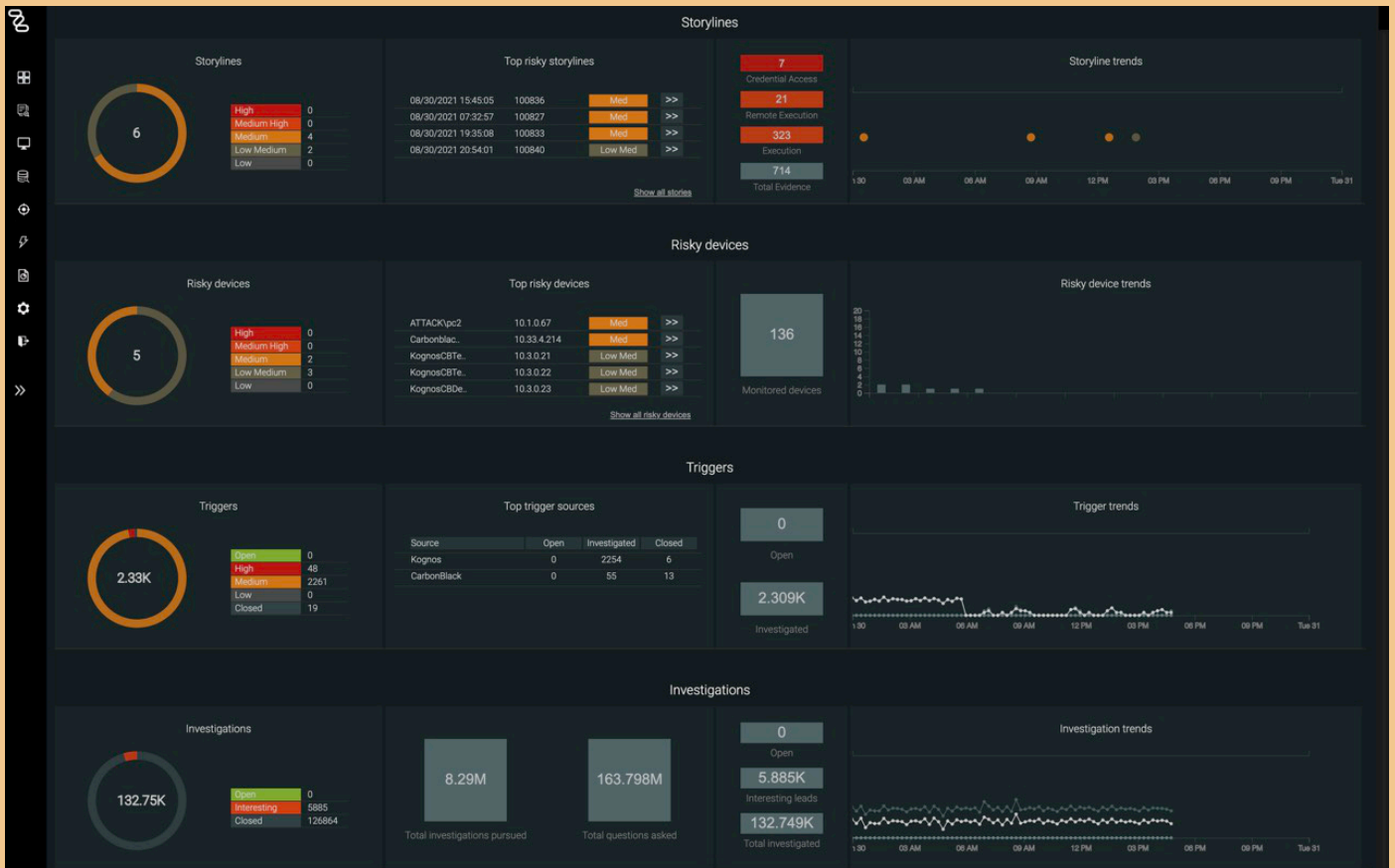


Figure 1 - Dashboard showing vital statistics

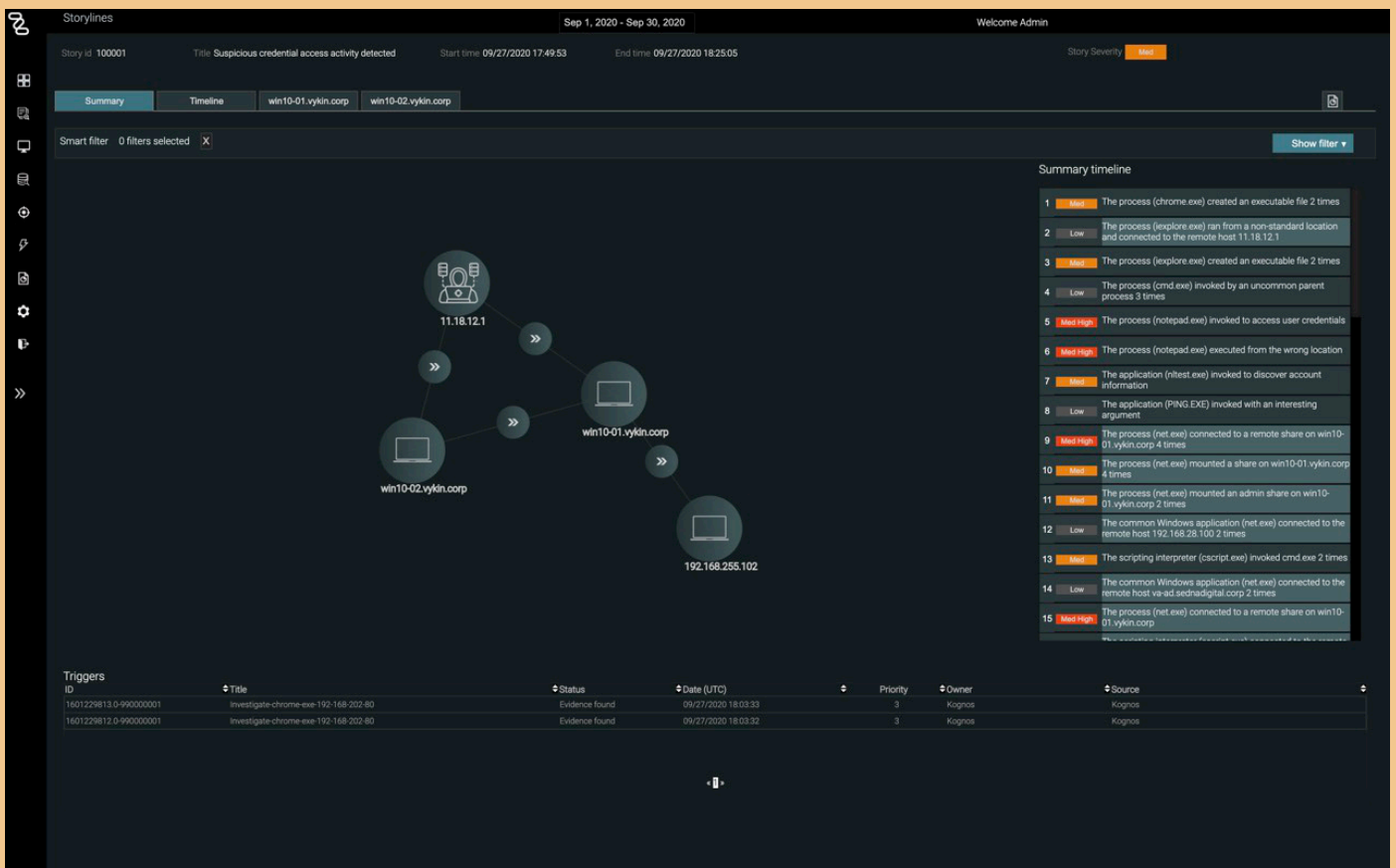


Figure 2 - Story summary showing multi machine attacker activity

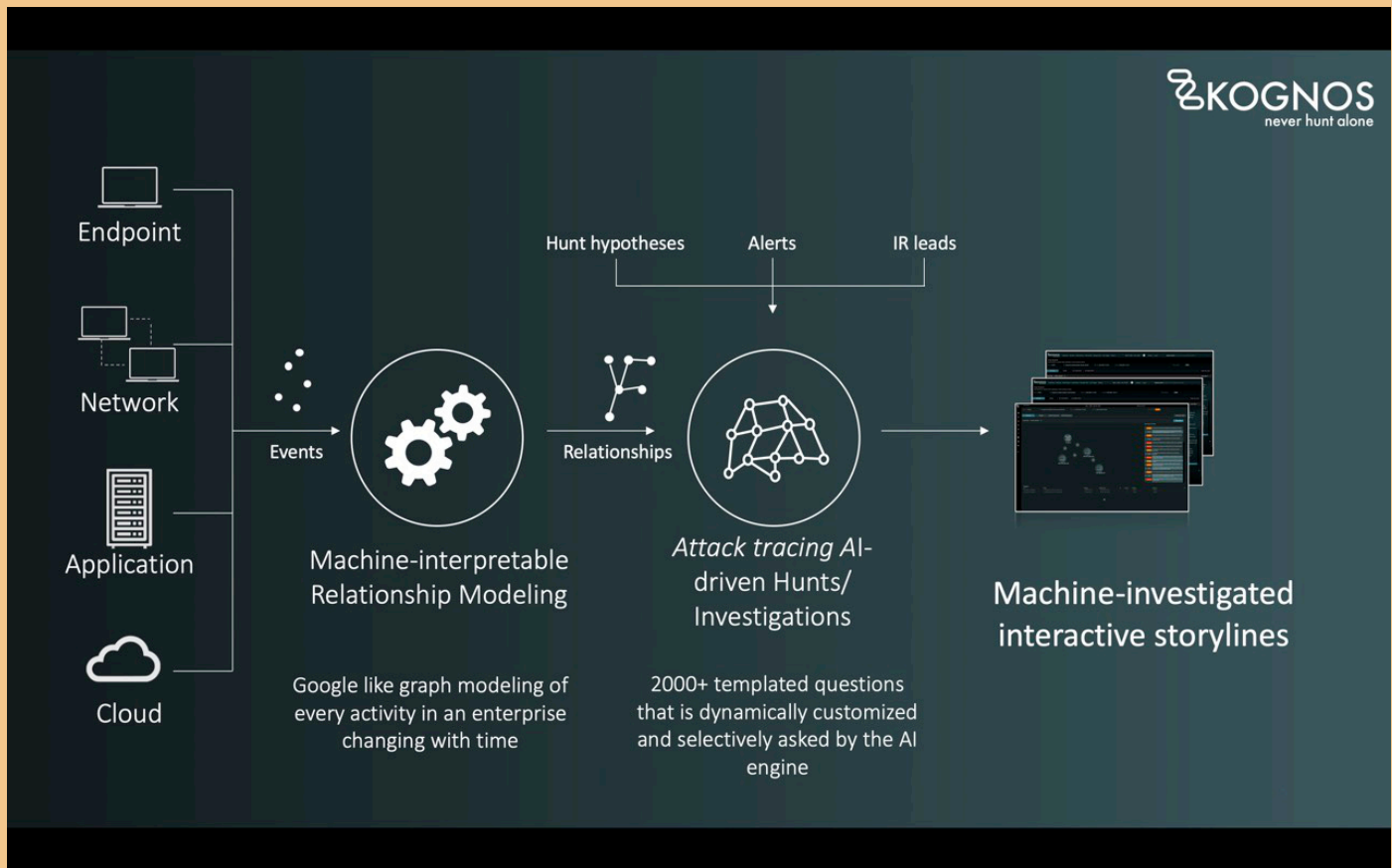


Figure 3 - Architecture showing how the system works

Kognos XDR Hunter

Kognos XDR Hunter uses its Attack-Tracing AI engine to solve several use cases. It can, for example, help automate alert investigations across any source and automate incident response. But first and foremost, it's a threat hunting platform that "sits" on top of an XDR engine.

It connects via APIs to your existing telemetry sources: your EDR solutions (CrowdStrike, Carbon Black, SentinelOne, Windows Sysmon, Linux AuditD, MacOS OpenBSM, etc.), NDR

solutions (Zeek, RSA NetWitness, etc.), Splunk and Elastic on the SIEM side, and it can also pull security logs from cloud services (AWS, Azure, etc.).

Data from EDR solutions is collected constantly, to create and keep updated the enterprise relationship graph – an enterprise-wide view of everything that is happening within the enterprise, including file manipulations, registry access, process creation, network connections, and so on. What data Kognos XDR Hunter pulls in addition to that depends on the

questions it asks.

"Any application log, cloud log, or network event that can provide answers to the questions that the Attack-Tracing AI engine asks, will be pulled on demand from SIEM and NDR sources to accomplish this," Nair explains.

"The questions are extensible, so if the customer has a proprietary application (e.g., a payment application), they can add additional forensic questions that will be asked if an adversary seems to access the payment server, to

augment the stories with additional answers.”

With Kognos, threat hunting (and autonomous alert investigation, and incident

response) is “point and click.”

“We provide a lot of 'seed' hypotheses to start with and threat hunters can also come up with their own,” Nair notes.

“Since Kognos is used by many MSSPs who employ experienced threat hunters, they often share interesting hunt hypotheses with us. We then curate them and make

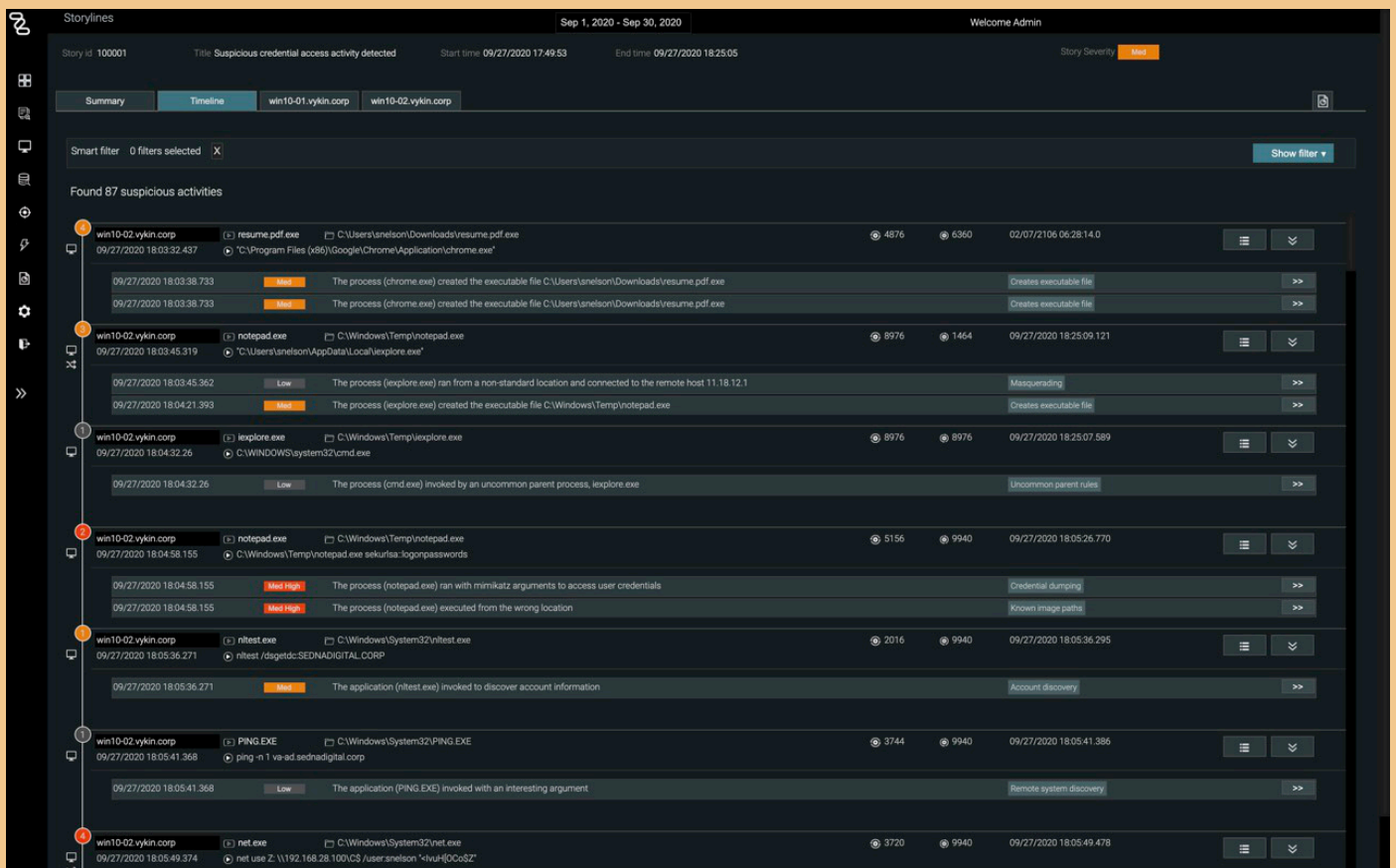


Figure 4 – Story timeline showing attacker activity as a timeline

Since Kognos is used by many MSSPs who employ experienced threat hunters, they often share interesting hunt hypotheses with us.

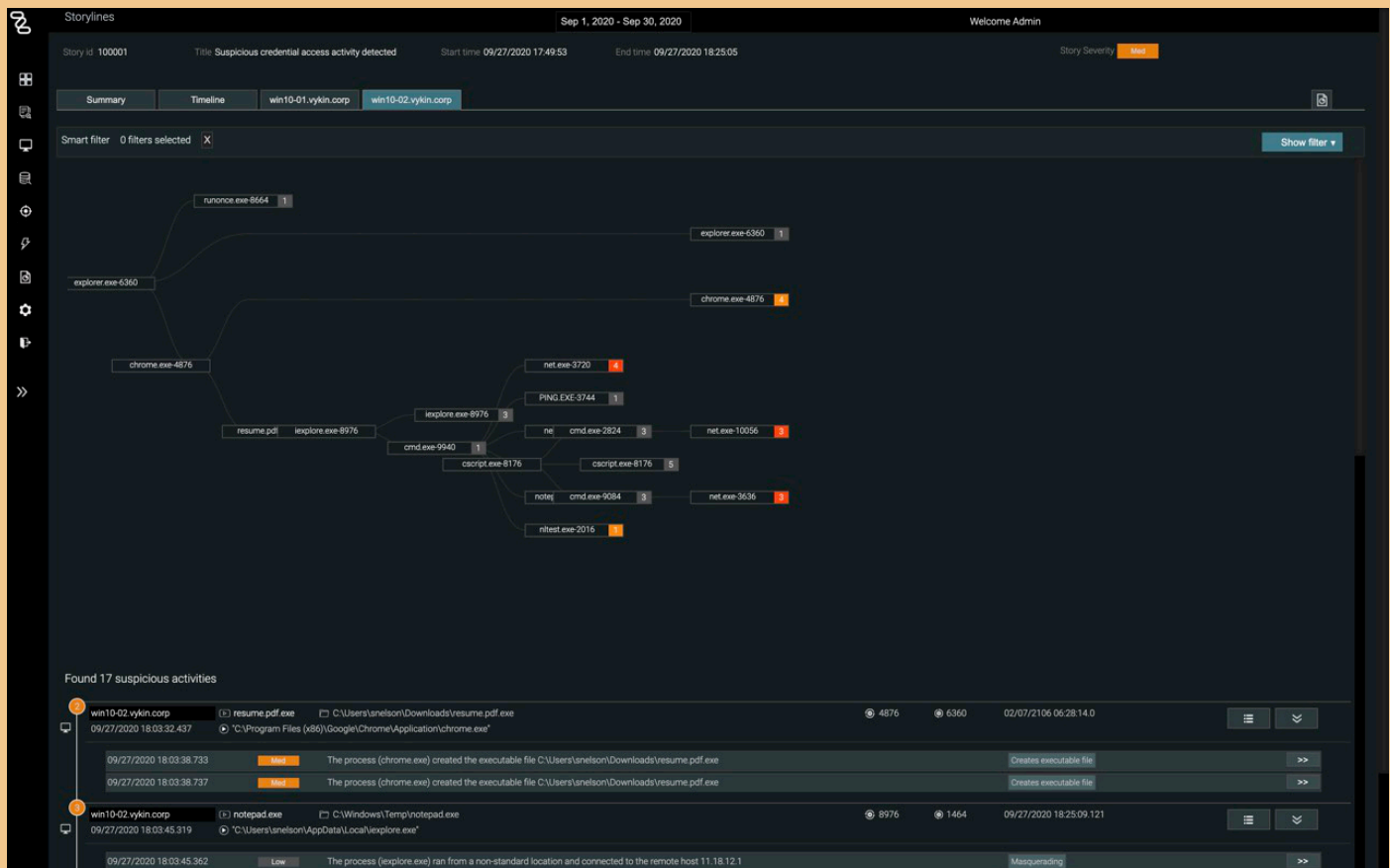


Figure 5 – Story command sequences showing command sequence executed by attacker

them available to the rest of our customers. They see it in their console, can download it and immediately use it in their environment.”

In short: Threat hunters tell Kognos XDR Hunter what they’re interested in searching for, and it does all the work: detects suspicious behavior, uses the Attack-Tracing AI engine to ask thousands of questions to fully contextualize the attack in minutes, and presents the findings as complete attack campaigns – not just a set of alerts.

In addition to that, threat hunters can schedule those hunts to repeat hourly, daily, or weekly. With Kognos doing all the work, they can pretty much investigate any suspicious behavior, such as living-off-the-land binary usage, use of persistence mechanisms or of lateral movement tools.

Kognos also diminishes the likelihood of threat hunters ending up investigating a false positive, Nair says, because it generates the complete context.

“Our analytics is very single goal-oriented. The questions the Attack-Tracing AI engine asks are very specific, so the system is not bubbling up all anomalies – the right context filters most of them out,” he explains.

Who’s it for?

According to the SANS 2020 Threat Hunting Survey, 85% of organizations have recognized the value of threat hunting and engage in it, but only 37% have a formal program and methodology

Kognos XDR Hunter can be of help to organizations of all sizes, but it will really shine at mid-size organizations with just one or two senior security professionals who have enough experience and knowledge – but not enough time – to hunt for threats.

with assigned staff. 45% of respondents run an ad hoc hunting process, dependent on their needs.

“Companies on the Fortune 100 list all do threat hunting. One of the teams that I’ve talked to told me they do hunting a half a day every week, and they are able to surface more suspicious activity than the entire week of passive monitoring,” Nair says.

“How many hunts is that during that time frame, I asked. 2 or 3 hunts per person, they said. During the same time, a threat hunter can initiate 2,000 to 3,000 hunts via Kognos XDR Hunter, and those are executed autonomously by the system.”

The resulting visual attack storylines are prioritized, the threat hunters can review them and can either continue

refining the hunt hypotheses or start mitigation and remediation actions. Some of the latter can be performed from Kognos XDR Hunter.

“If you have an orchestration tool, you’ve probably already created some automation playbooks. Since it’s all API-driven, we can add light-weight action scripts in the environment and hook into any of those systems. So, if you have, for example, a script to set up a firewall rule or block any machine from accessing a domain, you can trigger it from the UI,” he explains.

Kognos XDR Hunter can be of help to organizations of all sizes, but it will really shine at mid-size organizations with just one or two senior security professionals who have enough experience and knowledge – but not enough time – to hunt for threats. It will effectively allow them to

establish a threat hunting function without having to invest in extending their teams.

Kognos XDR Hunter (and, indeed, the entire Kognos XDR Automation Suite) is also a great tool for MSSPs, who are increasingly being asked by customers about the possibility of conducting threat hunting in their environment.

“We’re very flexible when it comes to deployment. We have a SaaS offering, but we can also deploy the software in customers’ data centers or their cloud environments. Provisioning and deployment can be done in less than 15 minutes, with pre-investigated stories forming within 30 minutes,” Nair concludes.



REVIEW: RELIAQUEST GREYMATTER

HRVOJE MARTINCIC, SENIOR IT CONSULTANT

XDR stands for extended (or cross platform) detection and response. The purpose of XDR solutions is to integrate disparate security tools across the enterprise technology stack to deliver a single, complete view of potential threats in the enterprise's digital environment, as well as a single console from which they can be investigated and acted on.

XDR solutions can be native (incorporating first and foremost that vendor's security solutions) and open (vendor-agnostic).

ReliaQuest GreyMatter

ReliaQuest GreyMatter is Open XDR-as-a-Service, delivering integration across tools from many different vendors and acting as an integration hub for security analytics and operations.

GreyMatter integrates with

over 60 different technologies (anti-virus, cloud, firewall, EDR, SIEM) and has a team of dedicated engineers who are continuously curating these integrations and adding others, as well as building additional content for threat detection, data normalization, automated response, and investigation enrichment plays and playbooks.

Integrations are powered by open APIs and the Universal Translator, a patented integration engine / translator layer that unifies and normalizes data from and queries directed to different tools. The Universal Translator allows analysts to use the language with which they are most comfortable to write queries, and GreyMatter "translates" those queries automatically to the integrated tools.

GreyMatter is used by around 300 customers, most of which

are on the Forbes Global 2000 list.

Home

When you open GreyMatter, you are shown the (simplified) Home screen by default.

At the top you see how many alerts and indicators of compromise (IOCs) have popped up in the last 24 hours and how many hunts are active.

Technology Status - the heart of GreyMatter - shows all the third-party technologies / solutions integrated with the platform. A link to the Resource Center is in the bottom right corner of the interface.



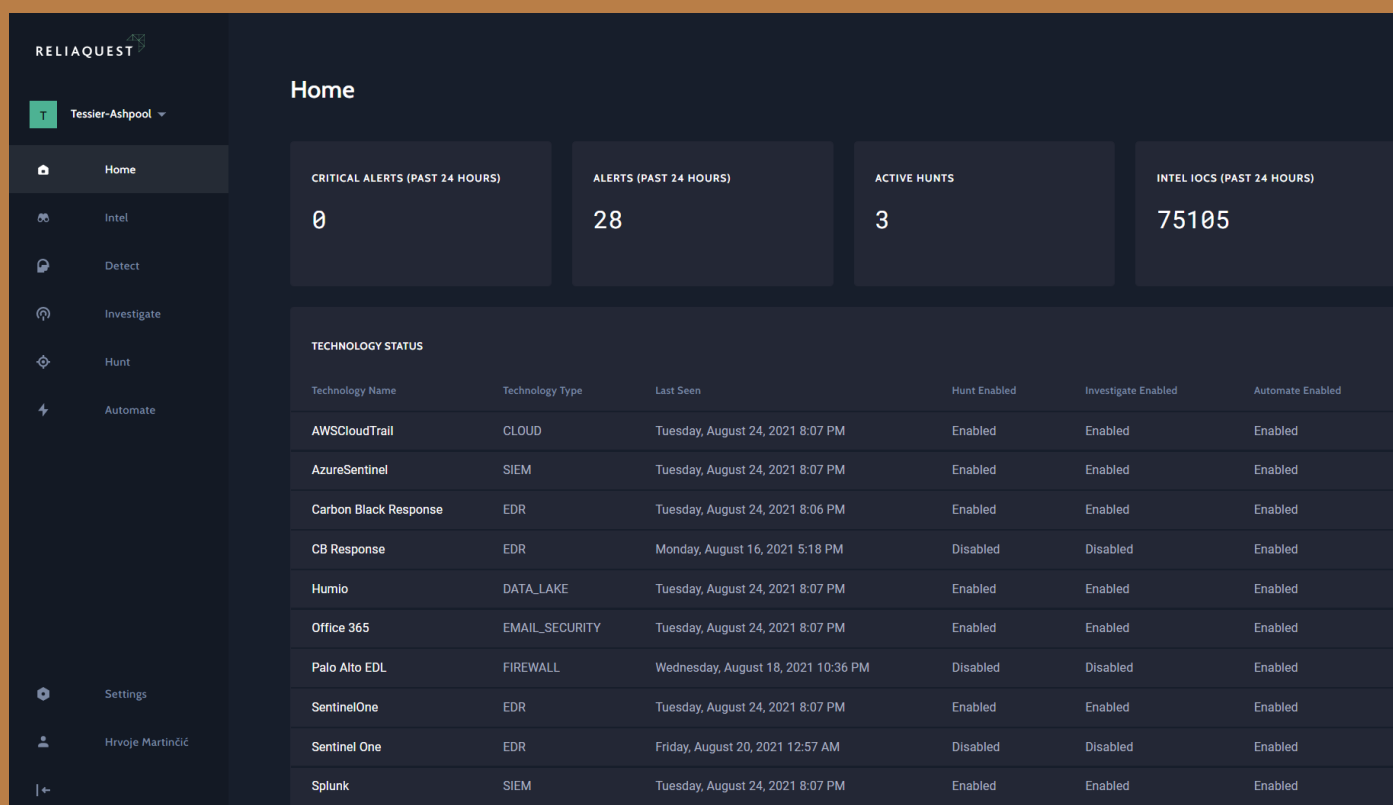


Figure 1 - The simplified Home screen



Figure 2 - The Resource Center provides a great starting point for learning how to use and master GreyMatter

Intel

To make real time alerting possible, GreyMatter puts threat intelligence gathered by ReliaQuest, its customers and over 40 open source, government, and commercial feeds into context.

The data is collected, de-duplicated, and prioritized by severity, and made available from GreyMatter’s Intel screen. Here you can look more closely at IP addresses, domains, URLs, and hashes. Secondly, GreyMatter can

deliver the high-fidelity threat intelligence back to the customer’s technologies – their EDR, SIEM platform, email security gateways, or their firewalls – to apply the threat intelligence to improve threat detection.

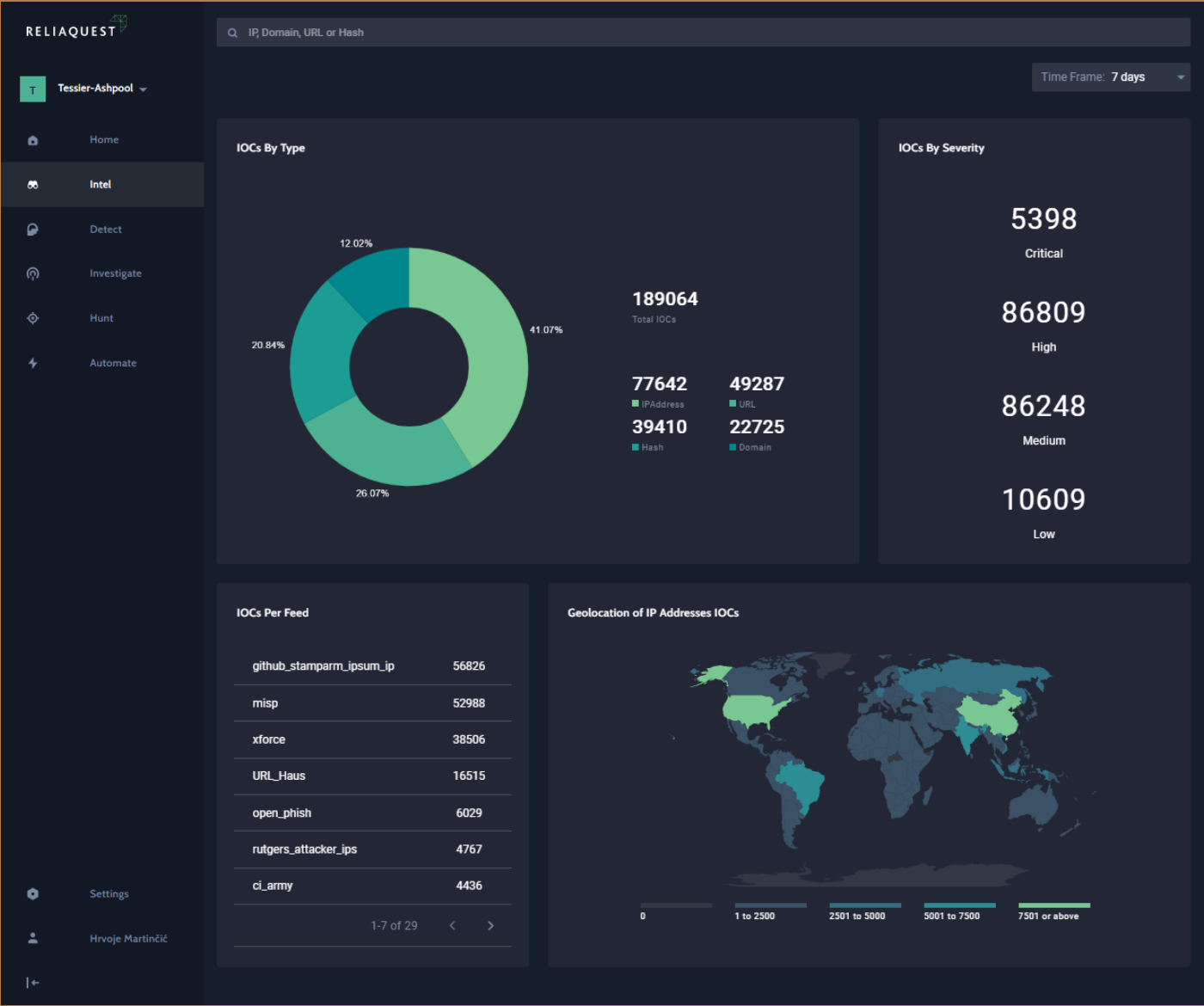


Figure 3 - An overview of IOCs flagged in the last 7 days

< Intel

yahoo.com

Search: yahoo.com

Filters: lastSeenDate >= 2021-08-21T00:00:00

IP (0) Domain (0) **URL (8)** Hash (0)

Threat Relevance (3)

Feed Name	Count
misp	3
open_phish	3
Phish_Tank	2

Resources

No data available with applied filters

Tags (0)

No data available with applied filters

IOC Name	↓	RQ Threat Score	Feed Count	Last Seen
https://saint-gobaine.com/cg-bin/yahoo/login/login.yahoo.com/index.php		9	2	2021-08-23
https://saint-gobaine.com/cg-bin/yahoo/login/login.yahoo.com/Login_Password.php		9	2	2021-08-23
https://improvepackage.com/auth/secured/login.php?https://login.yahoo.com/?src=ym&lang=en-US&intl=us&done=https://mail.y...		8	2	2021-08-22
https://fir-8128a.web.app/?email=alisampson32@yahoo.com		8	2	2021-08-21
https://fir-8128a.web.app/?email=alisampson32@yahoo.com		8	2	2021-08-21
https://emmakm07yahoo.com/		8	2	2021-08-27

Figure 4 - Searching for events related to a specific domain

https://saint-gobaine.com/cg-bin/yahoo/login/login.yahoo.com/index.php

Last Seen Mon Aug 23 00:00:00 UTC 2021

Feed misp

Threat Level HIGH

No description available

Threat Context

IOC Type	Feed Source	Sub Category
URL	misp	--

Observations	Related Artifact	IOC
--	--	https://saint-gobaine.com/cg-bin/yahoo/login/login.yahoo.com/index.php

Feed Category	Title	Type
--	--	--

Tags	Threat Tags
--	--

Country

Country Code	Country	City Name
--	--	--

Figure 5 - A deeper look into an IOC

Detect

The Detect screen has two tabs: Overview and Rules.

The Overview tab shows the rules that have been deployed and their correlation to the environment, as well as how they map to the MITRE ATT&CK framework or the Cyber Kill Chain.

The Rules tab shows the list of all available rules and their status. This is where you can discover more details about each rule and see what it's looking for. You can also change the logic to cover the latest threats. 600+ rules are currently available, and these existing rules are constantly being updated and new ones added.

GreyMatter's aim is to reduce reaction time by using different correlation rules and if-then statements. Triggering rules creates processed information that's used for investigations or can be delivered to the customer's integrated solutions, for them to act in their preferred platform.

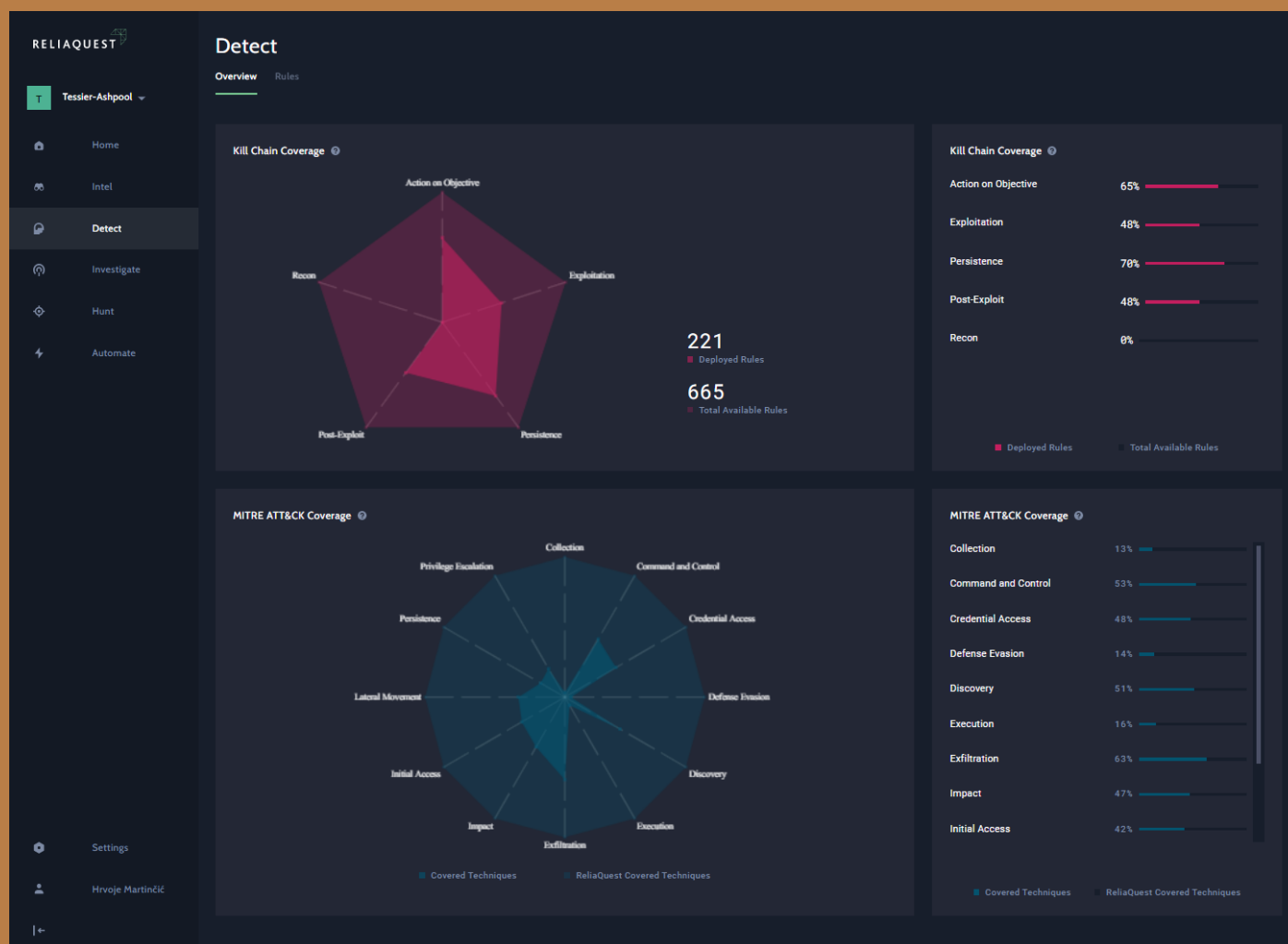


Figure 6 - A graphical overview of detection vectors

The screenshot shows the 'Detect' interface of ReliaQuest GreyMatter. On the left is a sidebar with navigation options: Home, Intel, Detect (selected), Investigate, Hunt, Automate, Settings, and a user profile for Hrvoje Martinčić. The main area displays a table of detection rules with columns for ID, Rule Name, Kill Chain Phase, MITRE Tactics, and Status. A search bar and filters for Kill Chain, MITRE, and Status are at the top. On the right, a detailed view for rule 000001, 'Addition to Privileged Security Group', is shown. It includes a description, a deployed integration, state (Deployed), severity (Medium), last updated time (Jan 19 2021 9:49 PM CET), and a kill chain phase (Post Exploitation). The MITRE ATT&CK categories listed are Credential Access, Account Manipulation, Defense Evasion, Initial Access, and Persistence.

ID	Rule Name	Kill Chain Phase	MITRE Tactics	Status
000001	Addition to Privileged Security Group	Post Exploitation	Credential Access, Defe...	Deployed
000002	Modification of Sudo File	Post Exploitation	Credential Access, Pers...	Deployed
000003	Privileges Escalated for Account with Abnormal ...	Post Exploitation	Credential Access, Defe...	Deployed
000004	Mass Group Deletes - Linux	Post Exploitation	Impact	Deployed
000005	Mass User Deletes - Linux	Post Exploitation	Impact	Deployed
000006	Shadow File Access	Post Exploitation	Credential Access	Deployed
000014	Privileges Escalated for Account with Abnormal ...	Post Exploitation	Credential Access, Defe...	Deployed
000015	Mass Group Deletes	Post Exploitation	Impact	Deployed

Figure 7 - Detection rules with the additional info

Investigate

Any time a detection rule is triggered, it leads to an investigation. On the Investigate screen you can see a high-level summary of what's happening that day.

The screenshot shows the 'Investigate' interface. The top section provides a summary: Active Alerts (0), Alerts Today (28), Resolved Today (0), and Critical Alerts Today (0). Below this is a table of alerts with columns for Alert Time, RQ Ticket, Description, Severity, Ticket State, and Data Status. On the right, a detailed view for alert RQ-S-000193-01-Suspicious File Downloaded From High Risk Site-04-1054718 is shown. It includes a severity of Informational, a data status of Completed data retrieval, and a donut chart showing the distribution of logs: Splunk (91.2%), AWSCloudT... (8.6%), and Carbon Bla... (0.2%).

Alert Time	RQ Ticket	Description	Severity	Ticket State	Data Status
2021.08.24 07:56 PM	DEMO1054729	RQ-S-000237-01-Suspicious Servic...	High	New	3k logs
2021.08.24 07:51 PM	DEMO1054728	RQ-S-000175-01-VPN Login from L...	High	New	4k logs
2021.08.24 07:51 PM	DEMO1054727	RQ-S-000117-01-Local Admin Creat...	Medium	New	3k logs
2021.08.24 07:48 PM	DEMO1054726	RQ-S-000092-01-IRC C2 Traffic Patt...	Medium	New	3k logs
2021.08.24 07:43 PM	DEMO1054724	RQ-S-000102-01-Brute Force - Singl...	High	New	3k logs
2021.08.24 05:55 PM	DEMO1054721	RQ-S-000041-01-DNS Over TCP_01...	Medium	New	2k logs
2021.08.24 05:17 PM	DEMO1054720	RQ-S-000144-01-VPN Login from L...	Informational	New	3k logs
2021.08.24 05:17 PM	DEMO1054719	RQ-S-000030-01-AWS Actions with...	High	New	1k logs
2021.08.24 05:03 PM	DEMO1054718	RQ-S-000193-01-Suspicious File Do...	Informational	New	481 logs
2021.08.24 04:36 PM	DEMO1054717	RQ-S-100219-01-SQLInjection_01-1...	High	New	7k logs

Figure 8 - The Investigate screen with additional information on alerts

In the example pictured below, the alert related to a suspicious file download was based on data retrieved from Splunk, AWS, and Carbon Black instances integrated with GreyMatter. The platform now allows the user (analyst) to go through the collected information and pinpoint the root cause.

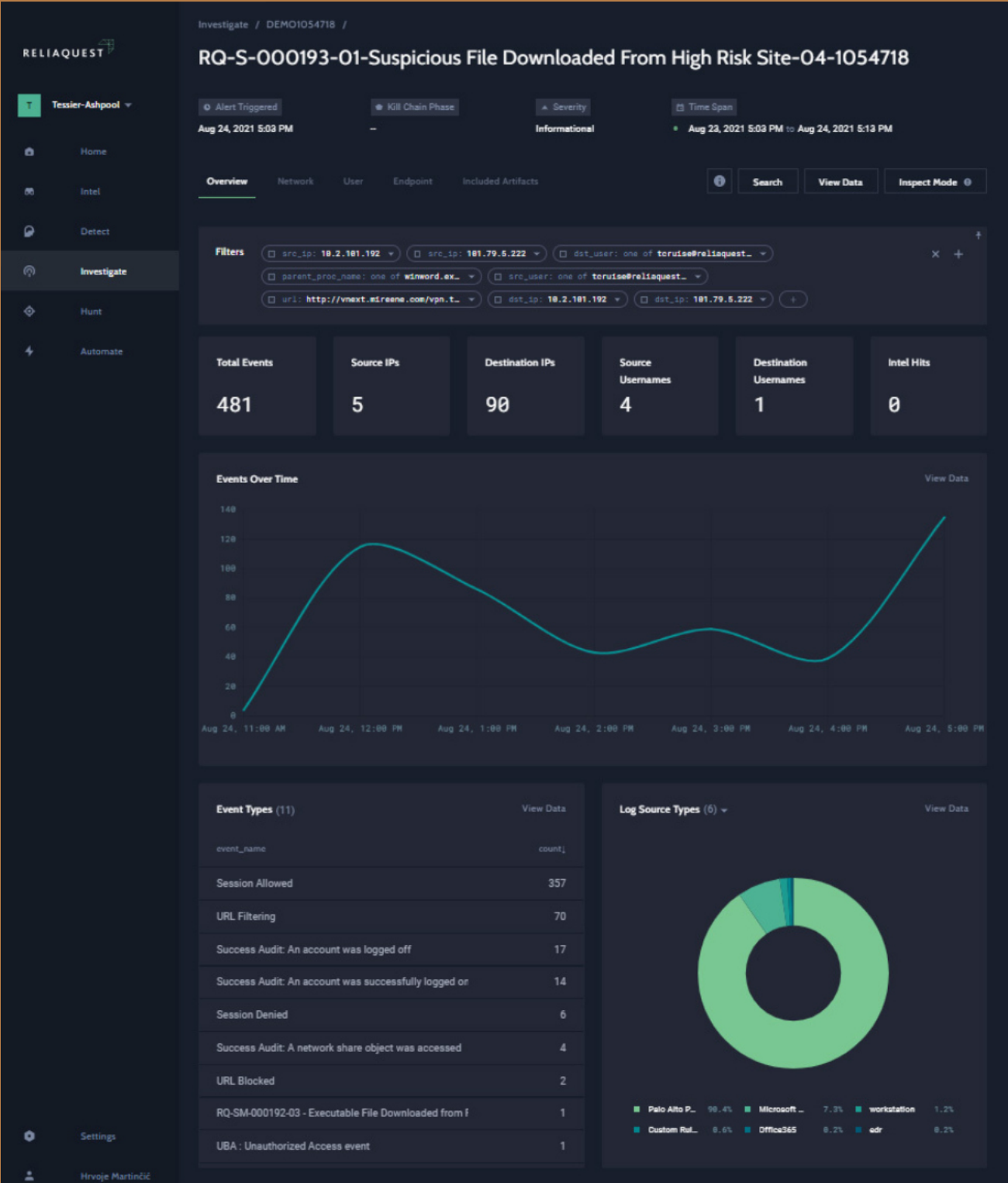


Figure 9 - Full overview of the alert

There are many other options and filters, but it's virtually impossible to delineate all possibilities. Suffice to say that users can correlate everything and are limited only by the connected technologies.

Hunt

Effective threat hunting depends on getting the right data. GreyMatter comes with pre-built hunt packages that look for different types of threats or cyber hygiene

issues that could lead to a breach at some point. Customers can use those to check, for example, their firewall or DNS cyber hygiene, or to look at all the traffic egressing the company network through port 53 of their firewall, or to see if there are misconfigured systems reaching out to non-authoritative DNS servers, and so on.

They can also create their own hunts by using GreyMatter's Query Builder, which is part

of the solution's Universal Translator engine.

What happens in the backend when you use the Query Builder? GreyMatter will break all queries into smaller queries and deliver them to the various integrated tools, then collect the data from them and deliver them to the analysts in the form a single data set, with recommendations for how to action hunt findings.

The screenshot displays the 'Hunt' section of the ReliaQuest GreyMatter interface. The left sidebar shows navigation options: Home, Intel, Detect, Investigate, **Hunt**, and Automate. The main content area is titled 'Hunt' and includes a 'Hunt Campaigns' tab. It features a search bar, filters for 'Package: Any' and 'Status: Any', and a 'New Hunt' button. Below these are two sections: 'Active Hunts' and 'Expired Hunts'.

Active Hunts: This section shows three active hunt campaigns:

- Duplicate of [Malware File Hash Hunt]**: RQ HUNT, Jul 28, 2021 to Jul 29, 2021, Expires in 8 days, Completed data retrieval: 71 logs.
- Compromised Account Hunt**: TESSIER-ASHPOOL HUNT, Jul 27, 2021 to Jul 29, 2021, Expires in 1 month, Completed data retrieval: 2.3k logs.
- Ransomware File Hash Hunt**: TESSIER-ASHPOOL HUNT, Jul 28, 2021 to Jul 29, 2021, Expires in 4 days, Completed data retrieval: 71 logs.

Expired Hunts: This section displays a table of expired hunt campaigns:

Hunt created	Hunt name	Package name	
Aug 18, 2021 11:11:01 PM	KQL Test	Custom	...
Jul 30, 2021 9:31:34 PM	Duplicate of [Compromised Account Hunt]	Custom IOC Investigation - IP (INTERNAL)	...
Jul 29, 2021 7:58:11 PM	Compromised Account Hunt -30	Custom IOC Investigation - IP (INTERNAL)	...
Jul 29, 2021 7:26:42 PM	Duplicate of [Compromised Account Hunt - 30]	Custom IOC Investigation - IP (INTERNAL)	...
Jul 26, 2021 4:40:12 PM	cryptOr Process Hunt	Custom	...
Jul 26, 2021 7:06:28 AM	Ransomware IoC Hunt	Custom	...
Jul 22, 2021 2:25:02 AM	Duplicate of [Ransomware IoC Hunt Test]	Custom	...

Figure 10 - Active hunt campaigns

ReliaQuest GreyMatter / Tessier-Ashpool

Hunt

Hunt Campaigns **Packages**

Search

Tech Type: Any Availability: Any

Package name	Description
Anti-Virus/Malware	Antivirus is a fundamental tool for preventing and identifying malicious files. Alerting typically focuses on detections for unblocked or high severity signatures, causing some blocked and lower severity signatures to go unnoticed. This hunt pulls logs for malware detection events regardless of severity or action taken in order to identify...
Web Proxy	Attackers may use web based protocols such as HTTP(S) to communicate with external resources to blend in with existing traffic and evade detection. Web proxies help to control web traffic by blocking known risks and can provide additional context such as site categorizations, downloaded files, and user agent strings among...
Windows Authentication - Privileged Accounts	Attackers will need elevated privileges to move laterally in a network and access high value systems and information. Often times they will accomplish this by compromising existing privileged accounts. This hunt focuses on pulling Windows authentication logs involving privileged accounts in order to identify anomalous activity...
Custom IOC Investigation - IP (INTERNAL)	Custom IOC Investigation - IP (INTERNAL) -- test update
Insider Threat	Data theft by employees or contractors with legitimate access to sensitive information may occur through the means such as email, cloud storage sites, messaging apps, or via removable storage devices. This hunt focuses on pulling logs from log sources such as file storage applications, web proxy logs, DLP, and EDR to look for...
DNS Query	DNS is a commonly targeted protocol for c2 communication because it is virtually always available, even those in some of the most locked down environments. This hunt focuses on pulling DNS logs for domains queried in the environment with the goal of identifying potential DNS tunneling as well as rare domains and infrequent...
Windows Authentication - Executive Accounts	Executive accounts may be targeted by attackers since they typically have access to sensitive company information. This Hunt focuses on pulling Windows authentication logs involving executive accounts in order to baseline ordinary activity and look for deviations that may indicate anomalous activity...
F5 RCE Search - (INTERNAL)	F5 RCE Search - (INTERNAL)
Firewall - Hygiene	Firewalls are an essential network security tool that can be configured to control traffic in and out of a network perimeter. As business needs change, old policy exceptions that are no longer applicable may still be in effect and put the network at risk. This hunt pulls firewall logs for outbound traffic to identify potential gaps in configuration...
GS IOC Search - (INTERNAL)	GS IOC Search - (INTERNAL)

1-10 of 28

Figure 11 – Pre-built hunt packages

Select Package

Search Packages

Tech Type: Any Availability: Any

Custom Campaign

Build and run a custom Hunt Campaign without preset queries.

OWindows Authentication - Hygiene T1110 - Brute Force T1078 - Valid Accounts T1098 - Account Manipulation... Timespan of 7 days Data kept for 60 days Select Package	Anti-Virus/Malware Antivirus is a fundamental tool for preventing and identifying malicious files. Alerting typically focuses on detections for u... Timespan of 30 days Data kept for 60 days Select Package	Custom IOC Investigation - IP (INTERNAL) Custom IOC Investigation - IP (INTERNAL) --test update Timespan of 7 days Data kept for 60 days Select Package
DNS Query DNS is a commonly targeted protocol for c2 communication because it is virtually always available, even those in some of ... Timespan of 7 days Data kept for 30 days Select Package	F5 RCE Search - (INTERNAL) F5 RCE Search - (INTERNAL) Timespan of 4 days Data kept for 30 days Select Package	Firewall - DNS Malware on infected endpoints may attempt to communicate directly with external DNS servers in order to bypass logging... Timespan of 7 days Data kept for 60 days Select Package
Firewall - Hygiene Firewalls are an essential network security tool that can be configured to control traffic in and out of a network perimeter. ... Timespan of 7 days Data kept for 60 days Select Package	GS IOC Search - (INTERNAL) GS IOC Search - (INTERNAL) Timespan of 30 days Data kept for 60 days Select Package	IDS/IPS (IN DEVELOPMENT) Intrusion Prevention and Detection Systems (IDS/IPS) are fundamental in identifying malicious network traffic such as ex... Timespan of 30 days Data kept for 60 days Select Package
Insider Threat Data theft by employees or contractors with legitimate access to sensitive information may occur through the means such as... Timespan of 7 days Data kept for 60 days Select Package	IOC Hunt - Domain (INTERNAL) IOC Hunt - Domain (INTERNAL) Timespan of 14 days Data kept for 60 days Select Package	

Figure 12 – Choose a pre-built hunt package or create build a custom hunt campaign

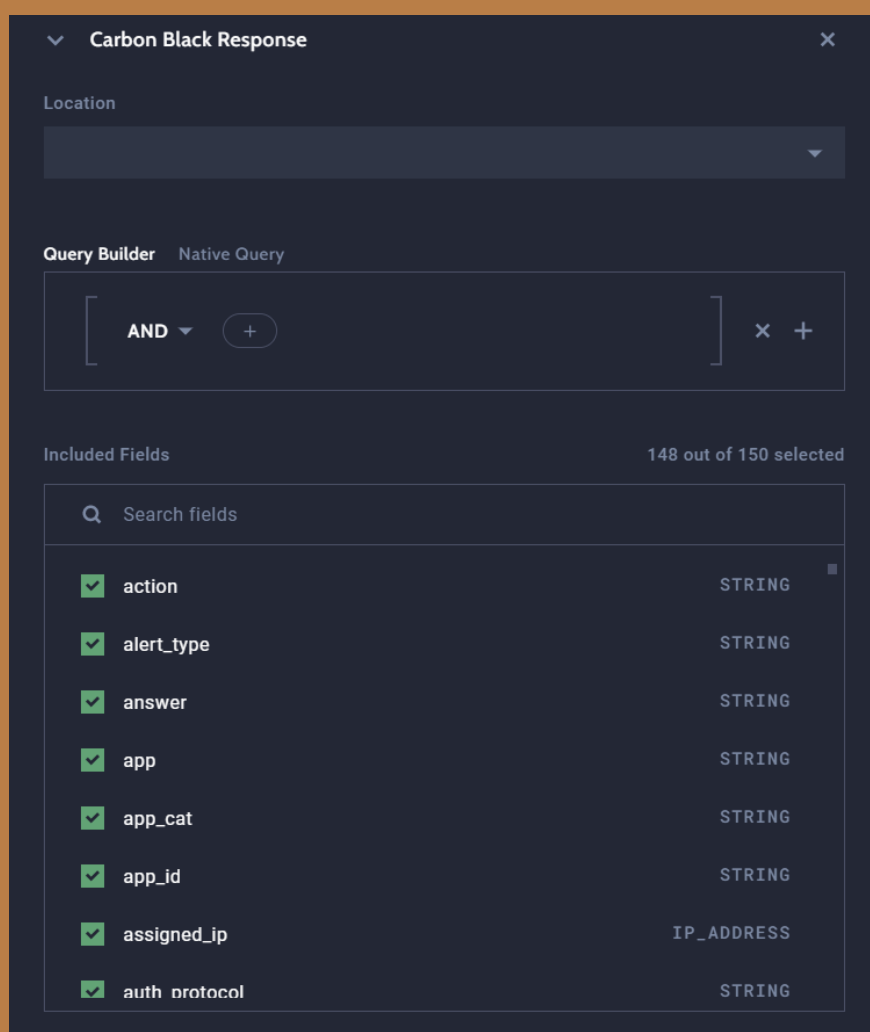


Figure 13 - The Query Builder

Automate

GreyMatter makes automated hunts possible via curated playbooks. New playbooks are released with each new technology integration, and GreyMatter provides additional customization options – playbooks can be tuned and tweaked based on customer's needs.

Playbooks can help analysts

understand if the company's IT controls are effective and if the security technologies the company has deployed really do help defend against the threats out there.

Customers can also install agents on their Windows, Linux, and Mac endpoints, and use pre-built playbooks to perform actions on them (e.g., search for evidence of lateral movement, mass user delete

actions, and so on).

If a pre-built playbook doesn't cover their needs, they can build their own. They can also build a playbook based on the latest "attack of the day." For example, they can make it check for password account guessing via SMB, followed by admin account manipulation. These "new" playbooks can be saved and executed at will.

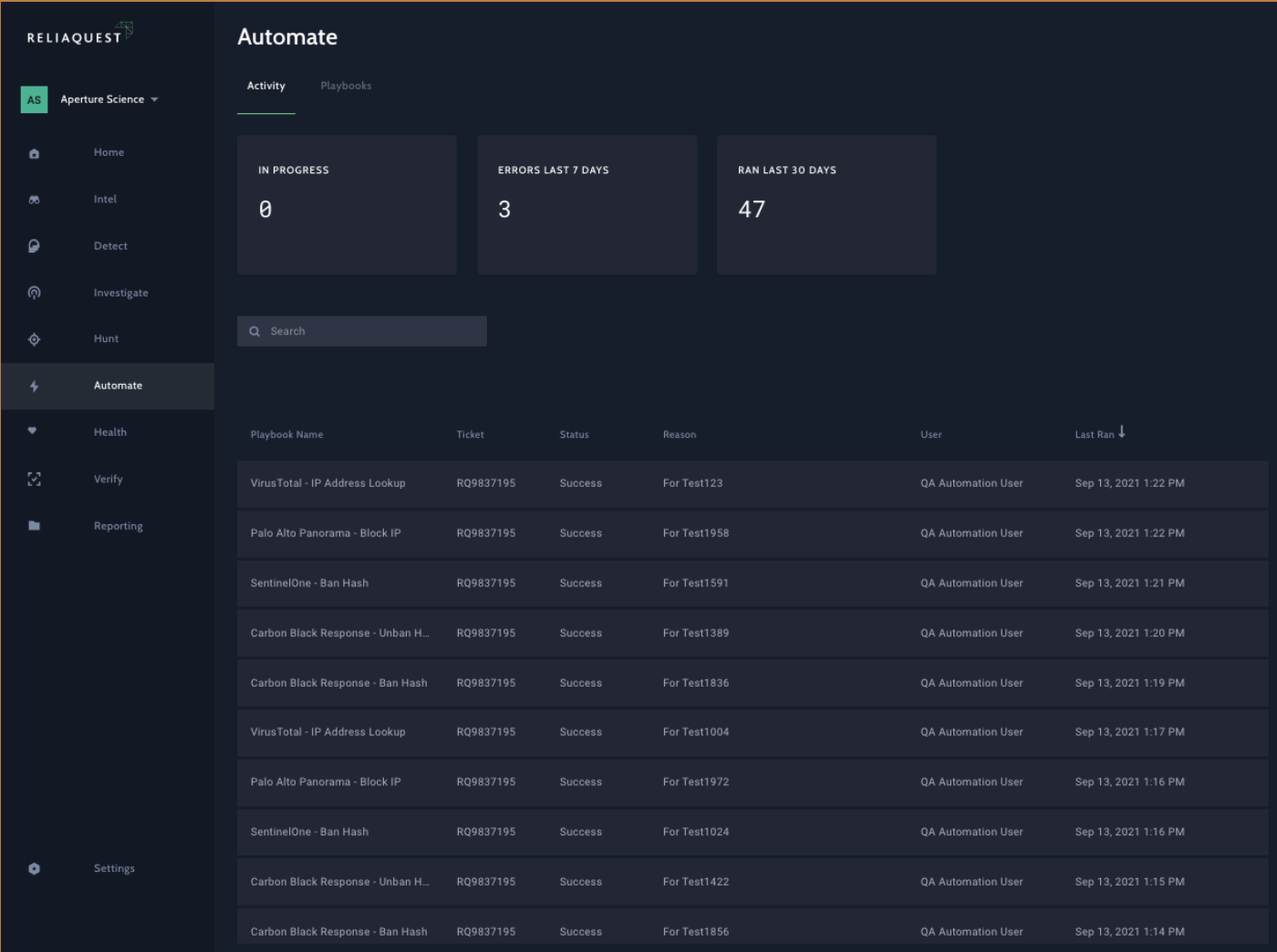


Figure 14 – Automation activity overview



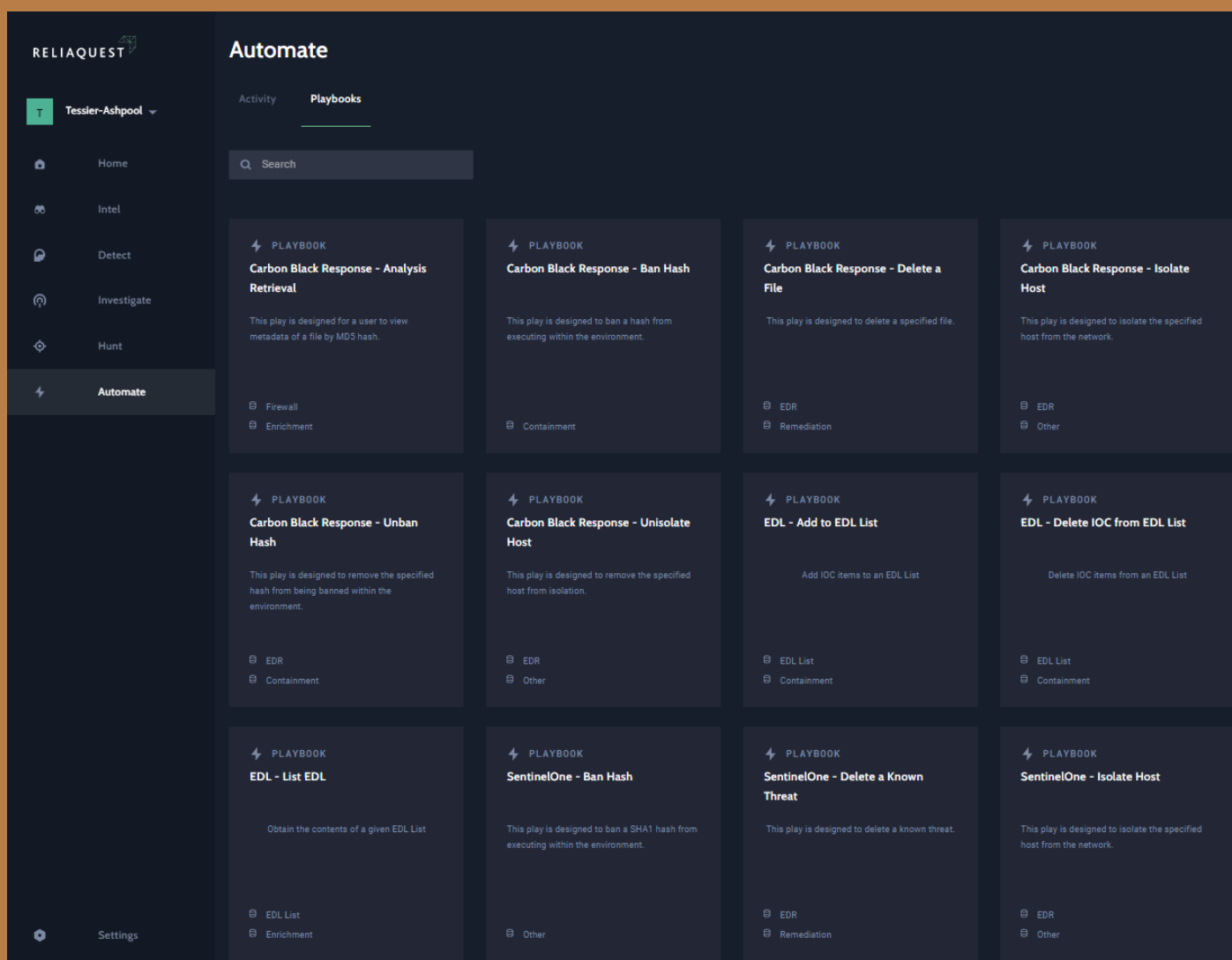


Figure 15 - Some of the prepared playbooks

Conclusion and verdict

Aggregating data across different technologies is not a new thing. What ReliaQuest brings to the table is an offering that shows an overview of active risks/threats and offers root cause investigation and response capabilities from the same console. A unified point of view beats checking and correlating data from 10 or

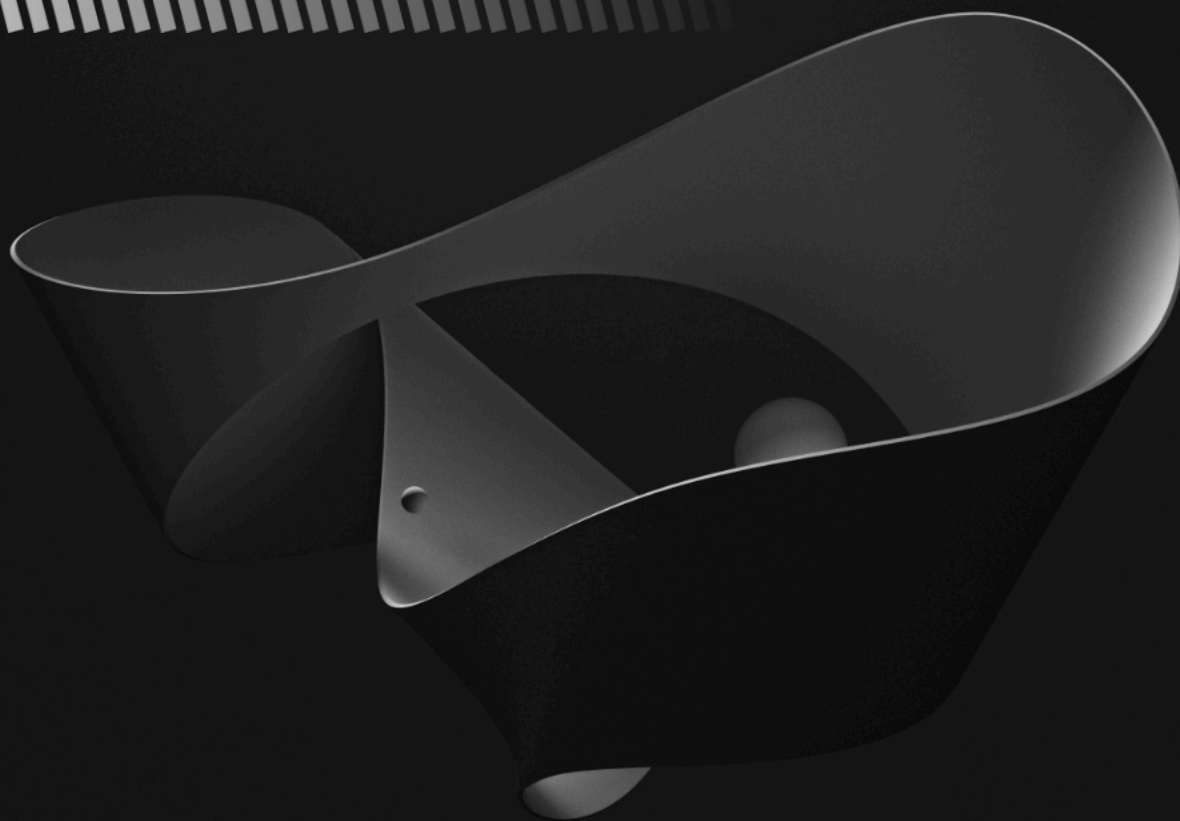
more consoles: It's faster, easier and, consequently, more economical.

The two features worth highlighting are the Universal Translator and the playbooks.

The Universal Translator is amazing: it allows the system to "talk" to any of the integrated technologies and removes the need for analysts to learn different

query languages.

Playbooks combine the experience gained by ReliaQuest engineers while collecting threats, identifying threat "fingerprints" and curating customer responses. They can help customers solve problems that they didn't realize they had and can be made to cover any situation imaginable.



SOPHOS IS SHAPING THE FUTURE OF SECURITY

Cooperation and information sharing is crucial to information security. You've heard this many, many times - from government and law enforcement officials, information security luminaries, enterprise leaders, infosec professionals, and academics - because it's an incontestable truth: we can't protect everything that needs protecting by ourselves.

Zeljka Zorz, Managing Editor, Help Net Security

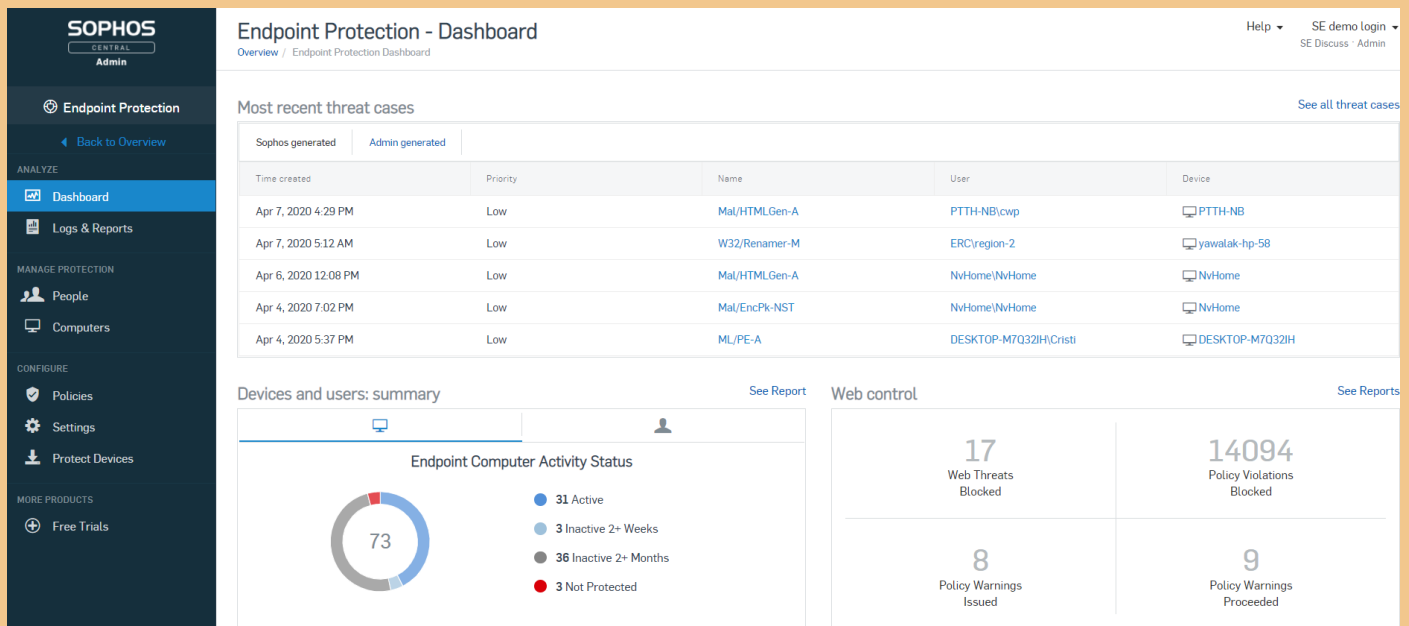


Figure 1 - Sophos Central is a single cloud management solution across all Sophos next-gen technologies

Our information systems are interconnected and part of a bigger ecosystem, and we must cooperate to help boost the cybersecurity of each element for the good of all, especially because cyber attackers out there are becoming increasingly sophisticated and are more than willing to work together, as well.

How the Sophos adaptive cybersecurity ecosystem advances the cybersecurity industry

There are formal, sector-specific collaboration initiatives out there, such as the US DHS Cyber Information Sharing and Collaboration Program, but there are also projects such as the Sophos adaptive cybersecurity ecosystem, an open security platform that optimizes threat prevention, detection and response and is constantly learning based on the collective input of Sophos products, partners, customers, developers, and other security industry vendors.

Sophos's security solutions are inherently part of it, but third parties can also take advantage of the ecosystem – even if they don't use the company's products.

"We believe that having an open platform is the only way to advance the industry and improve defenses," says Dan Schiappa, chief product officer at Sophos.

"Our information systems are interconnected and part of a bigger ecosystem, and we must cooperate to help boost the cybersecurity of each element for the good of all."

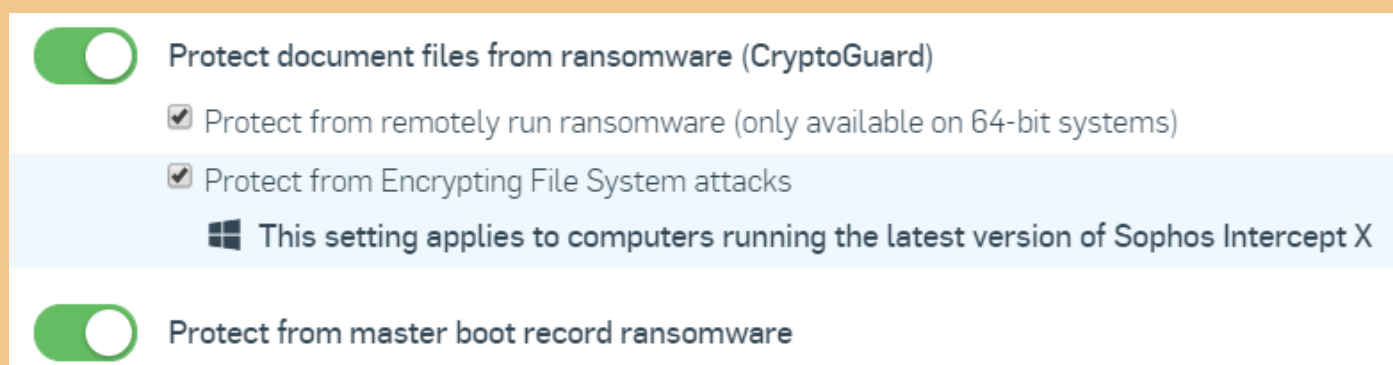


Figure 2 - Intercept X Advanced with XDR is built on top of the world's best endpoint protection, including ransomware specific protections

“Organizations need to have visibility into their entire security IT ecosystem. So, we have created a platform that allows for easy API-based integration into our adaptive cybersecurity ecosystem, so that third parties – whether adjacent technology vendors or competitors – can be integrated in the ecosystem.”

Another way in which Sophos is driving the entire cybersecurity industry forward is with Sophos XDR, the industry's only extended detection and response (XDR) solution that synchronizes native endpoint, server, firewall, and email security.

Sophos XDR

XDR solutions are considered by many to be the future of detection and response.

“The promise of XDR is to be what SIEMs were meant to be: a solution that will provide the right amount of data and the right amount of visibility to security operators, and that will be able to detect issues rapidly and resolve them quickly,” Schiappa opines.

“SIEMs failed at that because they collected

too much data and, as a result, they made it very difficult for an analyst to make heads or tails of it. Also, the correlation they used was not AI-driven – it was more of a rules-based model, and it made for a very noisy environment. The promise of XDR is that with the advent and maturation of artificial intelligence, it allows us to collect the right data and just the right data, and to use AI models to make what we present to the security analysts more actionable.”

Sophos XDR is built on the industry's richest dataset: its data lake stores critical information from Intercept X, Intercept X for Server, Sophos Firewall, and Sophos Email (and, very soon, Cloud Optix and Sophos Mobile).

Data is stored on devices for up to 90 days, and cross-product data is stored in the cloud-based data lake for up to 30 days. The data lake creates the ability to get key information from devices even when they're offline and combining cloud-based data lake forensics with on-device data provides broad and in-depth contextualized insights.

Sophos XDR combines the AI-correlated and

analyzed data with the knowledge and skills of its own experts and customers (companies and MSSPs) around the world, as well as the capabilities of technology partners and competitors in the security industry.

“We have a very advanced AI capability, and the best AI team in the industry,” says Schiappa.

“We apply AI not only to drive our protections, but to also drive detections, case

management, and as much automation into the system as possible. So, in some cases, it helps identify higher risk and higher threat cases to bring to the attention of the operator. In other cases, it goes all the way to executing the case management on behalf of the operator. The system can learn from how the operators do certain tasks and automate those tasks based on AI. The things we learn from those practitioners we build into our AI model and create a kind of a virtuous cycle that really benefits all of our customers.”

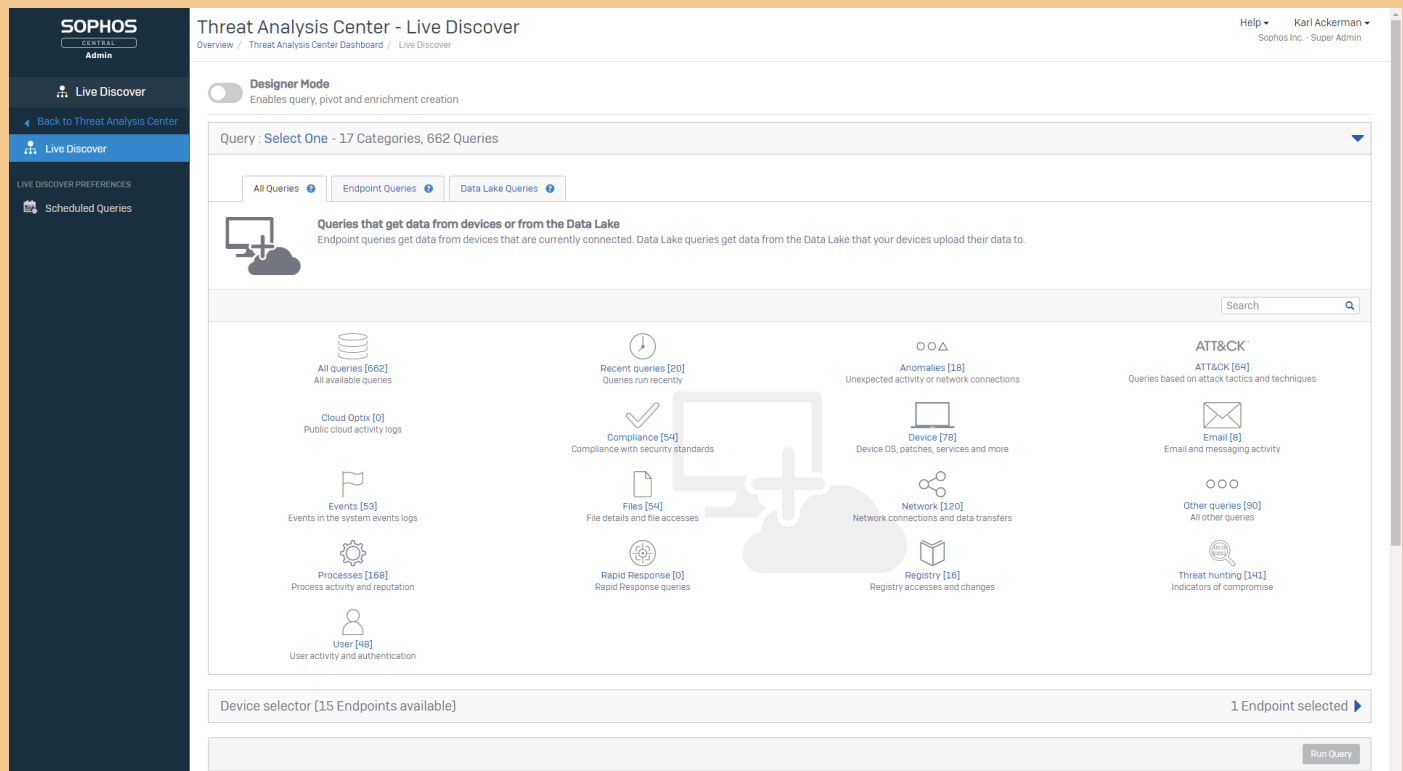


Figure 3 – Users can create their own custom queries or choose from hundreds of pre-written queries

"The system can learn from how the operators do certain tasks and automate those tasks based on AI. The things we learn from those practitioners we build into our AI model and create a kind of a virtuous cycle that really benefits all of our customers."

The screenshot shows the 'Threat Analysis Center - Live Discover' interface. The left sidebar contains navigation links: 'Threat Analysis Center', 'Back to Overview', 'Dashboard', 'Threat Cases', 'Live Discover' (highlighted), 'Threat Searches', and 'Threat Indicators'. The main panel displays a query titled 'Generic Search on Process Details'. Below the title are 'Edit', 'Save', and 'Delete' buttons. The query description states: 'All queries: Generic Search on Process Details. Search for command line, process name, parent processname, device or username. Includes deduplication to identify how RARE the occurrence is. Created by Karl Ackerman.' The 'Sources' section shows 'Data Lake' as the selected source. The 'Expected performance' section notes: 'No performance data available. To get performance data, run the query on one device to test it.' A 'Hide variable editor' section is expanded, showing a table of variables:

Descriptive name	Variable type	SQL variable name	*Enter value to use when query runs
Command Line	String	\$\$Command Line\$\$	%
Device	String	\$\$Device\$\$	%
Ignore when > N Duplicates	String	\$\$Ignore when > N Duplicates\$\$	10000
Parent Process Name	String	\$\$Parent Process Name\$\$	%
Process Name	String	\$\$Process Name\$\$	%
User Name	String	\$\$User Name\$\$	%

Below the table is the SQL query:

```
-- Generic Search
-- VARIABLE: $$Device$$          STRING
-- VARIABLE: $$Command Line$$   STRING
-- VARIABLE: $$Process Name$$    STRING
-- VARIABLE: $$Parent Process Name$$ STRING
-- VARIABLE: $$User Name$$       STRING
-- VARIABLE: $$Ignore when > N Duplicates$$ STRING

WITH Count_list AS (
  With DeDuplicate AS (
    SELECT
      xdr_data.meta_hostname epName,
      xdr_data.meta_os_type Device_Type,
```

Figure 4 – Users can search for almost anything; variables make it easy to customize queries

The screenshot shows the 'Threat Analysis Center - Live Discover' interface with a specific query titled 'Sophos XDR - Firewall - Anti-Spam log info'. The left sidebar is the same as in Figure 4. The main panel displays the query title and 'Back to categories / Events' link. Below are 'Edit', 'Save', and 'Delete' buttons. The query description states: 'Events: Sophos XDR - Firewall - Anti-Spam log info. Check the Sophos Firewall Anti-Spam log info. Created by Kevin Kingston.' The 'Sources' section shows 'Data Lake' as the selected source. The 'Expected performance' section notes: 'No performance data available. To get performance data, run the query on one device to test it.' The SQL query is as follows:

```
-- Sophos Firewall Anti-Spam - SMTP INFO
SELECT
  -- Device ID DETAILS
  device_name, device_serial_id, log_type, log_component, severity,

  -- Query Details
  src_ip, src_country, src_port, protocol, policy_name, action, source_file_name, subject, sender, recipient, message_id, email_size, quarantine_reason, hits,

  -- META information Common for all queries
  dist_key, ingestion_time, asset_id, timestamp, device_model, log_id, log_subtype, log_version, customer_id

FROM xgfw_data
WHERE log_component = 'SMTP'
```

At the bottom, there is a 'Device selector (All sources in Data lake)' section with a dropdown menu set to 'All sources in Data lake' and a 'Run Query' button.

Figure 5 – Sophos XDR Firewall Antispam Log Data Lake Query

SOPHOS
CENTRAL
Admin

Threat Analysis Center

Back to Overview

DETECTION AND REMEDIATION

Dashboard

Threat Cases

Live Discover

Threat Searches

Threat Indicators

Help Kevin Kingston
Kevin@test Super Admin

Threat Analysis Center - Live Discover

Live Discover

Query: ✔ Sophos XDR - Email URL Link Search

Back to categories / Events

Sophos XDR - Email URL Link Search

Edit Save Delete

Events: Sophos XDR - Email URL Link Search

Search for URLs across all Email log data in Sophos Data Lake

Created by Kevin Kingston

Sources

Data Lake

Expected performance

No performance data available. To get performance data, run the query on one device to test it.

Hide variable editor

Descriptive name	Variable type	SQL variable name	*Enter value to use when query runs
From contains	String	\$\$From contains\$\$	%
To contains	String	\$\$To contains\$\$	%
URL contains	URL	\$\$URL contains\$\$	%
client IP	IP Address	\$\$client IP\$\$	%
domain contains	String	\$\$domain contains\$\$	%
subject contains	String	\$\$subject contains\$\$	%

SQL

```
-- Sophos Email URL LINK SEARCH
-- VARIABLE $$From contains$$      STRING
-- VARIABLE $$To contains$$        STRING
-- VARIABLE $$URL contains$$       URL
-- VARIABLE $$client IP$$         IP_Address
-- VARIABLE $$domain contains$$    STRING
-- VARIABLE $$subject contains$$   STRING
SELECT
  timestamp Received_date,
  "from" FROM,
  envelope_recipient To,
  subject,
  domain,
  url Url_Link,
  client_ip,
  scheme,
  mime_date Send_date,
  reply_to,
  array_join(to,',') TO_ARRAY,
  array_join(cc,',') CC_ARRAY
FROM xdr_new_urls_data
```

Device selector (All sources in Data lake)

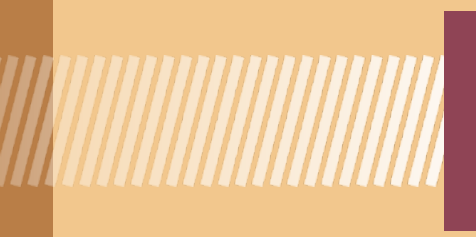
All sources in Data lake

Run Query

Figure 6 – Sophos XDR users can detect and investigate across endpoint, server, firewall, email, and other data sources

One of Sophos’s main goals is to offer an intuitive user experience for both experienced and less knowledgeable security operators, but their ultimate vision is for Sophos XDR to provide the basis for a “driverless” SOC.

“We plan to build interaction capabilities with our own products as well as the third-party solutions that come on board through our Technology Alliance Program. We already have playbooks to execute some automated responses, and users can write playbooks themselves for third-party solutions. We’ll also automate some of that playbook creation through our AI.”



Sophos has one of the largest XDR install bases in the industry, which means that its adaptive cybersecurity ecosystem is gaining an immense amount of input to improve threat prevention, detection and response.

Where response can't be automated, Sophos XDR offers a capability called Live Response, which allows the operator to immediately jump to action and respond to an incident in real time.

Conclusion

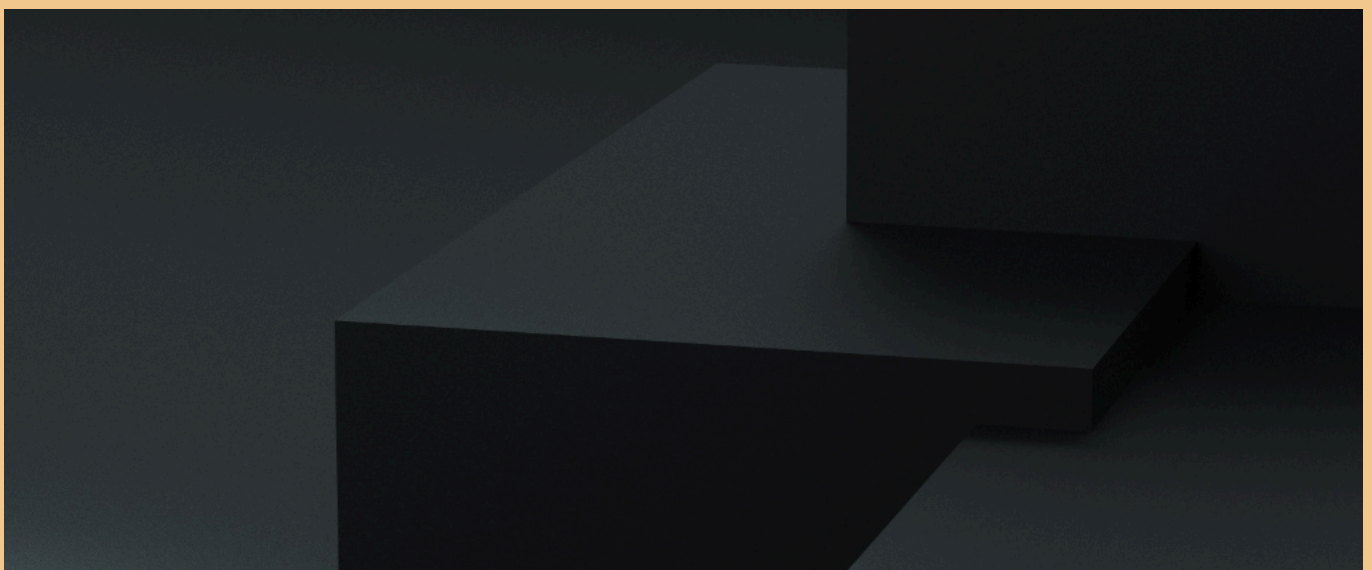
Sophos has one of the largest XDR install bases in the industry, which means that its adaptive cybersecurity ecosystem is gaining an immense amount of input to improve threat prevention, detection and response.

The integration of third-party tools into this native XDR solution is under way, with many MSPs and competitors already participating.

"We've worked with the vendors on some of

the integrations. In other cases, we simply found out one day that the vendor has integrated with us. We're reaching out to members of our Technology Alliances Program to work on more of them, and our current priority is companies that have products that we don't have in our portfolio and customers that have big IT data lakes," Schiappa shared.

"It's shaping up to be a really open, robust ecosystem that is going to provide a wider aperture and more visibility for our customers. And as this collaborative ecosystem grows, more and more vendors and customers will want to join, turning the Sophos adaptive cybersecurity ecosystem into an increasingly comprehensive and efficient cyber defensive apparatus."



USER INTERFACES AT A GLANCE

Features are king, but a software's UI can streamline the work process or degrade the end user's experience.

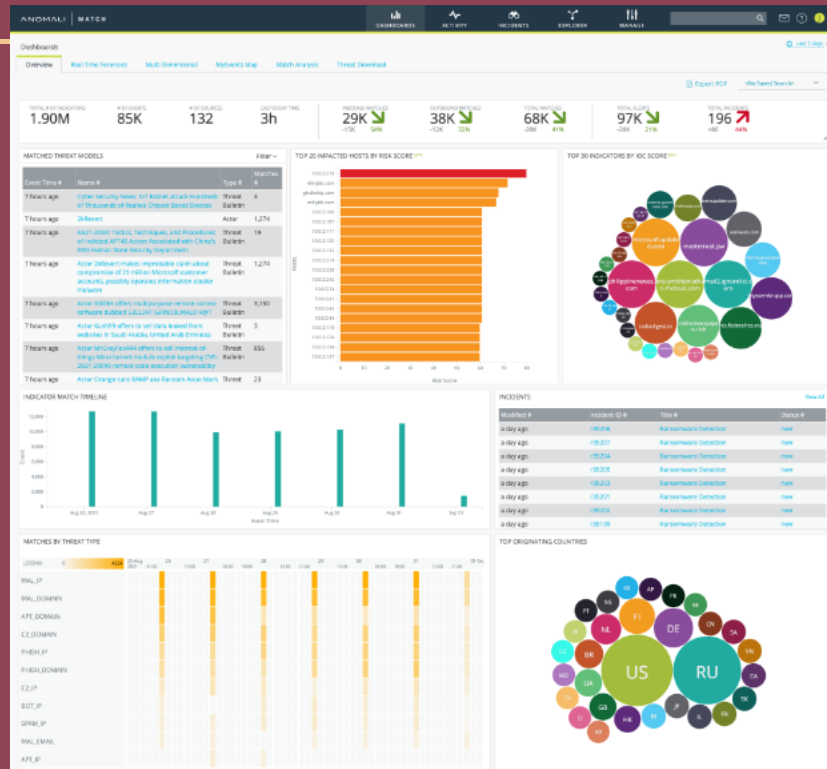
Taking into consideration the look and feel of a product is an important aspect of the decision-making process. This section showcases XDR vendors' product vision and illustrates the software experience they deliver.

ANOMALI

Anomali Match is an intelligence-driven XDR solution that helps organizations identify and respond to threats in real-time by automatically correlating all security telemetry data against active threat intelligence.

Recently added features include custom dashboards, industry news monitoring, enhanced STIX 2.0 support, and MITRE ATT&CK v9.0 integration, which further helps analysts to identify threats and take steps to defend against them.

Match is available on-premises and via the cloud, and can now be used by customers that use the Anomali ThreatStream TIP and by those that don't.



Anomali Match +

< > 🔍 🔒 ⚙️

ANOMALI MATCH
DASHBOARDS
ACTIVITY
INCIDENTS
EXPLORER
MANAGE

Activity

- Apr 13th 2021, 20:11:36 +01:00
APT34 (Digital Shadows Id...)
- Apr 1st 2021, 23:10:19 +01:00
APT10 (Digital Shadows Id...)
- Mar 10th 2021, 23:14:46 +00:00
yalishanda new
- Mar 10th 2021, 23:14:06 +00:00
yalishanda sixx 1.2 clearly
- Mar 3rd 2021, 16:41:47 +00:00
Maze (Digital Shadows Id...)
- Feb 26th 2021, 20:47:48 +00:00
APT33 - Tracking
- Feb 19th 2021, 10:40:06 +00:00
APT28 (Digital Shadows Id...)
- Feb 2nd 2021, 17:26:10 +00:00
Yalishanda Threat Actor ...
- Jan 12th 2021, 19:46:25 +00:00
APT29 (test)
- Jan 12th 2021, 12:11:49 +00:00
Turla (Digital Shadows Id...)
- Jan 5th 2021, 16:55:37 +00:00
UNC2452
- Jul 24th 2020, 10:15:36 +01:00
GRIM SPIDER
- Jul 13th 2020, 10:08:33 +01:00

APT33 - TRACKING

OPEN IN THREATSTREAM

Scanned 46M+ Events across 0 Sources

1 MATCHES

ASSOCIATED IOCS	COUNT
DATE POSTED	Feb 26th 2021, 20:47:48 +00:00
PUBLICATION STATUS	new
TLP	white
ALIASES	
TAGS	Pupy CVE-2017-11774 poshc2 Refined Kitten CVE-2018-20250 APT 33 Quasar APT33 Shapeshift NetWire APT MAGNALLIUM Remcos CVE-2017-0213 Dropshot TurnedUp Iran Nanocore Dark Comet Eflin

MATCHES (1)
ACTOR DETAIL
MITRE ATT&CK

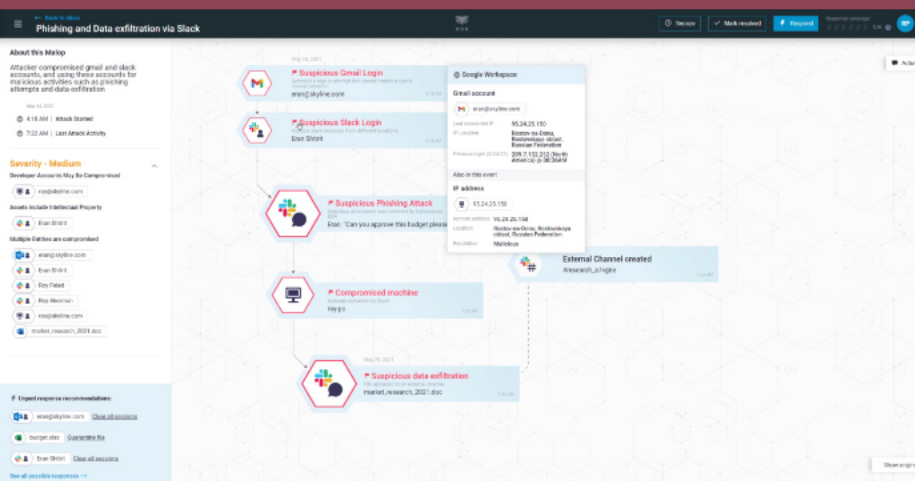
Legend: Associated Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 Items	31 Items	56 Items	28 Items	59 Items	20 Items	19 Items	17 Items	13 Items	9 Items	21 Items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Account Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Clipboard Data	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	BITTS Jobs	Browser Bookmark Discovery	Brute Force	Distributed Component Object Model	Data from Information Repositories	Data Encrypted	Data Transfer Size Limits	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Bypass User Account Control	Credentials in Files	Credential Dumping	File and Directory Discovery	Data from Local System	Exfiltration Over Alternative Protocol	Custom Command and Control Protocol	Custom Cryptographic Protocol
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package Load	Application Shimmmg	Clear Command History	Credentials in Registry	Network Service Discovery	Logon Scripts	Data from Network Shared Drive	Exfiltration Over Other Channel	Data Obfuscation
Spearphishing via Service	Execution through API	BITS Jobs	Bypass User Account Control	CMSTP	Exploitation for Credential Access	Network Share Discovery	Pass the Hash	Data Staged	Exfiltration Over Physical Medium	Fallback Channels
Supply Chain Compromise	Graphical User Interface InstallUI	Change Default File Association	DLL Search Order Hijacking	Component Firmware Hijacking	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Scheduled Transfer	Multi-hop Proxies
Trusted Relationship	LaunchIt	Component Firmware Hijacking	Dylib Hijacking	Control Panel Items	Hooking	Peripheral Device Discovery	Remote Services	Input Capture	Man in the Browser	Multi-band
Valid Accounts	Local Job Scheduling	Component Object Model Hijacking	DCShadow	Deobfuscate/Decode Files or Information	Input Prompt	Permission Groups Discovery	Remotely Executed Task			



Cybereason's mission is to “reverse the adversary advantage” by empowering Defenders with technology and ingenuity to end cyber attacks. Why do adversaries have the advantage? For one, attackers are taking advantage of our increasingly dispersed workforce,

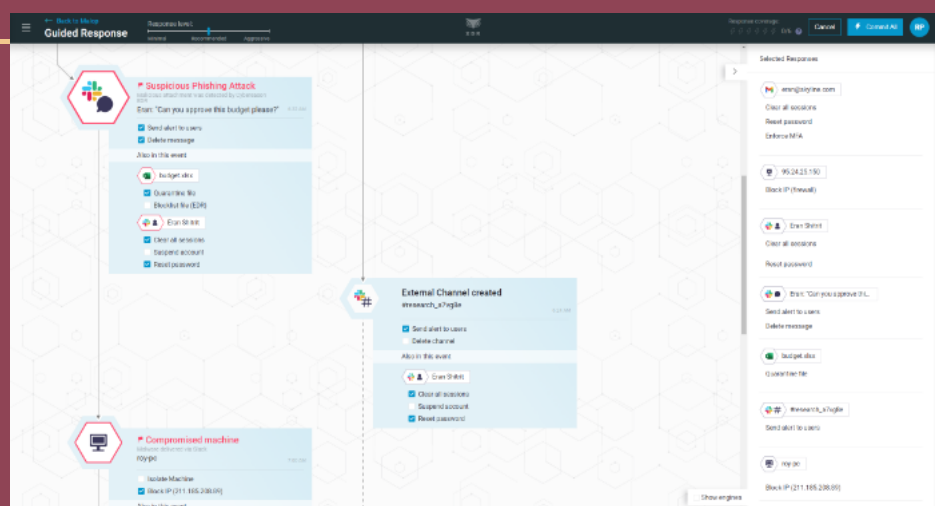
data, and IT infrastructure. Cybereason XDR extends security detection and response capabilities from the endpoint to the complete IT environment, including workspace & identity, cloud infrastructure, and network sources and tools.



This is accomplished through an operation-centric approach, which focuses on ending Malicious Operations (MalOps) instead of generating individual alerts. MalOps are visual attack stories that automatically surface (1) root cause, (2) affected users & assets, (3) attacker tools & known C&C, (4) a timeline of events, and (5) suggested response actions. This time-saving correlation and analysis slashes alert fatigue & false positives, and upskills

analysts with innovations like Guided Response, which recommends actions based on best practices, Incident Response learnings, and past workflows.

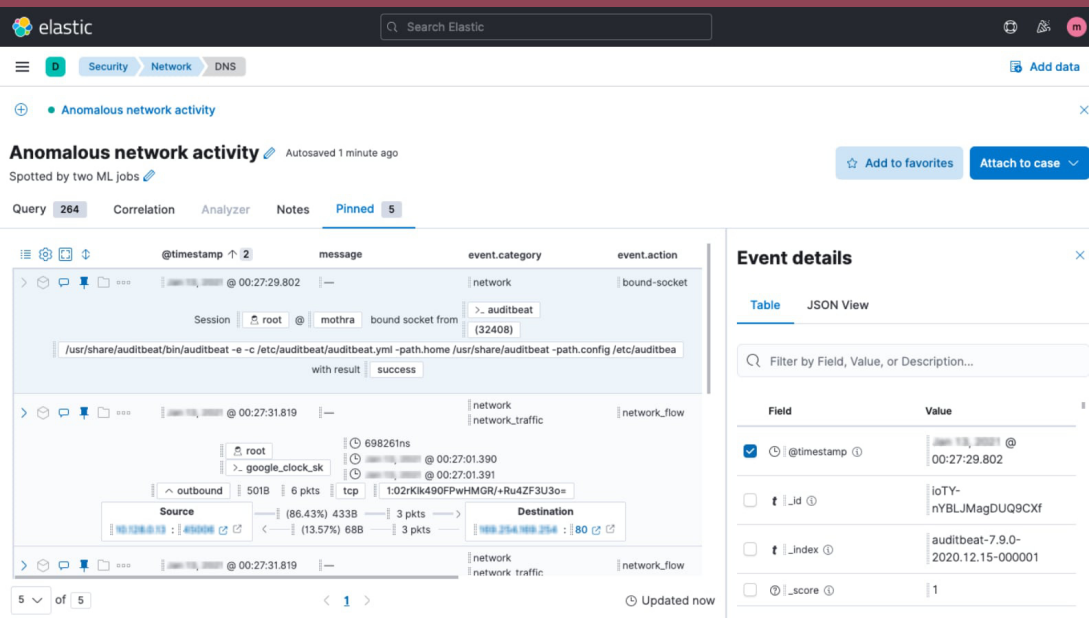
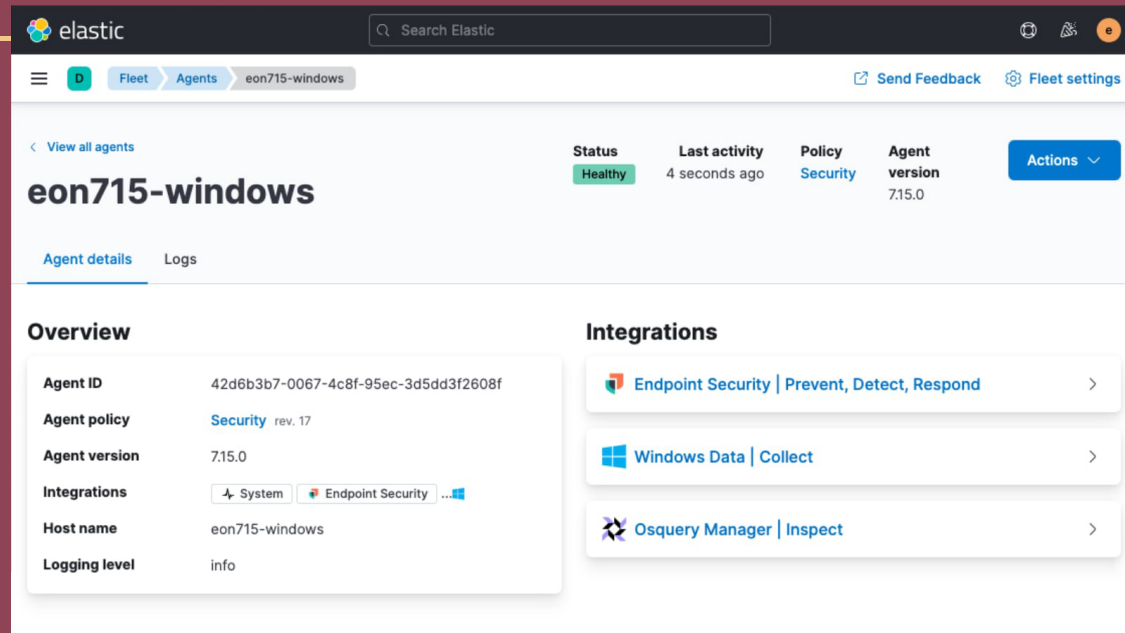
Unlike SIEM and log management solutions, Cybereason XDR can be deployed across a large-scale environment of 100,000+ endpoints and users in 72 hours. Cybereason XDR can be used out-of-the-box to respond to an active attack. If you're seeking to build security operations with an approach focused on Prevention and Response that supports your existing IT & security investments, consider XDR.





Elastic Security unifies SIEM and Endpoint Security for XDR. With a single agent for Linux, Windows, and macOS hosts, organizations can block ransomware and malware, stop advanced threats, collect endpoint data, perform ad-hoc host inspection, and remotely invoke response actions (e.g., isolate an infected host). Elastic

Security is built for speed and scale, and available free and open to organizations everywhere.



Elastic Security equips the SOC with limitless environmental visibility and the power to analyze years of data, appreciably improving organizational security posture. Practitioners can quickly search and correlate data of any kind, whether in the cloud or on-prem, driving efficient threat hunting, alert triage, and investigation. Data is

presented on an interactive timeline that guides analysts to quickly comprehend the relationships between key data points. From this unified view, practitioners can examine raw logs, annotate and pin key events, and prepare findings for immediate escalation.



FireEye XDR enables security analysts to investigate breaches, identify the root cause, and remediate attacks for organizations with products in every major market category, including Network Security, Endpoint Security, Email Security, Cloud Security, Security Orchestration, Automation and Response (SOAR), and Security Information and Event Management (SIEM).

In addition to providing detection through FireEye products, out-of-the-box integrations for hundreds of third-party vendors is provided for data aggregation and guided response actions. This is all delivered via a native-built SaaS architecture that is high-performant, scalable, and removes operational burden from users.

FireEye XDR provides guided investigation workflows, allowing organizations to reduce the impact of a security incident. This approach improves analyst and SOC efficiency by correlating disparate events from multiple tools into actionable investigations which provides reduced organizational risk by automating threat detection and investigation, accelerating response, and prioritizing the prevention of incidents.

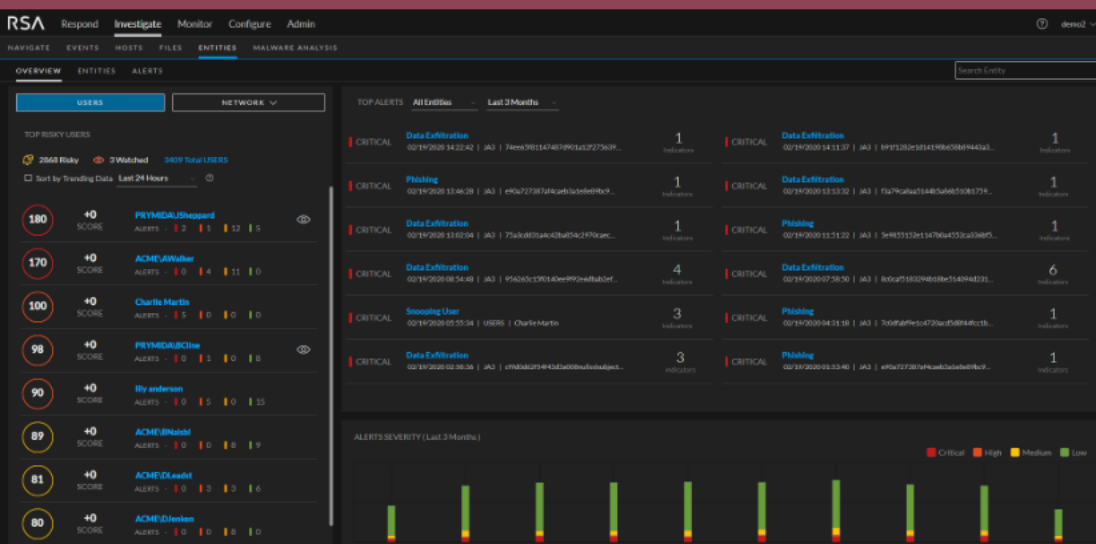
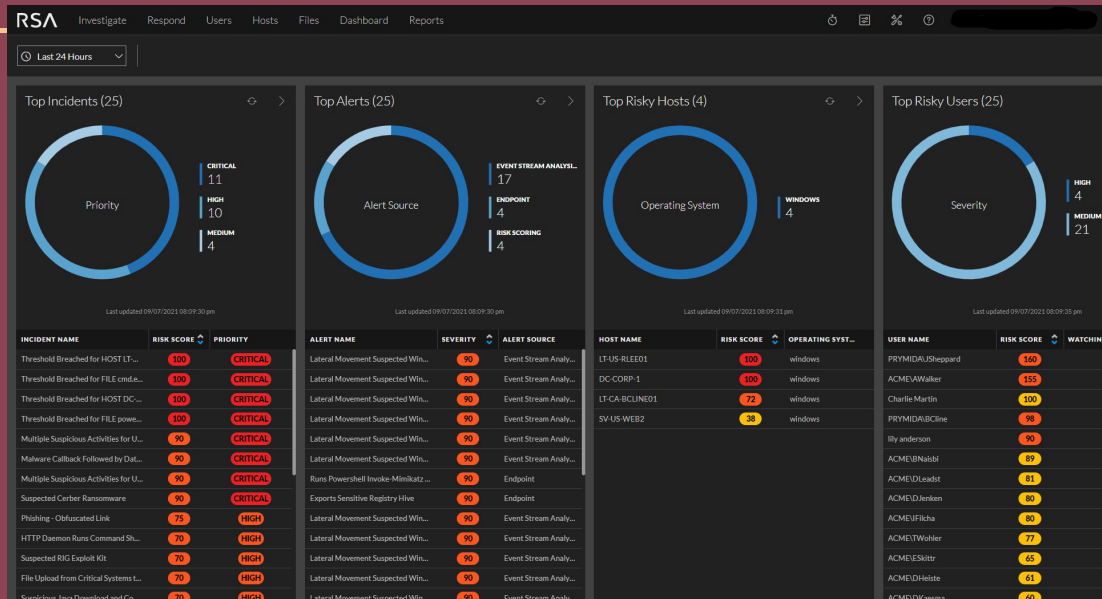


This approach delivers high levels of detection efficacy and analytics, with incident response best practice playbooks updated daily to reflect the changing global threat landscape. Ultimately, teams gain the ability to prioritize analyst time and mitigate risk by addressing what is critical to their security operations.



NETWITNESS

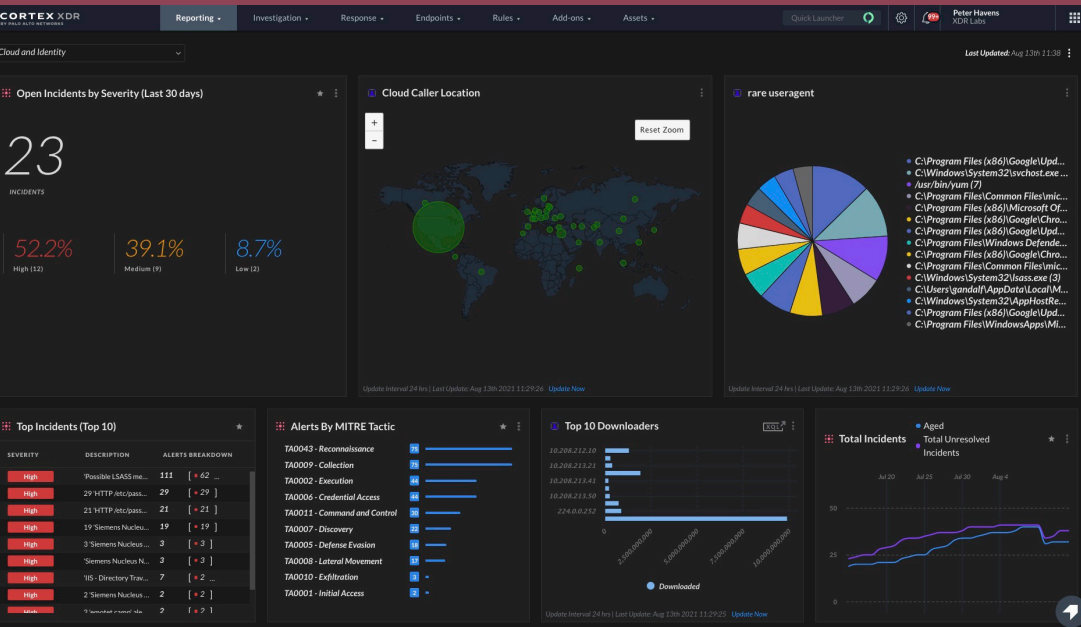
The NW Platform Springboards view provides analysts a consolidated perspective on all threats present in their environment with a unified XDR data model approach. Data is enriched with context, analytics, and threat intelligence and presented in an easy-to-understand layout that draws users attention to relevant threats to take action natively within the tool.



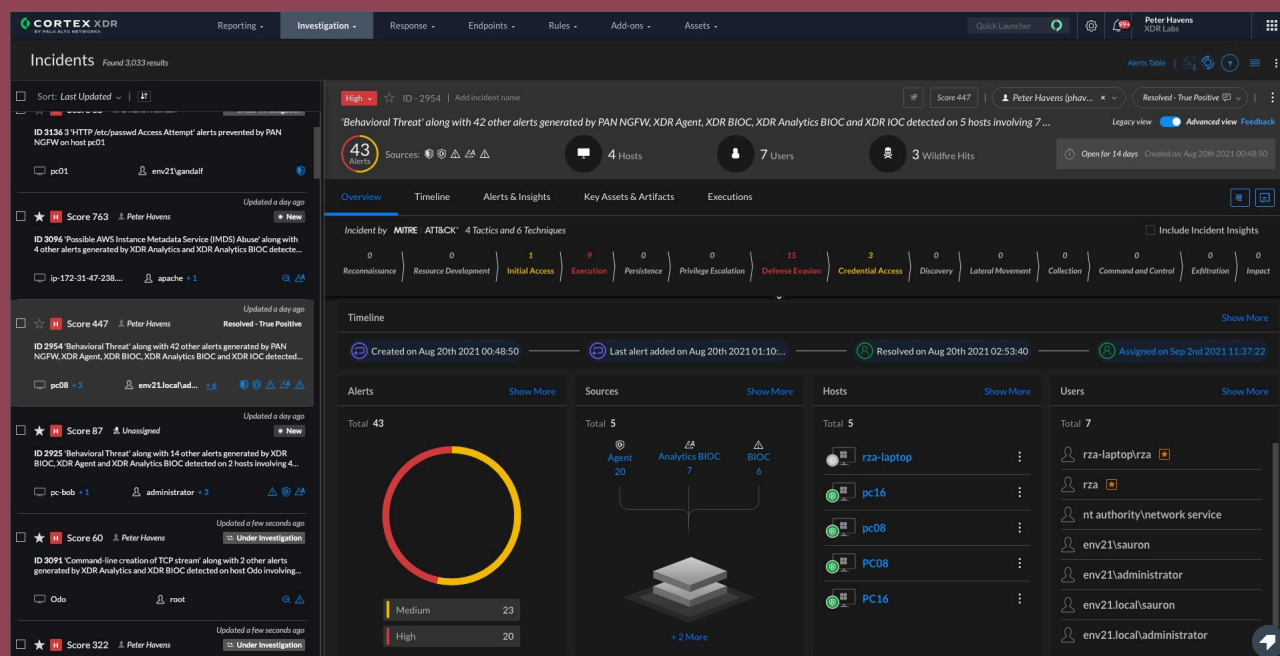
The NW Platform Detect AI engine provides cloud-powered advanced user and entity behavior analytics (UEBA) on hundreds of data points from log, endpoint, and network data in a true unified XDR approach. This unsupervised machine-learning technology

gives analysts a more robust arsenal for detecting anomalous behaviors and responding across their IT environment.

Analysts see behavior and anomalies grouped into relevant use-cases with aggregated risk scores and dynamic feedback to show the most relevant threats to the business.



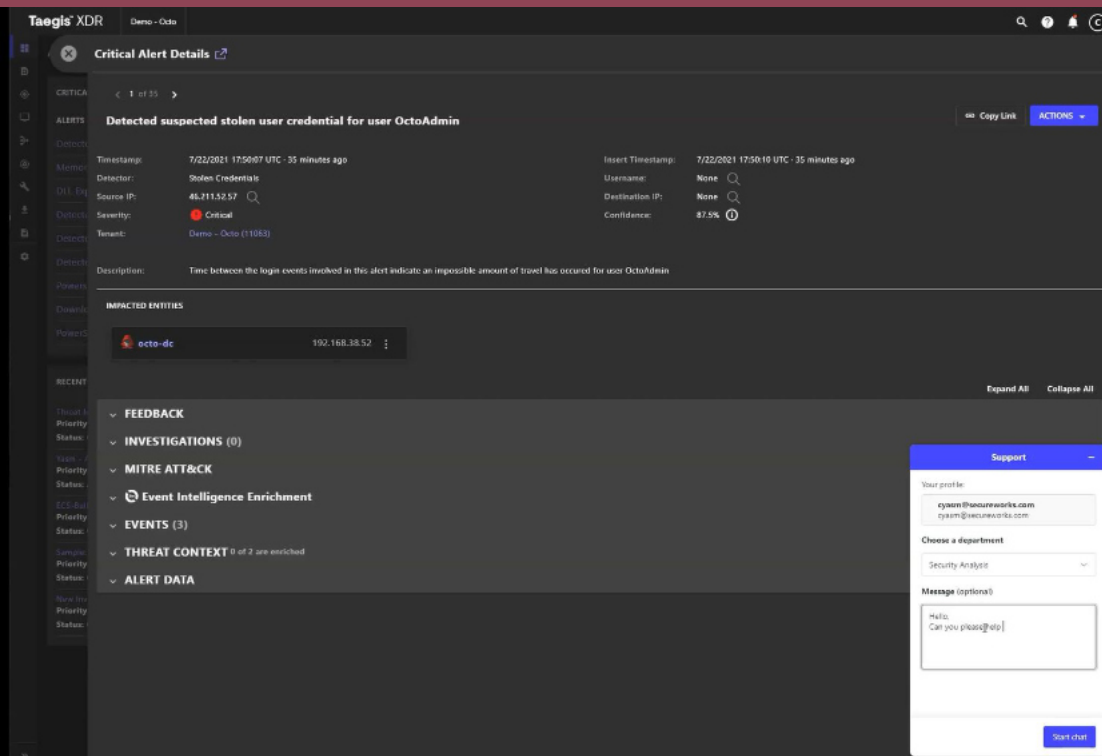
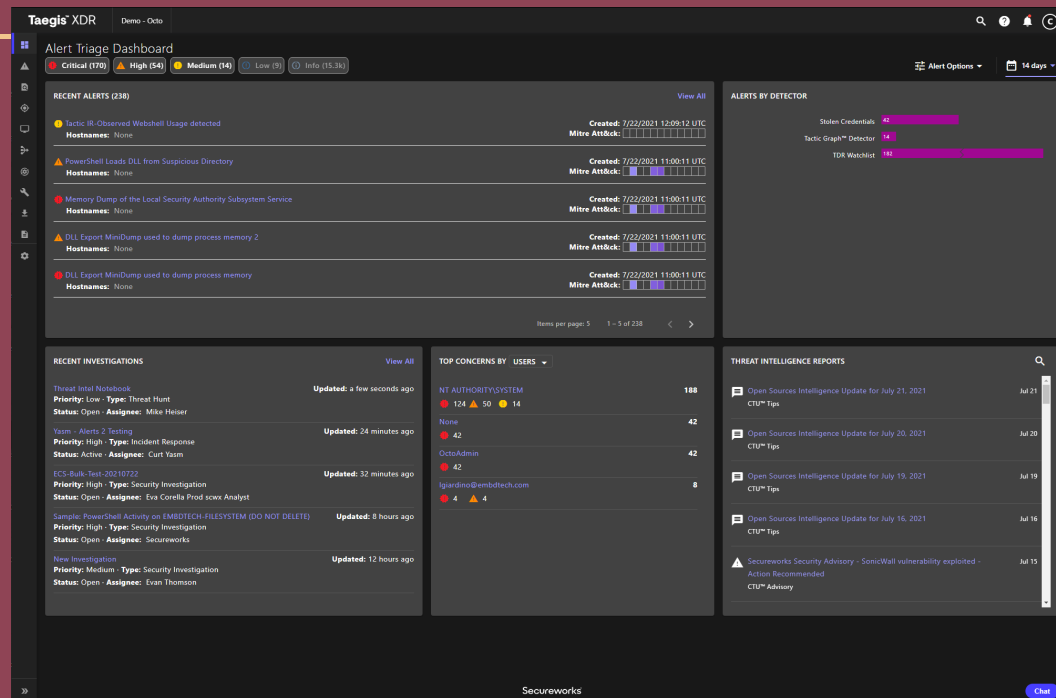
Cortex XDR 3.0 extends deep analytics-based detections for cloud threats and attacks that involve activity from compromised accounts or malicious insiders. Cortex XDR leverages machine learning to identify and correlate activity from multiple sources into attack scenarios that optimize analytics-based detections and threat hunting.



Cortex XDR 3.0 enables security analysts to quickly evaluate threats across their entire business, automating the early phase of investigation by leveraging machine learning to stitch correlated activity and alerts into complete security incidents. The newly revamped incident management UI provides unparalleled speed when scoping, investigating, and responding to cyberattacks that span multiple users and assets.

Secureworks®

The Alert Triage Dashboard allows users to view activity in their environment and quickly assess possible ongoing threats of malicious activity. The Critical Alerts Dashboard Panel displays critical alerts by specified date range. The MITRE ATT&CK category of each critical alert is indicated by the inline info bar.



Secureworks Taegis XDR has a live chat support feature. To bring it up, select the chat button in the lower right-hand corner of Secureworks Taegis XDR. The “Ask an Expert” chat feature provides real-time collaboration to help with an investigation or recommend a response when it matters most.



Stellar Cyber's Open XDR Platform delivers an XDR Kill Chain, fully compatible with the MITRE ATT&CK framework, presenting every aspect of attacks while remaining intuitive to understand. All Stellar Cyber alert types are aligned to the XDR Kill Chain out of the box. The GUI dashboard is shaped like a loop to help highlight the severity of the breach and indicate the earliest stages of a breach.



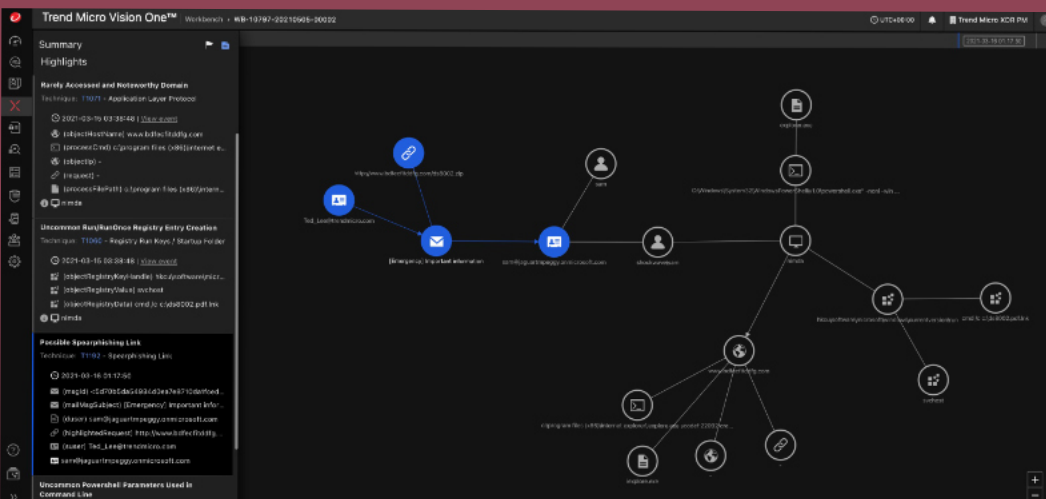
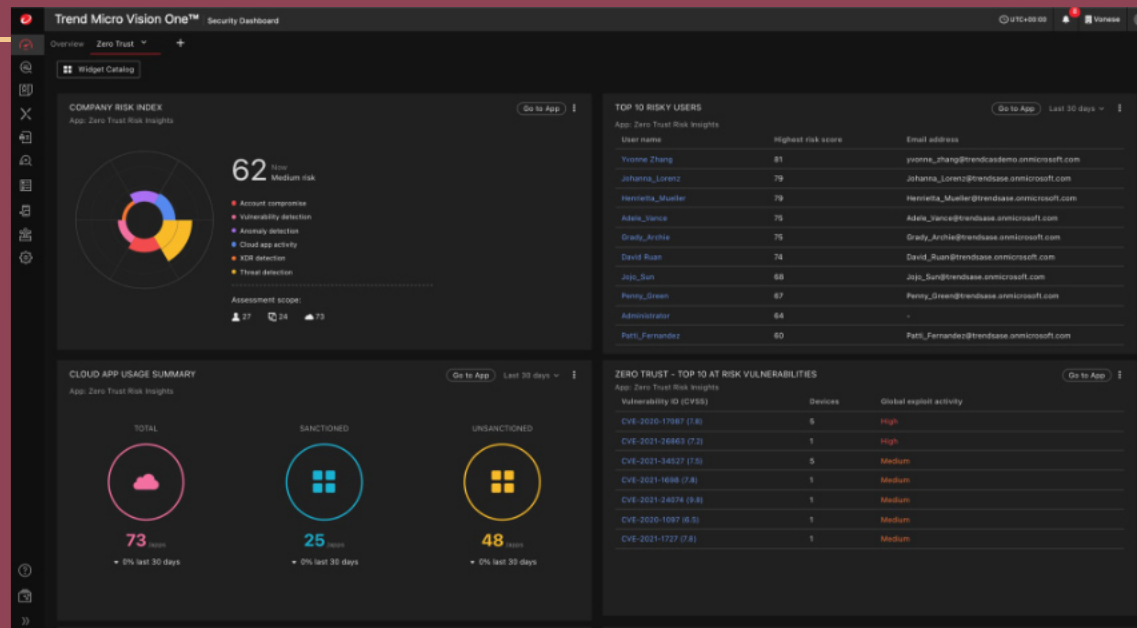
The AI engine in the Stellar Cyber Open XDR Platform automatically groups related alerts into incidents and prioritizes them in order of severity, so analysts know exactly which incidents to target first. This automation reduces the investigation effort from the number of alerts (hundreds) to the number of incidents (tens of incidents) – an order-of-magnitude improvement in MTTD. Automated playbooks can be triggered to drive a similar improvement in MTTR.



Zero Trust Risk Insights equips security teams with the ability to continuously monitor the security posture of their organization and effectively prioritize critical threats that require attention.

It helps to proactively identify risks such as those that stem from a business' devices or applications and

helps to seek out threats as a result of a spoofed identity that has infiltrated an organization's perimeter. With the risk score, organizations can track trending and compare to peer companies in the same industry or region.



The Workbench app within Trend Micro Vision One produces alerts triggered by XDR detection models that correlate suspicious activity across the customer's environment.

Within the workbench, a security analyst gains a

view of the full attack story and can investigate through an in-depth root cause and impact analysis to understand the scope and severity of the detection, along with the ability to take immediate action to respond.



STELLAR CYBER OPEN XDR: MAKING SECURITY FUN AGAIN

Endpoint detection and response (EDR) is a crucial part of extended detection and response (XDR), but XDR does not just mean extended EDR – the “extended” part of the label refers to extended coverage, visibility, integration, analytic, detection, investigation and response capabilities XDR solutions offer.



Zeljka Zorz, Managing Editor, Help Net Security

XDR is a relatively new product category, but the XDR market segment is expanding at a good pace.

For Stellar Cyber, one of the notable players in the market, the “X” in their flagship security operations platform Open XDR stands for “everything”, as it can collect and correlate data from the entire enterprise infrastructure and every existing security tool, and aims to protect the entire enterprise attack surface: endpoints, network, cloud, identity, applications, and email.

XDR promises to reshape security operations

XDR is a relatively new product category, but the XDR market segment is expanding at a good pace.

Forrester analyst Allie Mellen has recently pointed out that one of the reasons why XDR is getting so much hype lately is because “there is a yearning in the security community for a solution that can provide better outcomes than what they are using today.”

Also, a recent survey conducted by the Ponemon Institute has shown that working in a security operations center (SOC) is often a painful affair and that many SOC members battle with burnout, overload and chaos.

Sam Jones, VP of product management at Stellar Cyber, says he understands their frustration; as a former SOC member, he often spent his days connecting systems, managing and manipulating data into the

same format, writing rules to discover threats, and often realizing at the end of the day that he had not done any actual “security.”

“Our Open XDR platform makes connecting the systems simple, the data is automatically normalized into an easy-to-understand format, there's different alerts that come out of the box so that you can focus on investigating and doing real security work, and you can quickly add your own context into the system,” he notes.

“It's simply more fun to work in security through a platform like this, because the low impact, boring stuff you usually spend most of your time on is automated, and you can work alongside an AI that presents interesting stories and pieces of data so that you can respond and work with the system more effectively.”

XDR needs a new cyber kill chain

To deliver the on the promises of XDR – improved visibility (of the entire attack surface), threat detection, investigation, response, and overall SOC productivity and effectiveness – Stellar Cyber found that existing kill chains just didn't work. As a result, they created the XDR Kill Chain, which covers the complexity of modern attacks by focusing on anomalous / suspicious behavior as well as on attackers' TTPs, and works both for human analysts and Open XDR's algorithms.



Figure 1 – All Stellar Cyber alert types are aligned to the XDR Kill Chain out of the box. The GUI dashboard is shaped like a loop to help highlight the severity of the breach and quickly indicate the earliest stages of a breach

Based on MITRE ATT&CK, the XDR Kill Chain is general enough for all detections and can differentiate between internal and external attacks, thus helping analysts know exactly where to look to stop attackers.

Its loop design, which mimics hackers' thinking and acting, prioritizes detections into five phases – initial intrusions, persistent foothold, exploration, propagation, and exfiltration – that have been layered on top of MITRE ATT&CK tactics.

“Attacks aren't linear, and the loop reflects that: Exploration and propagation happen over and over again, and that's how we

characterize it so that we can detect it accordingly,” Jones explains.

Alerts appear in the context of these five phases and are prioritized, so analysts can see attacks as they happen and respond to the most emergent needs first.

Finally, the XDR Kill Chain also makes it easy for users to add new tactics and techniques, and allows (multi-)tagging, which makes it easier to pinpoint new attack trends.

Stellar Cyber Open XDR

XDR solutions can be native or hybrid/open.

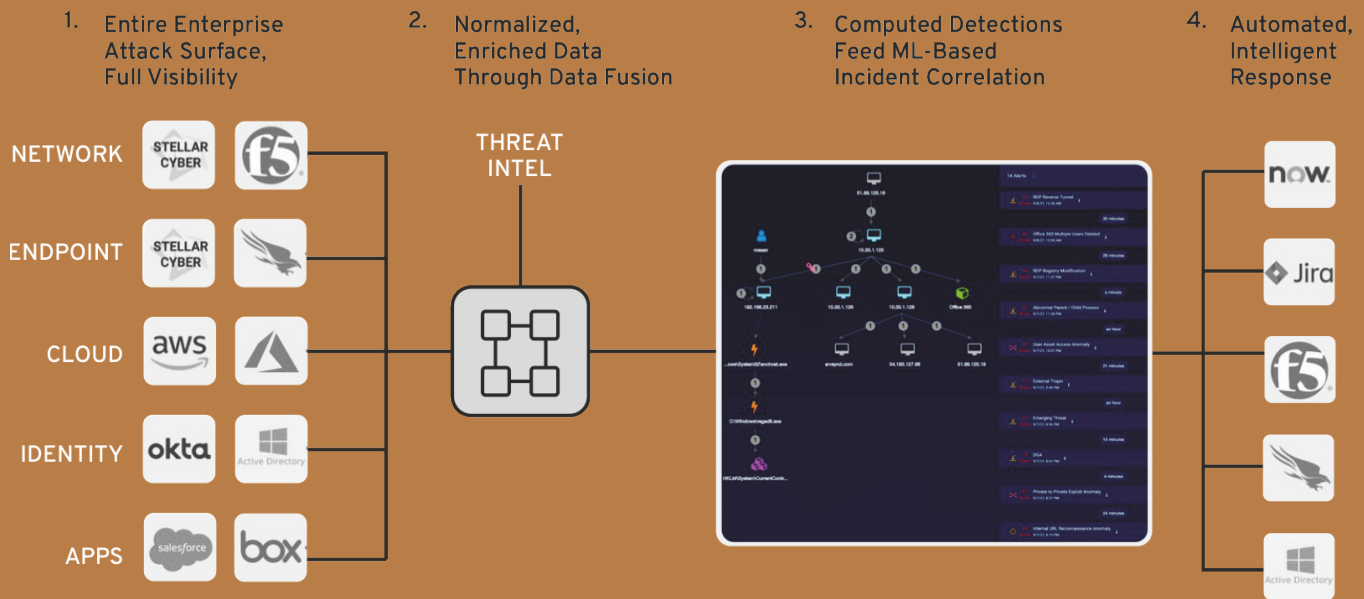


Figure 2 - The AI engine in the Stellar Cyber Open XDR Platform automatically groups related alerts from all data sources into incidents and prioritizes them in order of severity, so analysts know exactly which incidents to target first

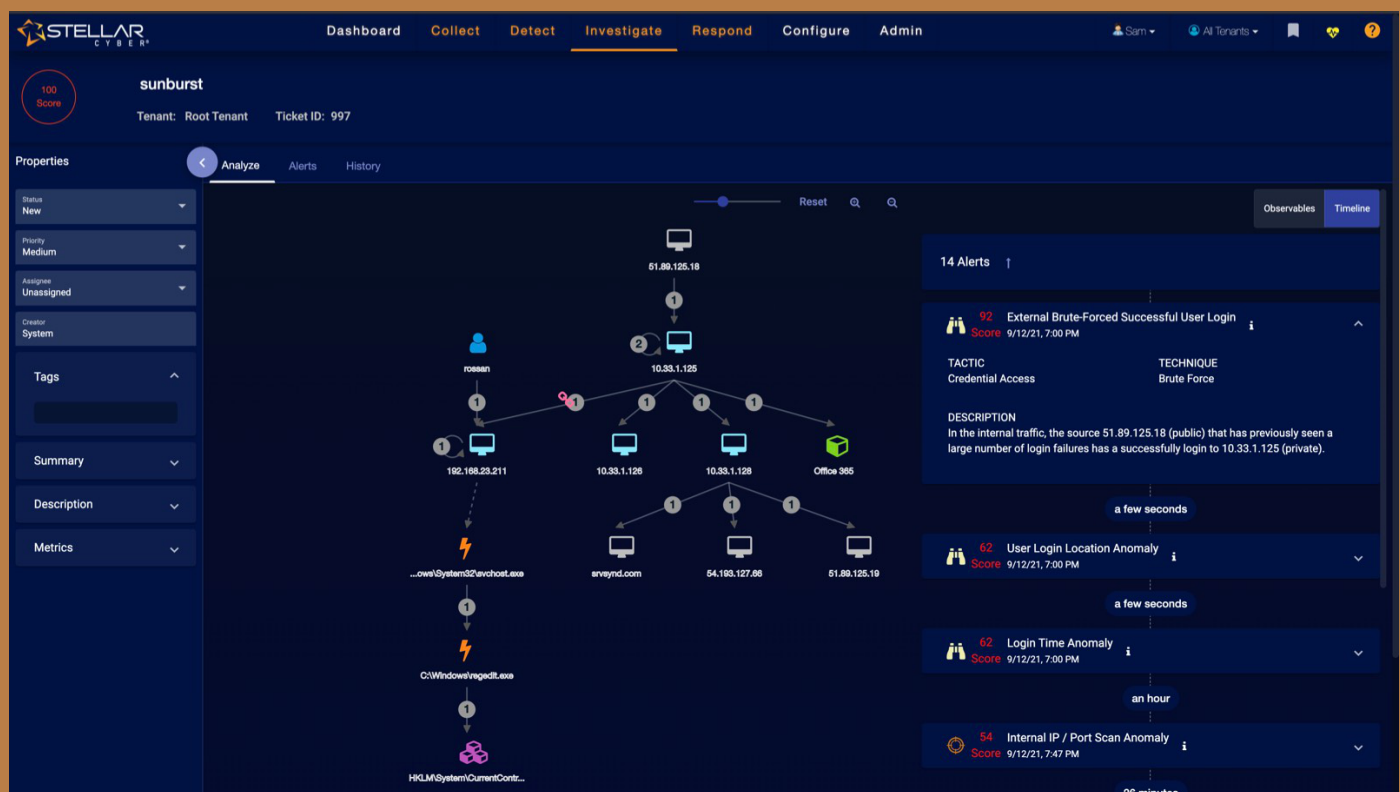


Figure 3 - Part of Stellar Cyber's incident correlation analysis offers a timeline of events. The timeline illustrates the threat that is propagating through your environment from initial attempt to the exfiltration stage

The former prioritize the use of the vendors' own tools, while the latter focus on integrations with third-party tools.

The Stellar Cyber Open XDR platform does provide some native, out of the box capabilities: network detection and response (NDR), a next-gen SIEM, and a threat intelligence platform that aggregates multiple threat intelligence feeds and distributes them to all deployments, whether on-premises or in the cloud, to enrich data for effective detection and response.

But, it is also designed with an open architecture to integrate with all common third-party security tools, to collect telemetry from and respond through them.

And then there are also physical and virtual

sensors that can be deployed and used to create visibility where it does not yet exist: container sensors, deception sensors, cloud connectors, log forwarders, and more.

“Open XDR is 'Everything Detection and Response', but critical to that strategy is that we don't do everything,” says Jones.

“We don't try to integrate with every IT tool, just the best-of-breed, security-focused tools. Our goal is to be the brains behind the whole operation – our platform focuses on the data, the AI that provides out of the box detections, and on delivering automatically correlated, context-based alerts that greatly speed up attack detection (8X improvement in MTTD) and response (20X improvement in MTTR).”

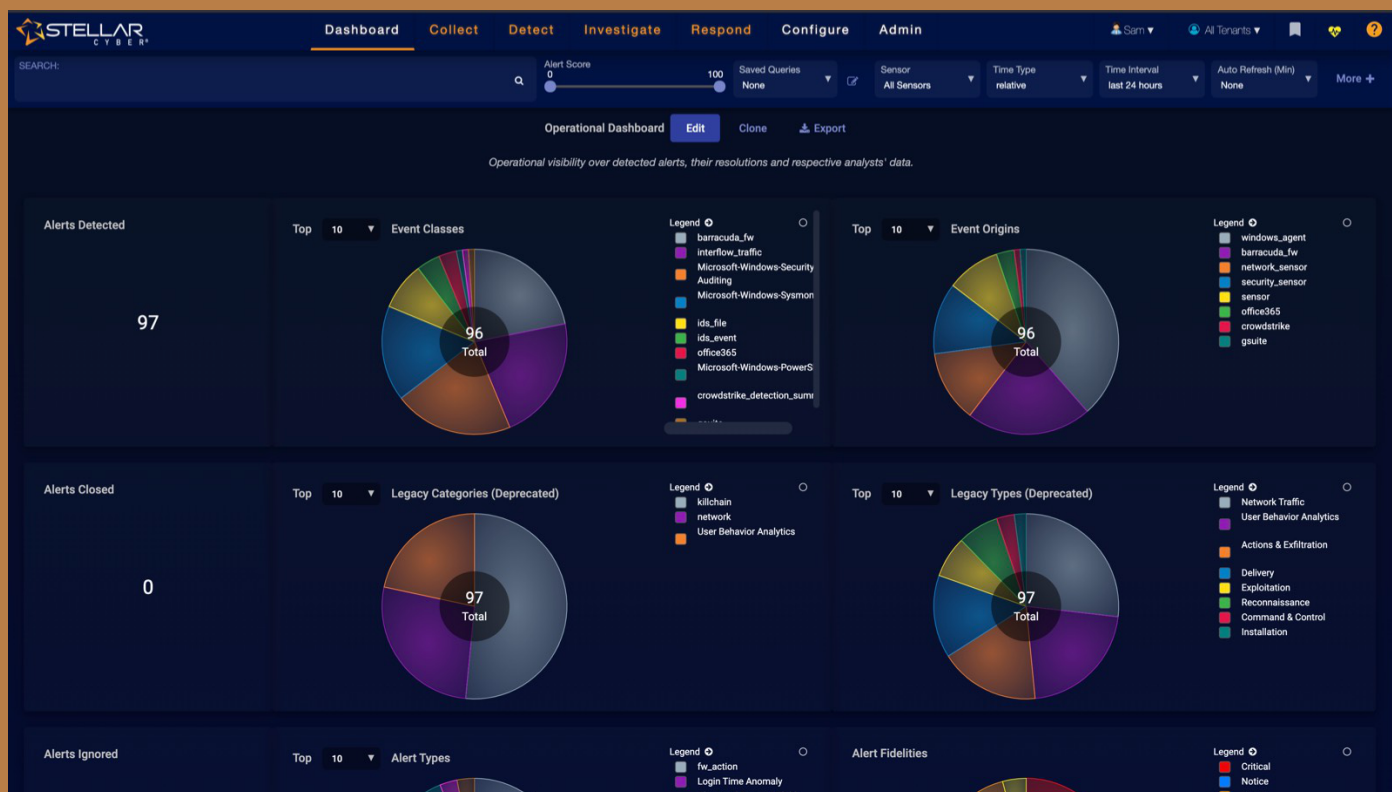


Figure 4 - Stellar Cyber Open XDR collects from everything in your attack surface. This dashboard shows all event classes, firewalls, network traffic, SaaS applications, user event data and event origins, including integrated tools like EDRs

That said, new tools can be easily added to the integration suite.

Jones says that one of the reasons Open XDR works so well is the data normalization process, on which their team of engineers concentrated from the very beginning.

“It's our number one engineering priority – always has been and always will be. The system needs to be purpose-built for data normalization, because otherwise a lot of the AI stuff doesn't work. We've invested a lot in researching tools, figuring out the right data model, and building infrastructure to make adding new tools easy.”

Who's it for?

The value proposition of Open XDR is easy to understand: SOC analysts can see all the data they need in the platform, and the AI does the heavy lifting so that they can focus on actual analysis and then respond directly through the platform (when the integrated tools allow).

They can investigate, make changes and take external mitigation actions (or automate them), create rules and playbooks (or simply import some from templates and modify them), review the output of AI, add context, hunt for threats, and more.

The hundreds of integrations with third-party security products are another great benefit of using Open XDR, as enterprises and MSSPs can continue to leverage existing investments.

“Stellar Cyber Open XDR is a great tool for organizations that are overworked and

understaffed but need to improve protection of their data and assets. It enables enterprise security teams for success despite budget constraints, as it maximizes the use of tools they've already invested in and provides many out of the box capabilities through one platform (and one license),” Jones says.

“It also enables MSSPs to offer more valued security services to SMBs, as it lowers the cost to own and operate the platform. In effect, it provides them with a fast, low-overhead path to getting into the Managed SecOps business.”

They can manage their various tenants straight from the same platform / instance because the data is logically separated. And, again, that's just one license they must pay for, which allows them to improve their profit margin and scale their business revenue.

Still, there may be cases where customers may require a separate installation, possibly even on-premises – and that, too, can be done.

“I'm happy to report that almost all of our customers stay with us because they're happy,” Jones says.

“I often interview customers: cybersecurity executives, SOC analysts, and MSSP directors of security that use Open XDR. The former tell me that they have been detecting things they previously weren't able to and protecting their organizations against high-profile attacks. The analysts are glad that they finally get to do real security work. The MSSP executives are delighted because they can provide a better service, while simultaneously making more money.”

Choosing to go the XDR route doesn't have to be a time-consuming and painful ordeal.

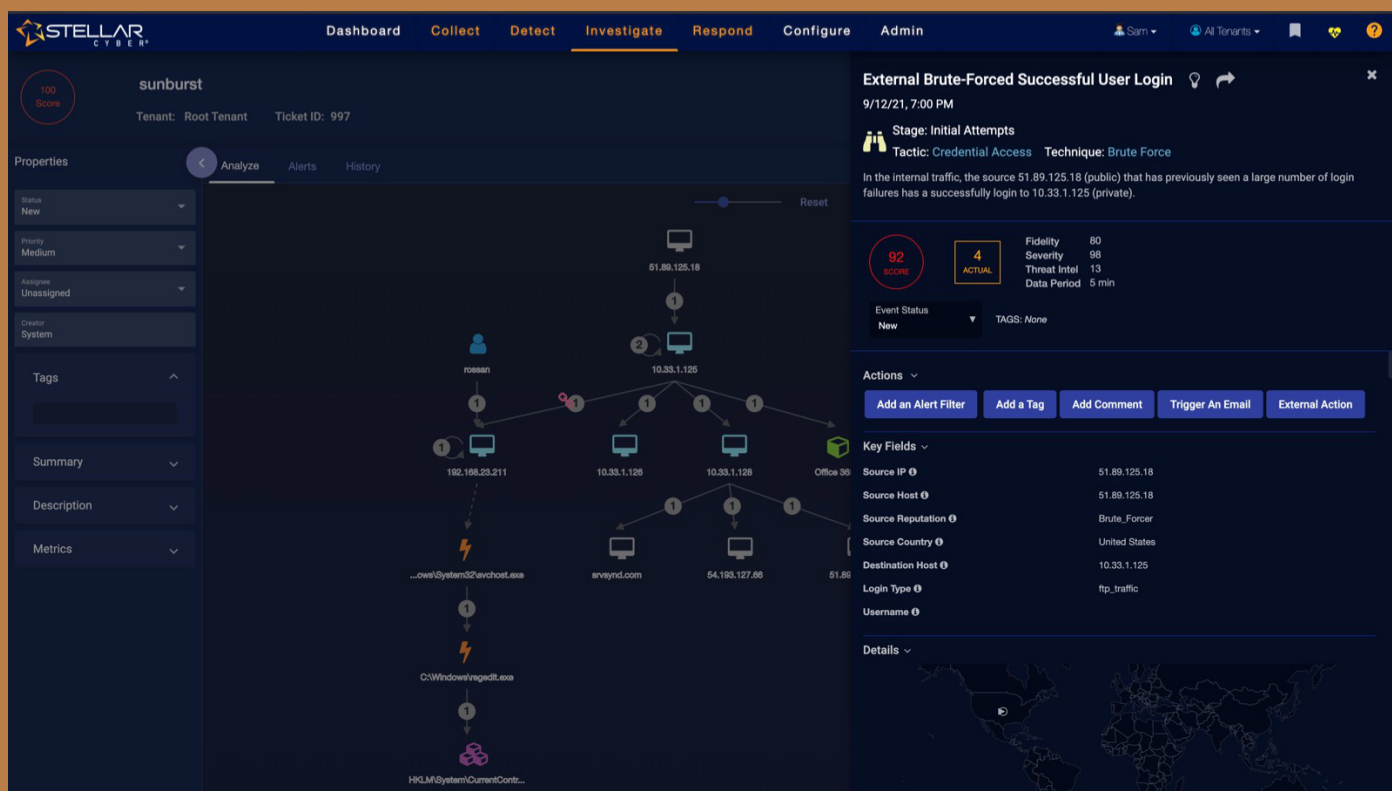


Figure 5 - Any Stellar Cyber alert can be validated easily by exposing the JSON metadata called Interflow. The user can then take an action such as disable the user or send a message to the firewall. Under the Response tab, the user can set up an automated playbook to trigger that response for future alerts that match this condition

Conclusion

Choosing to go the XDR route doesn't have to be a time-consuming and painful ordeal.

Setting up Open XDR is easy. Connections to new tools are made via APIs, from a dedicated tab of the platform's dashboard. Sensors can also be deployed, upgraded, and managed via the dashboard.

“Integral to our platform is that we're shipping out of the box with different alert

types for customers, and this is really just about making it easy to get your security program up and running without having to tune your SIEM or write different rules over the course of months or even a year,” Jones adds.

Still, as they say, seeing is believing. If you want to check whether Open XDR is the right tool for your organization and can make your analysts happier and more productive, a free 30-day trial option is available.



HOW DO I SELECT AN XDR SOLUTION?



SAM ADAMS,
VP OF DETECTION & RESPONSE,
RAPID7

In these early days of the XDR market, products may be high on promises, but light on delivery. To recognize the detection efficacy and response efficiency promised by XDR, I recommend the following tips:

What's in the box? Many vendors promising XDR outcomes are doing so based on an assumption that customers are willing and able to integrate (and pay for) many other technologies to access the complete telemetry set required to have extended environment visibility. Endpoint agents, network sensors, cloud hookups, user behavior, log ingestion are all critical pieces of the XDR puzzle, so it's important to understand what's included and what you may be expected to bring yourself. Too many integrations may start to negate the consolidation and efficiency benefits of XDR.

Understand the detection philosophy. One of the most anticipated outcomes of XDR for many teams is a promise to end noisy alerts and deliver the high-fidelity detections often recognized with EDR tools across the broader environment and data set. However, it's important to understand exactly how detections are curated and maintained. Detections based on static IOCs, for example, go stale very quickly. Understanding the methodology, threat intelligence, and diligence behind the detection library will offer insight into its efficacy and scalability. It's important to understand the philosophy and proof-of-concepts to experience detections firsthand, and look at any third-party analysis or reviews to learn more.

Don't forget the "R." Too many products often gloss over the "Response" element of XDR, assuming that with the right detections in place the right actions will follow suit. This is not the case. When a machine is breached, the last thing you want is an analyst running around trying to figure out what to do next. Good XDR requires a more prescriptive approach. This begins with high-context, well-correlated investigations. How do many disparate data sets converge into one cohesive picture of an event? With the right context in place, analysts must be primed for action. Well manicured playbooks, embedded expert guidance, and one-touch automation can help analysts at any level accelerate their response. This can be the difference between a breach and a non-event.



AUGUSTO BARROS,
VP OF SOLUTIONS,
SECURONIX



First thing to do is to make sure you will be able to operate and use the solution. Most XDR solutions have been presented as a simpler version of EDR plus SIEM and SOAR combos, but you still need people to operate and use it. You'll need someone to triage and respond to alerts, not to mention all the work around managing deployed agents. If you believe that'll be a problem, better look for an MDR provider instead.

If you can run an XDR solution, it's time to look at what you want it to cover. Coverage can be viewed in two dimensions: coverage of technology environments (endpoints, cloud apps, data centers) and threat coverage (ransomware, phishing, APTs, business fraud cases).

Most XDR solutions have a strong focus on traditional endpoints, such as Windows workstations. But if you need to cover cloud apps that your users can access from their own devices, including smartphones and tablets, these endpoint-oriented solutions may not be adequate. Instead, look for those capable of monitoring or ingesting telemetry directly from those cloud apps and cloud providers. If you need to protect business applications too, you are starting to move outside the XDR comfort zone; better look for SIEM and UEBA solutions capable of ingesting data from custom sources and work with custom detection use cases.

The threat coverage is similar. Most XDR solutions have a strong focus on the traditional “cybersecurity” threats, such as ransomware. Those are the threats that affect any organization connected to the internet. If those are the threats you need to detect and respond to, you are right on target for XDR solutions. But if you also need to cover business-oriented threats, such as fraud scenarios or insider threat cases, you need to look for more flexible XDR solutions, those where you can develop custom detection logic and ingest data from business applications too.

Finally, pay attention to your existing technology stack. Some vendors only offer closed XDR suites, so you may need to replace what you already have with the components that are part of that package. If you have security solutions you want to keep, or if you want more flexibility around the parts of your security architecture, better pick “Open” XDR solutions that allow you to connect to third-party solutions and leverage them to obtain telemetry and perform incident response actions.



BOGDAN CARLESCU,
DIRECTOR,
PRODUCT MANAGEMENT,
BITDEFENDER



With so many vendors and solutions in the market, choosing the right security solution for your business is not always an easy decision to make. The new XDR is no exception, most organizations are having difficulties in deciding which solution to choose or whether moving towards XDR makes sense for them at all.

In an April 2021 Forrester blog post, analyst Allie Mellen defined XDR as “the evolution of EDR, which optimizes threat detection, investigation, response, and hunting in real time. XDR unifies security-relevant endpoint detections with telemetry from security and business tools such as network analysis and visibility (NAV), email security, identity and access management, cloud security, and more.”

This definition offers important clues for organizations looking for the best suited XDR option. You should consider the following when shopping for XDR:

Make sure it's genuine.

Upgrading from EDR to XDR should provide (at least) two key benefits: enhanced threat detection and enhanced threat visibility. These are made possible by a new generation of event correlation engines coupled with the ability to collect incident data from endpoints and from additional sources like network, email or Active Directory. Make sure solutions you evaluate tick both boxes.

How significant is the upgrade effort?

Compared to EDR which is endpoint-exclusive, XDR is more complex. For reducing the implementation risk (important as XDR is still an emerging category) and a shorter time to value, look for the solutions that offer the flexibility to start small (for example with an endpoint-only component) and gradually enhance detection and visibility with additional telemetry. Implementing everything at once could be challenging.

Tight integration versus flexibility.

Depending on whether additional sources of telemetry are part of the same vendor portfolio or not, an XDR is classified as “Native” or “Hybrid”. Native XDR relies on the tight alignment of the vendor’s own portfolio and stronger integration between the elements providing telemetry. Hybrid XDR relies on integrations with third-party vendors to collect non-endpoint telemetry and execute response actions. The first is likely faster to purchase and to deploy while the latter offers the flexibility suited for mature security teams.

Overall value and effectiveness.

There are not many XDR focused industry reports and third-party evaluation tests yet. How can one evaluate the effectiveness of an XDR solution? As XDR is an evolution of EDR, industry analysts recommend considering the EDR solution from which it evolved as an “indicator of value” when evaluating XDR options.



JONATHAN COUCH,
SVP STRATEGY,
THREATQUOTIENT



A first step should be to think about goals – what do you want to achieve? How will you leverage this cross-communication between your devices to improve security operations efficiency and efficacy? If you can't prevent or respond to attacks more effectively with XDR, then you may need to go back and review other security processes first before moving in that direction.

As with most security technologies or capabilities, after knowing what you want to achieve, your next question should be "build or buy?" Organizations must look at their current technology stack and security monitoring capabilities. If you have the resources, the implementation and additional monitoring required to take advantage of XDR, then you're just looking for a technology solution. If you don't have the resources, then you should consider a managed capability. Many MDR (managed detection and response) companies are now offering XDR services: they will install and maintain various security infrastructure (perimeter, endpoint, proxies, DNS, etc.) and the ability to collect and communicate between all of them. You may lose some of the customization and control of doing it yourself, but it will most likely cost less and create less of a distraction for your team.

Once you determine whether you are going to build an XDR capability yourself or outsource it, you should review what "level" of XDR will help to achieve your goals. XDR can be as simple as connecting perimeter devices or your SIEM to an endpoint technology, or you can have a very expansive implementation to cover proxies, DNS, vulnerability management, identity management, and others. While it seems like you would want to connect as many technologies as possible together (and that may give you the greatest ability to take advantage of the integrations), it can be difficult to manage all those connection points and there should be reasoning behind "why" devices are talking to each other.

The overall goal that I feel organizations should be looking at with XDR is automation. If you can align integrations in your security stack with automated processes to save your security analysts time, then you will have achieved a very significant goal. Application of machine learning to identify new attacks or leveraging XDR to respond to complex attacks in your network is great, but that is also a much higher maturity level and will take some time to properly leverage within security operations.



AL HUGER,
SVP AND GM,
SECURITY PLATFORM &
RESPONSE,
CISCO



Security teams face an expanding threat landscape and an environment that is rife with friction – making security efficacy elusive. XDR promises to help security teams tackle the most pressing security operations challenges. However, before starting your XDR journey, below are 5 critical considerations.

Coordinated telemetry: True XDR must bridge data and telemetry from the widest security control categories, data repositories, and threat intelligence vendors to determine malicious intent probability. The goal must be a holistic network view, respective activities on it, and anything happening on devices that come and go. Once achieved, speed of analysis is key.

Leverage existing detection functionality: Each component in your security stack has unique detection elements – IoC detection, machine learning, behavioral analytics—becoming more powerful when brought together. Weak signals from silos become strong signals in aggregate. Detection working together is critical to XDR, so ensure the choice platform works with your whole stack.

Unify context for faster, more accurate responses: Unifying insights from multiple security control points provides a more accurate understanding of events, progression, and steps needed to remediate the threat. Unity isn't the point – there is no XDR without native response capabilities, preferably within just a click or two. Response actions like isolating a host, deleting a malicious email from all inboxes, or extracting observable data need to be readily available. Your XDR solution should have an easy way to create custom response actions.

Automation and orchestration to reduce human-powered tasks: You want an XDR that makes automating repetitive security tasks easy, without requiring a massive learning curve. Automating critical workflows frees teams across the full lifecycle, from discovering an alert to taking a response action quickly. Meaning, more time for critical tasks like threat hunting.

The power of a single investigative viewpoint: With telemetry unified from all detection and response elements, a single console is critical for direct remediation, access to threat intelligence, and tools to provide a unified view of an alert. With aggregated information, your security team will execute threat investigations at scale with greater efficiency, efficacy, reliability, and speed.

Start your XDR journey with these 5 critical elements to help guide your assessment while ensuring achievement of measurable outcomes and ROI.



SAMANTHA HUMPHRIES,
HEAD OF SECURITY
STRATEGY EMEA,
EXABEAM



Threat detection, investigation, and response (TDIR) is a core component of modern security programs, driving significant investment in tools to improve visibility, efficacy, and efficiency. However, security teams continue to struggle to detect and respond to threats as quickly as they would like or need.

On average, security teams have 19 TDIR solutions. Despite having impressive arsenals at their disposal, common threats like phishing and malware are regularly missed. Why? Security tools often operate in silos and lack visibility or context on what's happening in other tools. An open XDR solution, however, breaks down these silos enabling a complete view of the attack story to deliver detection, investigation, and response across all data sources.

When looking at all the tools used today for threat detection and response, more than half of IT professionals say modern SIEM software is one of their most valuable tools. Nevertheless, when it comes to selecting a solution it shouldn't be a question of either-or. SIEM and XDR are not exclusive.

While both SIEM and open XDR can share some use cases, their design philosophy and core capabilities make them different. SIEM technology anchors many SOCs and IT security teams today, and the intelligence of XDR not only can improve threat detection and response, but can also help modernize, integrate, and automate security operations processes.

IT security leaders should choose an XDR solution that complements and can be easily integrated into their security stack, alongside other solutions like SIEM and EDR, that doesn't force them to rip-and-replace existing tools to centralize on a single vendor. What's more, effective XDRs must include prescriptive, threat-centric workflows. XDR solutions should provide fast time to value and minimum configuration. Ultimately, SOCs should be able to use XDRs to address immediate concerns from start to finish.

While XDR has fast become a recognized approach, it's still a relatively new term in the industry causing a fair bit of confusion. If you ask 10 people to define XDR, you'll get 11 different answers. It can be disconcerting for CISOs responsible for providing threat detection, investigation and response in their organizations. In order to educate and spread awareness for XDR best practices, a number of thought-leading vendors in cybersecurity launched the XDR Alliance.

Its main mission is to foster an open approach to XDR that enables organizations everywhere to protect themselves against the growing number of cyberattacks, breaches, and intrusions. Through collaboration and prioritizing cooperation above competition, the industry can collectively win the battle against the adversaries.



SAM JONES,
VP,
PRODUCT MANAGEMENT,
STELLAR CYBER



There's a lot of interest in XDR / Open XDR these days, but there are also a lot of products on the market and a lot of claims being made about them. Here are five criteria you can apply to narrow your search:

Consider your existing security infrastructure: If your company is like most, you have probably collected a variety of different security tools over the years, such as SIEM, UEBA, EDR, and so on. Typically, you will want to integrate an XDR solution that causes the least disruption, requires the least data normalization, requires the least training time and is the most cost-effective.

Minimizing disruption: If you choose an Open XDR solution, you can preserve all or most of your existing tool investments. If you opt for a "native" XDR solution from a single vendor, you'll probably have to abandon your existing investments in third-party tools and replace them with solutions that are part of that vendor's XDR ecosystem.

Reducing data normalization: Look for an XDR solution that automatically normalizes other tools' data on ingestion. An XDR solution is supposed to pull data from all of your security tools, but different tools use different data formats. If your team has to manually convert tools' data formats to one your XDR solution can process, they'll spend a lot of time doing that instead of focusing on security incidents.

Minimizing training: What skill sets does your analyst team have, and how do they mesh with the XDR solution? You'll want to get your team up and running as quickly as possible, so you should opt for an XDR solution that has an intuitive interface and that uses an AI engine to handle grouping alerts into correlated incidents – that's the heavy lifting. Also, the XDR solution should have a strong response capability so you can build playbooks to automatically respond to conditions you set forth. These features will help you have peace of mind so your team can focus on complex exploits.

Minimizing costs: Your staffing costs will be lower if you can reduce training time and integration time. Look for an XDR solution that has existing APIs to other parts of your security infrastructure to minimize integration effort and is built for low- to mid-maturity analysts, so you can hire from a broader pool of analysts.



RAHUL KASHYAP,
VP/GM,
AWAKE SECURITY



Organizations looking to adopt XDR should consider what is motivating their journey. If the desire is to simply have a single vendor XDR solution, the benefit is the proverbial “one-stop shop.” However, this also means you have access to a single threat research team and average efficacy at best across the distinct aspects of XDR.

On the other hand, the appealing alternative to many sophisticated customers is the notion of an “XDR experience” or “open XDR.” In the latter case, customers would do well sourcing XDR components—SIEM, EDR, NDR, etc.—from vendors that are leaders in their respective categories.

The key benefit of this best-of-breed approach is that it delivers the threat discovery and response capabilities from a broader spectrum of the industry—a more diverse set of eyes and ears on the threat landscape. Moreover, customers adopting open XDR should ensure they evaluate whether the component platforms have deep workflow

integrations. This is what ultimately delivers on an important XDR promise: enabling SOC teams to move seamlessly between the various tools thereby improving time to remediation and reducing human error.

Another out-of-the-box integration to look for is the ability to take investigative, containment and remediation actions in one tool that automatically reflect in the others; for example, pulling endpoint telemetry into the NDR tool or enabling one-click device quarantine from the SIEM or NDR using an EDR agent.

There are a few additional aspects customers should consider as they evaluate XDR:

- First, ensure that the XDR solution provides coverage across all infrastructure components, from the traditional campus and data center to IoT and OT networks and cloud-based workloads and applications.
- Second, validate that the XDR strategy minimizes visibility blind spots, and that the components complement each other for a comprehensive assessment of the organization’s attack surface.
- Finally, consider how the information from the XDR solution will be consumed. This final mile of an XDR solution can determine the success or failure of the effort.

Some of the key questions to ask include:

- How will threat hunting, digital forensics and incident response responsibilities evolve in a post-XDR world?
- Does the vendor(s) offer an MDR solution over and above the technology offering?
- Will such an MDR solution work well with existing SOC personnel, whether internal or an incumbent-MSSP?
- How will these service providers work together to deliver timely and concrete actions for the organization in order to minimize risk and reduce impact?



MORTEN KJAERGAARD,
CEO,
HEIMDAL SECURITY



XDR is a mandatory choice if you're interested in ensuring top security for your company, whether you outsource it or opt for something developed internally. The most important aspect is not to go through thousands of alerts from multiple solutions manually but use a unified state-of-the-art system, with all the necessary technologies in one place.

It's much easier and affordable to opt for an XDR solution that can provide unified detection, analysis, response and remediation in real-time, offering an enhanced (and simplified) overview of your company's cybersecurity state.

How do you select the perfect XDR solution for your business? From my experience, you must consider the efficiency of the key elements that any good XDR software on the market must have – Extended Detection, Extended Analysis, and Extended Response.

- For the Extended Detection part, XDR must be able to gather information from across the

company, correlate it, and analyze it in order to condense a large amount of raw data into a smaller number of precise details regarding probable occurrences. The solution must include a substantial number of attack vectors to allow you to discover more active threats.

- Obviously, XDR wouldn't be so efficient without Extended Analysis. Every incident should be (automatically!, through artificial intelligence augmentation) investigated, and the solution must provide accurate answers to questions like: Is this a real threat? Is it a false positive? Can this be part of a more complex threat?
- The next step is the Extended Response where, with all the details and information collected from Detection and Analysis, XDR solutions must be able to come up with an efficient, swift and coordinated response that perfectly fits the attack's scope. A particularly important aspect here is that the response provided by the XDR solution must help close those gaps that allowed the threat to reach the network in the first place, thus acting as a valuable prevention catalyst.

I strongly recommend looking for a solution that offers Detection, Analysis and Response in one platform, of course, not separately.

Other major-league aspects that can foster the decision to acquire a certain XDR solution from the multitude of options available today on the cybersecurity market are:

- The ability to gather and compare information across different sources – endpoints, networks, emails, cloud workloads.
- A consolidated, cohesive approach that provides superb visibility and real-time alerting on phone or email in case of an infection or attack.
- Excellent threat intelligence and advanced machine learning capabilities, allowing the solution to become more effective over time, with an admirable ROI.



ED MARTIN,
PRODUCT MANAGEMENT
DIRECTOR,
SECUREWORKS



The immense volume of data involved in the multitude of security solutions available to SecOps teams today has put intense pressure on budgets and affected decision-making. XDR, and its cloud-native approach, is proving to alleviate those budget issues while improving visibility and connectivity across endpoint, network and cloud data. So where should a team start? Here are four key considerations when investing in XDR:

Find an invested partner

First, look for a security partner who can demonstrate and validate investment in the XDR platform as part of their overall corporate and product development strategy. There is a high-level of technical and security competency required for extensive data lakes and highly curated threat intelligence. Seek out an established security provider with a strong track record of service availability and scalable systems.

Seek out services

The ability to upskill your team as security needs change may be tied to volatile investments, and budget changes can drastically impact your team's ability to scale quickly. The XDR platform provider you invest in should offer a collection of services that can plug and play into security programs – either directly, or through highly trained partners.

Keep a close eye on capabilities

Be sure the service wrappers offered by your XDR provider include a full range of capabilities including: tier one (reactive workflows), tier two (proactive threat hunting), and Incident Response, and they should have strong availability for your needs around the clock. Decision makers should seek out high-quality service options that include multiple methods of communication such as in-context chat, serviced by actual security practitioners to meet your needs at all times.

Transparent and simple pricing

Many SIEM-based and data centre-based XDR solutions use volume consumption pricing that can discourage SecOps teams from sending more data. According to Enterprise Strategy Group (ESG), 30% of IT/Cybersecurity professionals across multiple industries surveyed feel that these tools are not as effective at identifying unknown threats. Limiting data can result in missing important data when you need it. Work with a partner that keeps pricing transparent, simple, and straightforward.

And an extra tip: be sure your data retention is properly aligned with your organization's risk profile. At least one year of threat data retention is recommended, to deal with the aforementioned issues and it will also allow leaders to make more data-informed budget decisions in the future.



SARYU NAYYAR,
CEO,
GURUCUL



XDR begins with endpoint security, in that it does detection and threat response at the outer edges of the network. However, modern XDRs also incorporate data from other sources, perform correlation and generate analytics, and produce some level of automated threat response. An XDR is a complex tool that should integrate within the overall computing environment to meet threat analysis and response requirements.

A cloud-native solution is rapidly becoming essential, as it scales well and can provide coverage in real time across a wide range of geographic regions and devices. A cloud XDR lets you produce real time responses no matter what the level of data that is being collected. And because we don't have to provision new servers when traffic grows, we can rapidly adapt to changing circumstances.

To select an XDR, you want a detailed analysis of your network to determine your endpoints, what other data you can pull in for correlation and analytics, and what level of automated response that you're looking for. Further, as we talk about real time analytics and response, we need to define what you mean by real time. By understanding the types of threats that you face, you can better understand how much time you can spend in analysis and response.

As a part of the XDR evaluation, organizations also have to look at the types and amounts of data they are collecting through existing cybersecurity tools. If your prospective XDR can ingest data from a variety of point solutions and correlate that data to determine the true risk of threats, you will have high-fidelity alerts and far less noise.

So you may need much more information on your network environment, existing data collection efforts, your threats, and your possible responses in order to fully understand what an XDR can do for your cybersecurity efforts. Rather than going with the lowest cost solution, or the simplest alternative, you have to make an informed decision based on how the strengths and limitations of solutions mesh with your network and your requirements.

That's not a short or easy process. Be prepared to expend some time and effort into fully understanding what you need and what the alternatives offer. But you will ultimately be rewarded with a solution that does what you need it to do, and when you need it.



NAVEEN PALAVALLI,
VP OF PRODUCTS,
MCAFEE



A first step in assessing which XDR vendor is a right fit for your organization is to have a complete picture of your security needs, gaps and architecture. This means understanding how their application solution is delivered and how it will integrate with your security architecture.

There are two XDR vendor camps to consider: one is an open-XDR approach, which includes best-of-breed solutions allowing you to determine the depth at which integrations are required; the second camp is solely proprietary, whereby an organization may need to rip and replace existing security solutions in place of a single vendors' offering/solution.

Both camps call for the same baseline requirements:

1. Centralization of normalized data/harmonizing security controls and data across all vectors.
2. Correlation of security data and alerts into incidents or having actionable intelligence.

3. Centralized incident response capabilities or simply embracing the dance between security and IT.

XDR provides a single console for multiple security products (and services) that comprise a unified platform. An XDR approach to your SecOps program will shift processes and likely merge and encourage tighter coordination between different functions like SOC analysts, hunters, incident responders and IT administrators. For example, traditional EDR analysts can now do threat hunting beyond the endpoint, such as cloud apps and email.

The ideal XDR solution must provide enhanced detection and response capabilities across endpoints, networks, and cloud infrastructures. It needs to prioritize and predict threats that matter BEFORE the attack and prescribe necessary countermeasures allowing the organization to proactively harden their environment.

In summation, no matter what the selling point is for "XDR," there remains a few constants—security practitioners, specifically incident responders, need reliable threat sensors, intelligence, and telemetry sources to enhance their security program and security posture. So here are the keys your CISO needs when selecting the right XDR vendor for your organization:

- CISO teams should assess what are the current gaps in their SOC solutions (if they have one). A recent ESG survey found that the number one gap is cloud visibility.
- CISO teams should assess whether they want a build-your-own XDR platform that integrates with their current investments or do they want a pre-integrated solution. This is the Open Vs Native track.
- They should assess whether they want to operate it themselves (depending on skills, resources, maturity) or if they want to consume XDR as a service.

The goal is to empower the SOC to do more with unified visibility and control across endpoints, network, and cloud. For most organizations, XDR will be a journey, not a destination.



BEN SMITH,
FIELD CTO,
NETWITNESS



Above all, don't be distracted by the “small rocks” of bells and whistles pointing to specific features. Keep these two “big rocks” in mind when selecting an XDR solution:

Decide what kind of visibility you require into your environment. If you're considering an XDR solution, you've already figured out that your classic SIEM alone isn't going to provide you with the real-time visibility you need today. How does a solution give you the highest-fidelity look into your environment? Look for multiple methods for collecting data, above and beyond collecting logs – for example, collecting network traffic, endpoint data, and IoT data. Don't be put off by “too many” ingestion methods; even if you don't need everything today, you will probably need it tomorrow. Find a solution with a track record of past innovation, and room for future growth. And double-check to validate that all these capabilities are natively included in the XDR solution, and not bundled from some third party. Bundles almost always mean your XDR provider may not be in a position to influence that third party's development plans.

Where that visibility is required is also important. Do you need that visibility into your on-premise environment only? Are virtual, cloud or IoT environments in the mix here as well? And what about where the XDR solution is actually running – in the cloud, on-premise, or some combination of these two? Look for solution providers who can clearly supply the answers to these “what to ingest” and “where to ingest” questions.

Keep the needs, and the natural limitations, of your analyst team front and center at all times. If your XDR provider brings the world's best technology to the table, but creates too much friction when your SOC team is trying to do its job, you have wasted your money. Look for an XDR provider who can demonstrate they have built an interface, and accompanying workflows, which respects the reality that your SOC is staffed by human beings. Human beings, especially under the bright and harsh glare of a currently-underway incident, are prone to making mistakes.

Your XDR solution should orchestrate and automate the remediation path for your SOC team. Instead of an analyst having to remember the dozen steps needed to work a phishing incident, provide those steps in a runbook where each step is defined, timed, and escalated as needed automatically.



JIM WAGGONER,
VP,
PRODUCT MANAGEMENT,
FIREEYE



To select the right security solution for your business you should follow the same steps used for all security purchases. First, complete a risk assessment to determine if you deployed security controls and operations are accomplishing the task at hand. If attacks are getting through your defenses, then upgrades in security may be at risk or be used to identify those gaps.

If your primary weakness is from email, then upgrade your messaging solutions or enhance them with additional email security that will identify, and block messages not captured by your existing solution.

If your business is reliant on cloud services, ensure that you have a cloud security solution that helps you identify unexpected web services, identifies, and corrects misconfigured policies and accounts, and provides protection against key theft.

Inventory your endpoint security solution to ensure that you are protected against ransomware and have the tools that will guide you to discover threats that have made it through all your defenses and give you the tools to restore your systems to a state of good health.

After the assessment is done for the deployed security, do an inspection of the team who shoulders the responsibility for identifying threats, updating controls, and keeping the business running.

If they are spending their time on tactical responses, look to offset the manual work by leveraging automation of threat response using orchestration across the entire system of events, alerts. Give them the tools to filter through the influx of data using workflows that guide their activities like investigations and data manipulation.

Ensure that the solution enables them to get a holistic view of the security landscape within your environment and is balanced with enough insight from outside your business to provide context of attacks that are specifically targeted to your business.

And finally, don't feel the need to have to upgrade all at once. Your XDR solution should grow as you grow. Starting at whatever point will give you the best outcome. If you need an overlay on top of your existing solutions, then choose a Security Operations console that has intelligence and orchestration built in and brings the telemetry together with reduced complexity. If you want tighter integration between protection and workflows look for a solution that natively integrates and works together to adapt to the attack surface.

The background of the page is an abstract architectural photograph. It features a series of curved, overlapping structural elements, possibly part of a modern building's facade or interior. The colors are primarily dark grey and black, with a prominent horizontal band of orange-brown in the center. The text 'COMPANY DIRECTORY' is written in white, bold, sans-serif capital letters across this orange band. Below the band, there is a decorative horizontal line composed of many thin, parallel, slightly wavy lines in shades of orange and grey. The bottom right corner of the page shows a dense, curved pattern of white lines on a dark background, resembling a modern architectural detail or a close-up of a building's structure.

COMPANY DIRECTORY

AWAKE

SANTA CLARA, CA, USA

www.awakesecurity.com

Awake Security, an NDR security division of Arista, is an advanced network detection and response company. By combining artificial intelligence with human expertise, Awake models and hunts for both insider and external attacker behaviors, while providing autonomous triage and response with full forensics across traditional, IoT and cloud networks. The platform performs deep data parsing including encrypted traffic analysis.

Bitdefender delivers threat prevention, detection, and response worldwide. With investments in research and development, Bitdefender Labs discovers 400 new threats each minute and validates 30 billion threat queries daily. The company has developed innovations in antimalware software, IoT security, behavioral analytics, and artificial intelligence and its technology is licensed by more than 150 technology brands.

Bitdefender®

BUCHAREST, ROMANIA, EU

www.bitdefender.com



Check Point®
SOFTWARE TECHNOLOGIES LTD

SAN CARLOS, CA, USA

www.checkpoint.com

Check Point is a provider of cybersecurity solutions to governments and corporate enterprises globally. Its solutions protect customers from 5th generation cyber-attacks with a high catch rate of malware, ransomware and other types of attacks. The company offers multilevel security architecture which defends enterprises' cloud, network and mobile device held information. It provides one point of control security management system and protects over 100,000 organizations of all sizes.



www.cisco.com

Cisco is a computer networking company whose hardware, software, and service offerings are used to create the internet solutions that make networks possible. Its engineers have led the development of IP-based networking technologies. This tradition of innovation continues with products and solutions in the company's core development areas of routing and switching, as well as in advanced technologies such as home networking, IP telephony, optical networking, security, storage area networking, and wireless technology.

Confluera is a computer and network security startup and provider of cloud cybersecurity detection and response. It offers real-time sequencing of various attack steps found in modern cyberattacks. Its patented machine learning technology automates the tedious and error-prone task of correlating events, removes the complexity of manual analysis of multiple systems, and provides a high degree of detection accuracy.



PALO ALTO, CA, USA

www.confluera.com



www.crowdstrike.com

CrowdStrike is a cybersecurity company that provides cloud-delivered endpoint protection. It offers unified antivirus, endpoint detection and response, and a 24/7 managed hunting service—all delivered via a single agent. It leverages artificial intelligence and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network.



cybereason

BOSTON, MA, USA

www.cybereason.com

Cybereason provides attack protection that unifies security from the endpoint, to the enterprise, to everywhere the battle moves. The Cybereason Defense Platform combines detection and response (EDR and XDR), next-gen anti-virus (NGAV), and proactive threat hunting to deliver context-rich analysis of every element of a Malop (malicious operation).

Cynet offers threat detection and response. It simplifies security by providing a platform for detection, prevention and automated response to threats with near-zero false positives, shortening the time from detection to resolution and limiting damage to an organization. It provides findings with associated risks without a lot of complexity and noise, so security teams can prioritize and respond to what matters.



BOSTON, MA, USA

www.cynet.com

eSENTIRE

WATERLOO, ON, USA

www.esentire.com

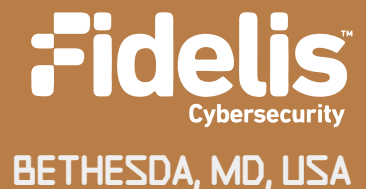
eSentire provides managed detection and response, protecting the critical data and applications of 1,000+ organizations in 70+ countries from known and unknown cyber threats. The company's mission is to hunt, investigate and stop cyber threats before they disrupt businesses. It combines machine learning XDR technology, 24/7 threat hunting, and proven security operations, to mitigate business risk, and enable security at scale.



www.exabeam.com

Exabeam enables security teams to use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. The Exabeam Security Operations Platform is a cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users and malicious adversaries, and minimize false positives.

Fidelis Cybersecurity provides cyber defense solutions, safeguards modern IT environments with detection, deception, response, cloud security, and compliance capabilities. It offers full visibility across hybrid environments via dynamic cyber terrain mapping and multi-faceted context and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle.



www.fidelissecurity.com



www.fortinet.com

Fortinet secures enterprise, service provider, and government organizations around the world. It provides customers with protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. It addresses the most critical security challenges, whether in networked, application, cloud, or mobile environments.



GURUCUL

EL SEGUNDO, CA, USA

Gurukul helps organizations protect their assets from insider threats and external cyberattacks, both on-premises and in the cloud. Its Unified Security and Risk Analytics technology delivers a platform for all cyber risks: security, identity and fraud. It leverages machine learning behavior profiling with predictive risk-scoring algorithms to predict, detect and prevent data breaches, fraud and insider threats. It also reduces the attack surface for accounts and eliminates unnecessary access rights and privileges to increase data protection.

www.gurukul.com

Heimdal Security focuses on continuous technological innovation. With the realization that cybersecurity has become a more and more complicated burden for companies, especially as they become larger, Heimdal solutions aim to block cyber threats before they compromise the system, strengthen security by closing security holes abused in cyberattacks, and protect financial data and resources from cyber criminal.



HEIMDAL

SECURITY

BUCHAREST, ROMANIA, EU

www.heimdalsecurity.com

Hunters.

TEL AVIV, ISRAEL

Hunters is a cybersecurity company that combines data engineering, security expertise and layers of automation to expedite decision making, helping security teams become attack-ready. The company infuses how attackers think and act into a platform that helps security operations see and stop attacks at their root. It enables companies to collect and automatically correlate data from multiple security and IT sources, unifying them into single threat detection, investigation, and response platform.

www.hunters.ai

KOGNOS

SANTA CLARA, CA, USA

www.kognos.io

Kognos is an autonomous XDR investigator platform that detects, investigates, and responds to attack campaigns. Founded on the principle that attacker behavior is indicative of attack methodology, attribution, and data for exfiltration, the company leverages the power of relationships using security aware AI to reduce dwell time by tracing the attacker's path in real-time.

LMNTRIX offers integrated, multi-dimensional threat detection / response architecture that hunts down and eliminates the advanced and unknown threats that routinely bypass perimeter controls. The company offers an integrated and multi-vector approach to cybersecurity which uses a combination of advanced network and endpoint threat detection, deceptions, analytics, and threat intelligence, all of which is complemented with proactive threat hunting and response.

LMNTRIX

ORANGE, CA, USA

www.lmntrix.com

MANDIANT[®]

MILPITAS, CA, USA

www.mandiant.com

Mandiant is a cybersecurity company that delivers a portfolio of solutions that help customers continuously validate that their people, processes, and technology will protect the organization from cyber threats. The company does this by combining threat intelligence and front-line incident response data with continuous security validation to deliver solutions that increase security effectiveness and reduce business risk.



SANTA CLARA, CA, USA

www.mcafee.com

McAfee delivers an all-in-one security, identity protection, and privacy service that helps keep people safe-across activities, devices, and locations through a personalized, intelligent, and inclusive approach. It secures home PCs, tablets, phones, and connected devices with easy-to-use, practical solutions. Its products also protect small businesses against a wide array of threats, including malware, spam, unauthorized network access, and threats in the cloud.

Microsoft is a multinational technology corporation which produces computer software, consumer electronics, personal computers, and related services. Its best known software products are the Microsoft Windows line of operating systems, the Microsoft Office suite, and the Internet Explorer and Edge web browsers. Its hardware products are the Xbox video game consoles and the Microsoft Surface lineup of touchscreen personal computers.



Microsoft

REDMOND, WA, USA

www.microsoft.com

Netsurion®

Powering Secure and Agile Networks

FORT LAUDERDALE, FL, USA

www.netsurion.com

Netsurion is a managed security service provider that converges network management, threat protection, and compliance readiness for SMBs and service providers. Its managed platform approach to combining purpose-built technology and a team of cybersecurity experts gives customers and partners the flexibility to adapt and grow while maintaining a secure environment.



NETWITNESS

BEDFORD, MA, USA

www.netwitness.com

NetWitness, an RSA Business, provides comprehensive and scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This enables security analysts to be more efficient and stay ahead of business-impacting threats.

Palo Alto Networks helps address security challenges with continuous innovation that leverages the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and assisting a growing ecosystem of partners, it protects many organizations across clouds, networks, and mobile devices.



SANTA CLARA, CA, USA

www.paloaltonetworks.com

RAPID7

BOSTON, MA, USA

www.rapid7.com

Rapid7 offers security data and analytics solutions. The visibility, analytics, and automation delivered through their Insight cloud simplifies the complex and helps security teams reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks.



MELBOURNE, VICTORIA, AUSTRALIA

www.redpiranha.net

Red Piranha is a cybersecurity products and services company with a global presence servicing large and small clients and partners across multiple industry sectors. The company allows organizations to lower the risk of a security incident, reduce time to detect and respond to a threat and minimize the cost of securing their business. The company also offers a suite of security consulting services to help customers get secure and achieve compliance.

ReliaQuest is a cybersecurity company that delivers visibility and automation on demand across complex environments with a platform purpose-built to protect organizations from security breaches. Its cloud-native SaaS solution integrates and improves an enterprise's on premise and multi-cloud technologies. By increasing visibility through the platform's proprietary universal translator and use of automation and artificial intelligence, the platform enables automatic and continuous threat detection, threat hunting, and remediation.

RELIAQUEST 
TAMPA, FL, USA

www.reliaquest.com

Secureworks®

ATLANTA, GA, USA

www.secureworks.com

Secureworks enables customers and partners to outpace and outmaneuver adversaries, so they can adapt and respond to market forces to meet their business needs. With a combination of cloud-native, SaaS security platform and intelligence-driven security solutions, it improves client's ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.



ADDISON, TX, USA

www.securonix.com

Securonix is a cybersecurity company that delivers a security analytics and operations management platform for the modern era of big data and advanced cyber threats. It helps customers address their insider threat, cyber threat, cloud security, and application security monitoring requirements. It delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NTA, and vertical-specific applications as a SaaS solution with unlimited scalability and no infrastructure cost.

SentinelOne delivers autonomous security for the endpoint, datacenter and cloud environments to help organizations secure their assets. It unifies prevention, detection, response, remediation and forensics in a single platform powered by artificial intelligence. Organizations can detect malicious behavior across multiple vectors, eliminate threats with fully-automated integrated response and adapt their defenses against the most advanced cyberattacks.



www.sentinelone.com

SOPHOS

ABINGDON, UK

www.sophos.com

Powered by threat intelligence, AI and machine learning, Sophos delivers a broad portfolio of products and services to secure users, networks and endpoints against ransomware, malware, exploits, phishing and the wide range of other cyberattacks. It provides a single integrated cloud-based management console, Sophos Central – the centerpiece of an adaptive cybersecurity ecosystem that features a centralized data lake that leverages a set of open APIs available to customers, partners, developers, and other cybersecurity vendors.



SANTA CLARA, CA, USA

Stellar Cyber is a security operations platform that provides threat detection and response across the entire attack surface. It is an investigation and automated response platform, delivering a 360-degree view of your entire attack surface with readily-available detections delivered through pre-built, tightly-integrated capabilities including NDR, CDR, NG SIEM, UEBA, and Automated Threat Hunting. It helps eliminate the data overload and tool fatigue often cited by security analysts while reducing operational costs.

www.stellarcyber.ai

ThreatQuotient aims to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, it accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, its solutions reduce noise and highlight top priority threats to provide focus and decision support for limited resources.



www.threatq.com



BOSTON, MA, USA

Threat Stack is a cybersecurity company that offers cloud security and compliance for infrastructure and applications, helping companies securely leverage the business benefits of the cloud with risk identification and real-time threat detection across cloud workloads. With its platform it delivers full stack security observability across the cloud management console, host, container, orchestration, managed containers, and serverless layers.

www.threatstack.com

TierPoint is a data center service provider of cloud, colocation, managed services and DR. With 40 data centers in 20 U.S. markets and local service, coast to coast, its carrier-class, carrier-neutral facilities provide uninterrupted access to host clients' critical services. Each facility has been SSAE 16 audited and provides customized solutions.



ST. LOUIS, MO, USA

www.tierpoint.com



SHIBUYA CITY, TOKYO, JAPAN

www.trendmicro.com

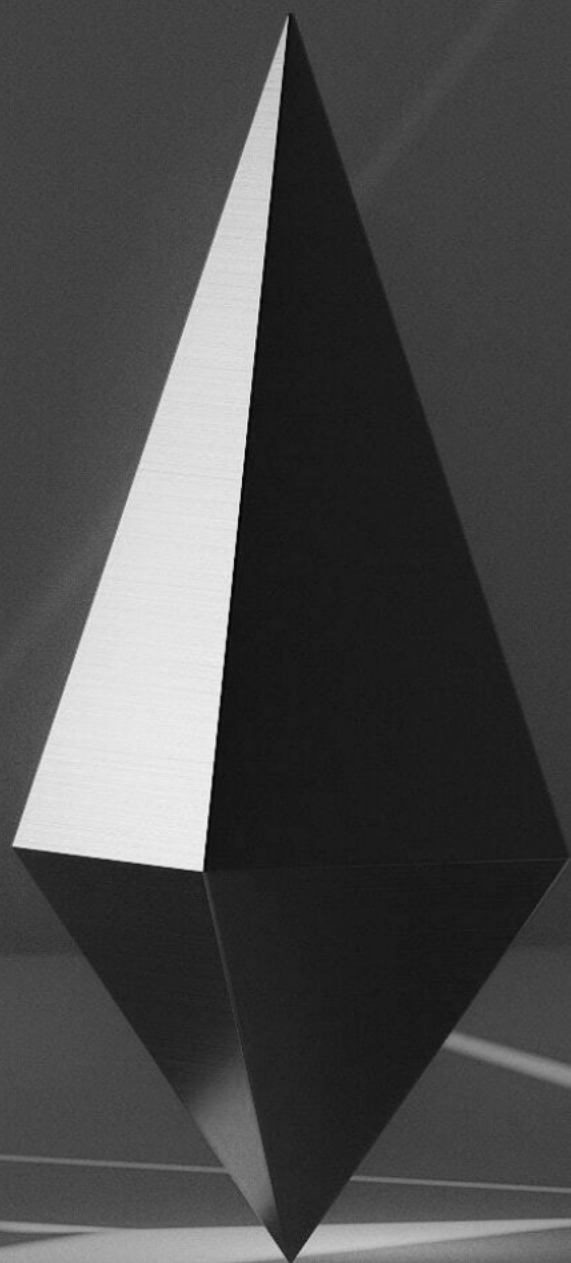
Trend Micro is a cybersecurity company which enables resilience for businesses, governments, and consumers. Its connected solutions are optimized for cloud workloads, endpoints, email, IIoT, and networks and deliver central visibility across the enterprise, enabling to promptly detect and respond to threats.

VMware is a cybersecurity company which offers a variety of digital solutions that powers apps, services and experiences which enable organizations to optimize their customer service and motivate employees. The company's software spans app modernization, cloud, networking and security and digital workspace. The company leverages technologies such as edge computing, artificial intelligence, blockchain, machine learning, Kubernetes and more.



PALO ALTO, CA, USA

www.vmware.com



XDR REPORT

 **HELPNETSECURITY**