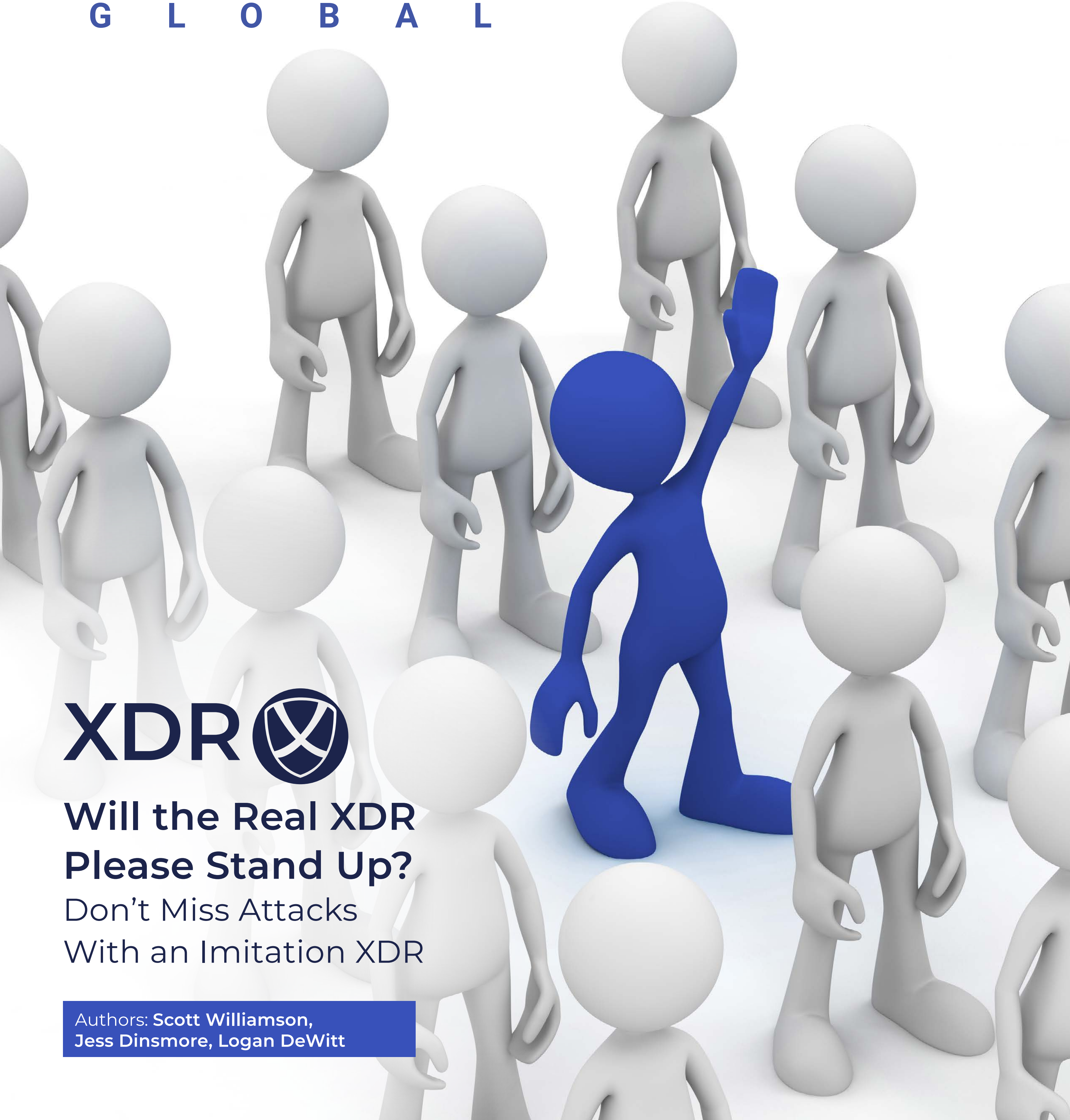
A **CISO GLOBAL** WHITE PAPER



XDR

Will the Real XDR Please Stand Up?

Don't Miss Attacks With an Imitation XDR

Authors: **Scott Williamson, Jess Dinsmore, Logan DeWitt**

Table of Contents

Key Takeaways

- Though they usually have tools, in-house IT security teams struggle to sort through the overwhelming amount of security data being generated in disparate systems. So, they are unable to build an accurate and comprehensive picture, and often miss the key warning signals that attack is under way, until it is too late to stop it. This minimizes ROI on major tool investments.
- Extended Detection and Response (XDR) is an advanced approach to corporate IT security. Which maximizes historical security spending by adding AI, ML and automation to help existing tools spot even the stealthiest of attacks earlier, all with expert, certified security analysts' oversight.
- The term XDR is being used to market a wide variety of solutions, some of which do not include essential features like broad telemetry, behavioral analysis, and customized, automated playbooks. Organizations should carefully assess and compare what is included in each solution.

The Digital Haystack

The battle against cybercriminals has ebbed and flowed over the years. Bad actors develop new attack types and strategies, and the IT security community responds with more effective solutions.

Cyberattacks **evolve** and attackers find **new ways** to circumvent **defenses**

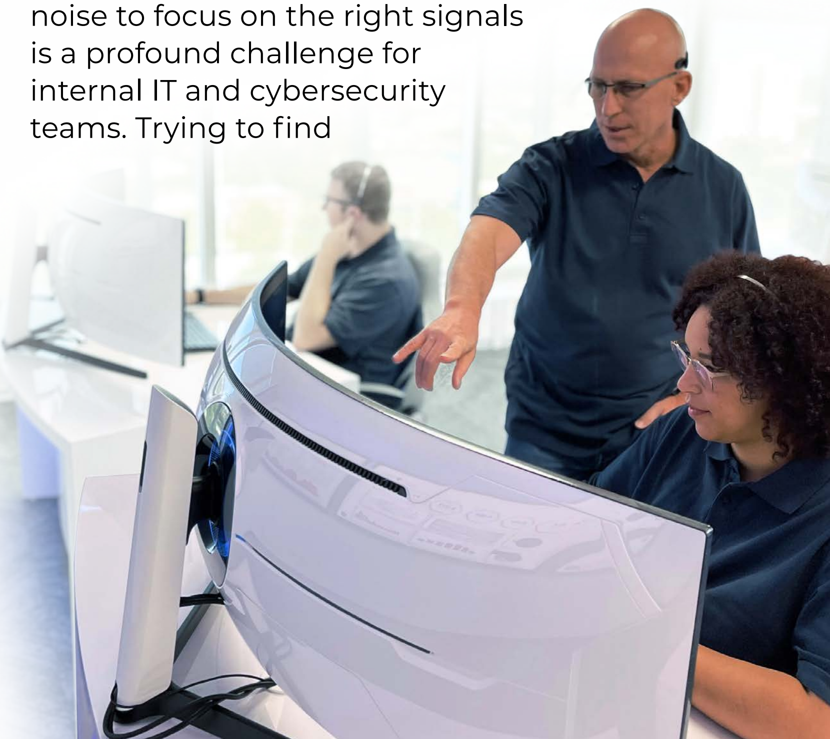
It's a virtual arms race which shows no sign of slowing down, and affects the entire organization. Financial experts agree that cybersecurity risk is a top concern for 2022, with reduced coverage or loss of cyber insurance looming for many, and costly business threats picking up speed, including ransomware, downtime, remediation costs, brand damage and regulatory penalties.

At the same time, C-suites are wrestling the challenges of poor ROI on SIEM solutions, inadequate security program improvement metrics, and extreme difficulty in hiring and retaining sufficient security talent to address such issues.

It could be said that security teams are the victims of their toolsets' success, with security alerts now being generated by firewalls, Software as a Service (SaaS) platforms such as Microsoft 365, Platform as a Service (PaaS) offerings like Amazon AWS and Google Cloud, as well as traditional endpoints to including laptops, workstations, and servers.

In one sense this is a good thing. As cyberattacks evolve and attackers find new ways to circumvent defenses, real-time monitoring of all platforms, networks, workstations, servers and other assets is becoming an increasingly vital component of any corporate security strategy.

However, event logs from all these platforms must be correlated and analyzed, while SIEM management and other admin tasks must be handled as well. Removing noise to focus on the right signals is a profound challenge for internal IT and cybersecurity teams. Trying to find



the real threats within the general flood of noise emanating from so many sources is the proverbial needle in the haystack search, for the digital age.

A resulting concern is that with cybercriminals deploying layered attacks designed to trigger only the subtlest of alerts, it's very common for overstretched security teams to miss bad actors' presence in their systems for weeks or even months. Every day attackers navigate quietly in systems increases the amount of damage they can do, and raises the cost to your organization.

The financial implications are sobering. Last year, it took security teams an average of 287 days to identify and contain a breach, raising the average cost to between $4.24 million and $4.87 million – depending on how many days it took them to identify and stop the attack (Ponemon, IBM 2021).

287

are willing to make a

SIGNIFICANT INVESTMENT

in **RISK MANAGEMENT**

Source: Ponemon, IBM 2021

As a result there is growing demand for solutions to pull all this disparate information together to quickly paint a picture of what is happening, and automate as much of the response and remediation process as possible – with experts handling escalations. This requires addressing data silos and speeding up the neutralization of attacks, removing attackers from the network in minutes, not hundreds of days.

The solution is Extended Detection and Response. XDR gathers security data from all platforms and networks and correlates it. In preferred solution types, XDR will also automate responses with 24x7x365 analyst oversight using a proper Security Operations Center (SOC). Far from being just another marketing buzzword, the best XDR solutions offer a practical, effective and scalable answer to the previously intractable problems we've outlined.

In this white paper we will look at what XDR is and how it works, the benefits it offers, typical use cases, and key things to have your security teams check when selecting a solution. As we will see, XDR can cut costs driven by vendor sprawl, dramatically improve threat detection, accelerate Mean Time to Detection (MTTD) and Mean Time to Response (MTTR) and enable analyst effort to be focused where it will deliver the greatest value.

What is XDR?

XDR is an evolution of the well-established Managed Detection and Response (MDR). While MDR focuses on endpoints such as desktops, mobile devices and servers, XDR extends detection and response management across a much wider range of assets and services, including firewalls, vulnerability scans, clouds, networks, PaaS and SaaS, as well as endpoints. The best XDR solutions go further still to cover DNS and the Dark Web. XDR supports telemetry from the broad range of infrastructure assets utilized by today's organizations, and leverages Artificial Intelligence (AI) and Machine Learning (ML) to deliver clear visibility and automated responses with the oversight of experienced SOC analysts. With the majority of IT and cybersecurity professionals remaining convinced that MDR provides better threat detection and response than they could deliver in house, SOC analysts are essential to any XDR solution.

Addressing the Flood of Alerts

XDR addresses two key challenges experienced by organizations using SIEM systems.

XDR supports telemetry from the **broad range** of **infrastructure assets** utilized by today's organizations

Generating substantial numbers of alerts, such systems require the manual intervention of human analysts to make response decisions and initiate remedial actions. With skills shortages biting hard and the relevant expertise being expensive and in short supply, this is a significant issue for all organizations.

Closely tied to this lack of in-house expertise is the matter of noise. Seeking to ensure no genuine threat is overlooked, SIEMs typically generate huge volumes of alerts. Before making response decisions and taking action, analysts must identify which alerts relate to genuine threats and which do not. Finding the important events amid the ongoing flood of alerts is a major challenge.

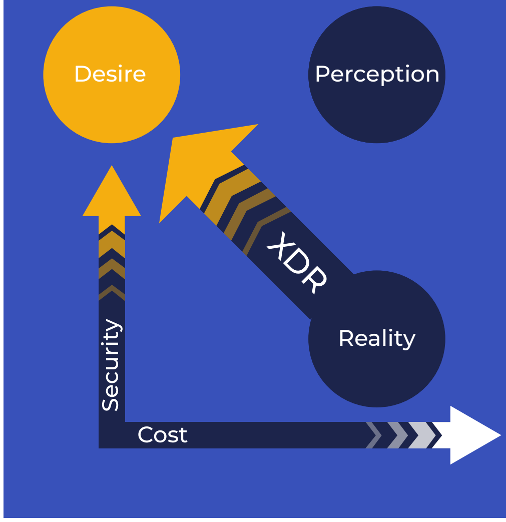
Without the right combination of sufficient human expertise and effective automation, these challenges form a toxic mix, with high noise levels' driving a tendency for overstretched human analysts to disregard issues raised by the SIEM. Alert fatigue is real, and exceptionally dangerous.

In addition to driving alert fatigue, these challenges slow down the time it takes to detect and respond, extending attackers' windows of opportunity to progress covert attacks, stealing and compromising assets as they go.

Security vs Cost – Perception, Desire and Reality

Everyone wants great security at low cost – a desire that runs against the general perception that effective security is expensive. The reality is that most organizations have weaker security than they want, or think they already have.

This is down to scarcity of resources and the complexity of the task. The security landscape is highly complex and constantly evolving. To address the risks in-house, it requires specialist human resources and costly software tools. In fact, it takes 10 full-time, highly experienced analysts to monitor and respond around the clock, 365 days per year but these experts are in exceptionally short supply, and software must be constantly refreshed and updated. This is why attackers tend to do their work at night, on weekends, and over holidays.



XDR delivers what it's typically impossible to deliver in-house: effective security monitoring and response, around the clock, every day of the year, at a manageable cost. It does so by automating detection and threat response with the oversight of expert, certified SOC analysts. It shifts the reality closer to the desire by making existing investments more effective and plugging gaps created by internal teams struggling to cope with increasing demands.

© Copyright 2023 CISO Global. All rights reserved.

Visibility and Automated Response

XDR leverages ML and AI to address these issues. It extends visibility across infrastructures and services while cutting through the noise and highlighting priority events. It can also automate responses, calling in expert analyst oversight where necessary, reducing workloads and accelerating threat detection and response.

In a typical XDR solution, the SIEM pulls in data from a broad spread of assets and services, all of which are continuously generating alerts. These are sent to the Security Orchestration, Automation and Response (SOCaaS) module which provides automated remedial action. Events are then reviewed by professional security analysts who gather threat intelligence and make decisions on what to do from there.

> **XDR** delivers automated **THREAT ASSESSMENT** and **RESPONSE**, with analyst **OVERSIGHT**

SOCaaS and the SOC: Superior XDR's Secret Weapons

Two components are fundamental to the power of superior XDR offerings, but are often missing from or limited in more pedestrian alternatives. They are Security Orchestration, Automation and Response (SOCaaS) and experienced SOC analysts.

In the established world of EDR and SIEM, when a suspicious event is logged by the SIEM, an analyst sees it, reaches out to the infrastructure team, opens a ticket with them, and waits for a response so they can provide guidance on a fix for the issue. This all takes time, even once the analyst has spotted the issue among the large numbers of alerts the SIEM is putting out – time which attackers will use to further penetrate and compromise the estate.

The SOCaaS component of XDR works closely with experienced SOC analysts to address these challenges.

Automating Responses

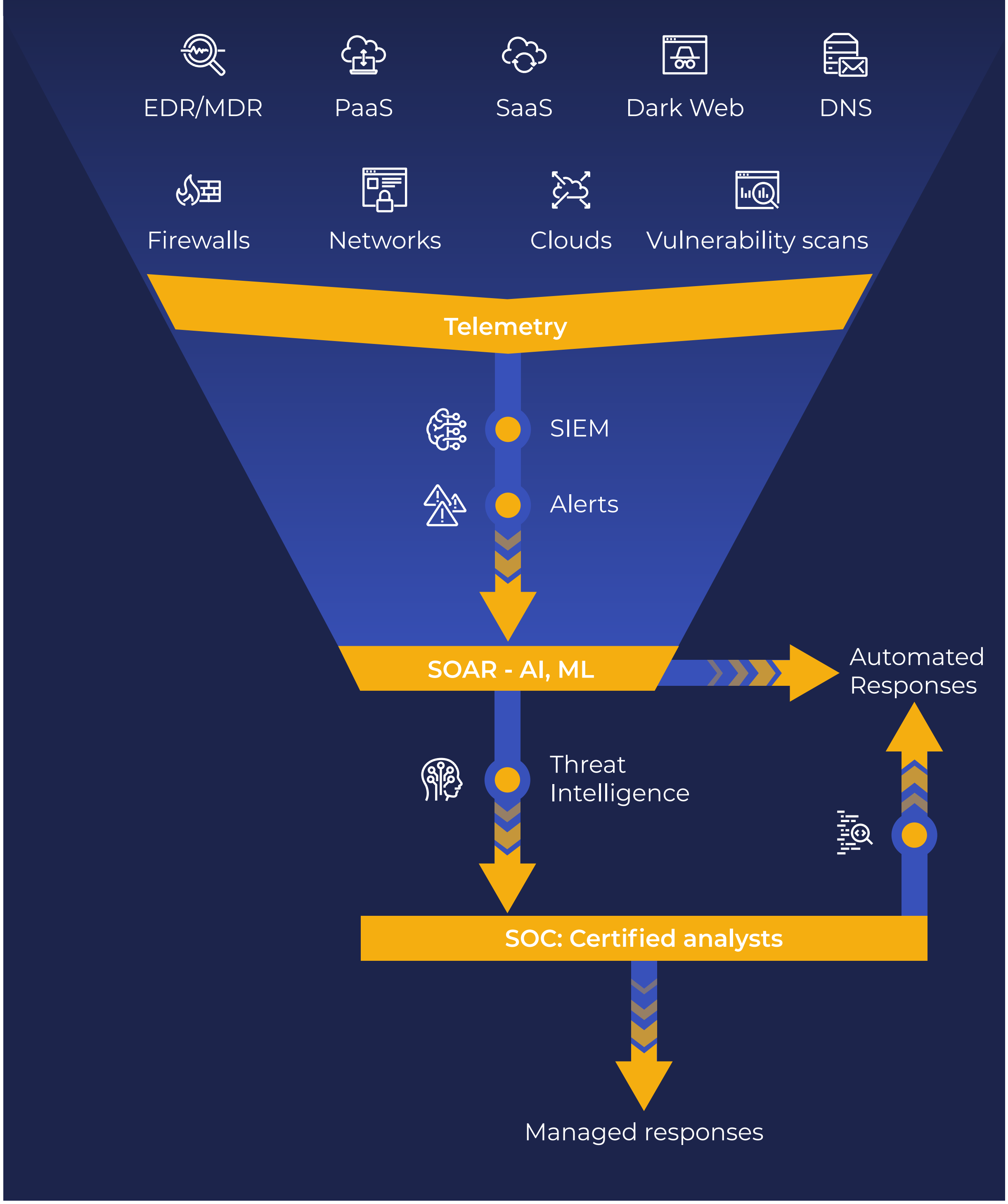
Instead of sending alerts straight to analysts for research and action, the SOCaaS receives them and uses threat intelligence and the appropriate playbook for the scenario at hand, to confirm which of them represent threats. Actions such as killing and quarantining rogue processes can then be taken automatically. The SOCaaS then passes the case to an analyst for review, with full information on the threat and the actions it has taken. Thus, XDR delivers automated threat assessment and response, with analyst oversight.

Fully customized, bespoke SOCaaS toolsets, created for the customer by the SOC, can immediately stop known malicious events and other specific events, as required by the organization, reporting as before to an analyst that they have done so.

If the SOCaaS receives inconclusive threat intelligence, it can pass the case to a human analyst for priority review before taking any action. The analyst can then decide on the appropriate response for the circumstances at hand.

This automation dramatically cuts both MTTD and MTTR. While actual timescales inevitably vary from alert to alert, response action timescales are typically reduced to minutes, from what could otherwise have been hours, days, weeks or even months, as illustrated by our Cautionary College Tale.

XDR – Key Components



EDR/MDR

PaaS

SaaS

Dark Web

DNS

Firewalls

Networks

Clouds

Vulnerability scans

Telemetry

SIEM

Alerts

SOAR - AI, ML

Automated Responses

Threat Intelligence

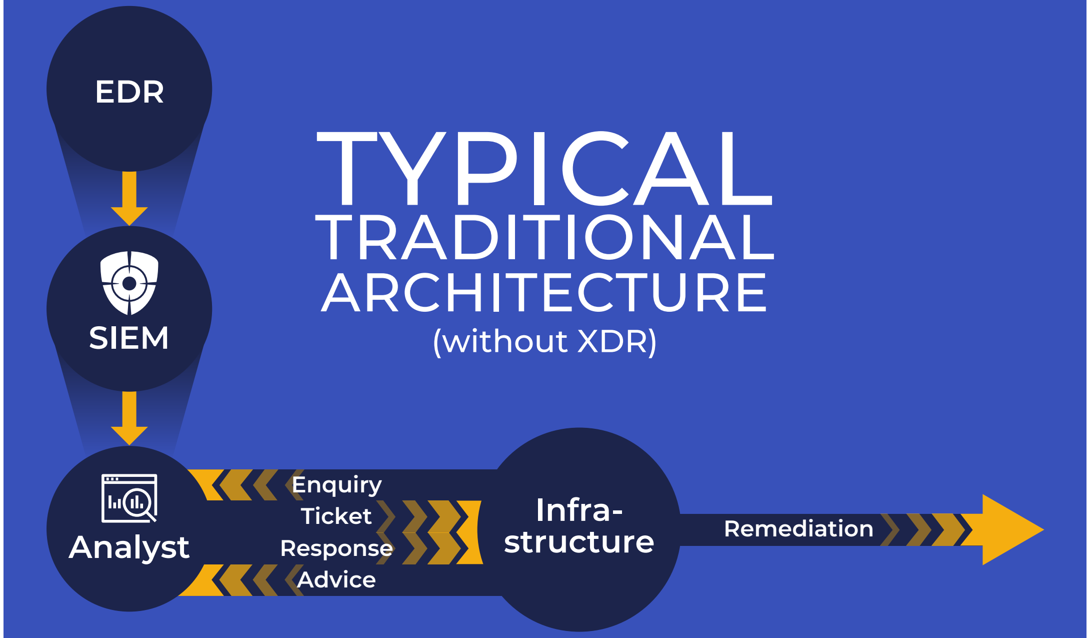
SOC: Certified analysts

Managed responses

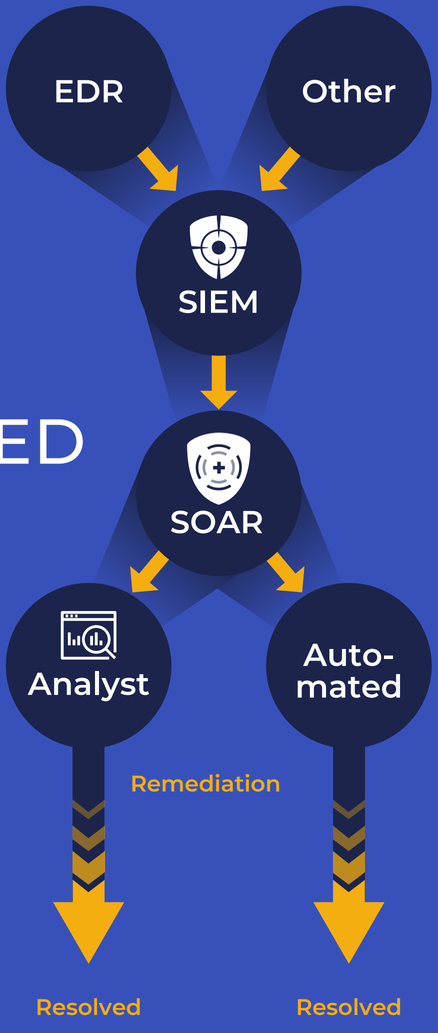
© Copyright 2023 CISO Global. All rights reserved.

Activity Flows **WITH** and **WITHOUT XDR**

TYPICAL TRADITIONAL ARCHITECTURE
(without XDR)



WITH FULL-FEATURED XDR



Known Goods and Bads

Attackers will often employ known good tools such as RDP in their penetration attempts, to avoid drawing suspicion. The simple presence and use of such tools does not necessarily suggest a potential attack; it's all in how they are used. For example, such a tool could be used to perform malicious actions instead of good ones. So, if you only look for the installation of malware, you could miss blatant data theft using an RDP tool. Using behavioral analysis, solid XDR solutions can identify anomalous usage of such tools, as well as other unexpected behaviors, like staff members logging into servers they don't usually use, or data being transferred at odd hours to IP addresses not normally accessed.

Then, the XDR's SOCaaS can use automated playbooks to swiftly take pre-determined actions in response to specific, common attack types, ensuring they are rapidly neutralized whenever they occur. Having taken action, the SOCaaS will alert an analyst with the details of the threat and the action taken. The analyst will then review and confirm or amend the action.

Alert Before Action

It is important to note that customization makes XDR possible in some organizations where it otherwise would not be. For example, if you are under special compliance requirements to review certain types of events before taking action. Here, it is essential to work with a provider whose solution can be tailored not only to your environment, but also to your communication needs.

For example, when unexpected logins occur on specific systems such as firewalls and Industrial Control Systems (ICS) the SOCaaS component can be configured to automate the raising of alerts via approved communications channels, keeping infrastructure providers compliant. In these cases, instant messaging is often used during working hours, and call trees out of hours, so that internal stakeholders can assess threats and decide promptly on the right actions to take, according to compliance and industry requirements. This process is only possible in XDR solutions that include customization and automation bespoke to the client's environment.

Working with experienced SOC analysts, the SOCaaS employs AI and ML to identify the threats hidden in the large amounts of information produced by EDR and the SIEM. Playbooks automate remedial action and communication, ensuring threats are swiftly and effectively dealt with, and key players are fully aware of such threats and the actions taken.

Playbooks

Also known as runbooks, playbooks are no different from a football coach's playbook: step-by-step plans used by SOC teams to address various scenarios that arise in security events. These are instructions on how to handle a variety of specific, defined disasters. Typical examples might include handling an infected endpoint or a phishing attempt.

Since most SOCs follow playbooks manually, reading digital files or paper in binders, all actions take place at human speed. Meanwhile, the attack is often progressing at machine speed. It's good to find out what kind of playbooks your provider is using.

© Copyright 2023 CISO Global. All rights reserved.

AutomateD

Superior XDR solutions automated playbooks, allowing predefined actions to be taken at machine speed. Drawing on multiple sources of intelligence – telemetry from diverse sources – the XDR assesses whether the event at hand is a threat, and if so, how critical it is. It can then take action right away, before passing to analysts for review.

This reduces the time it takes to stop an attack to minutes.

Customized

Playbooks should be fully customized by the XDR provider according to the customer's business use cases and workflows. For example, while one organization may require suspicious looking endpoints to be taken offline immediately, another may need workstations to be pulled offline, but servers to be left running.

When considering any XDR solution, it is important to ensure that playbooks are fully customized and automated, executed at machine speed, and in every detail support your specific business use cases and workflows.

With and Without XDR

Fully featured XDR solutions provide numerous benefits, essential in today's security landscape, over both traditional approaches and more limited solutions marketed as XDR.

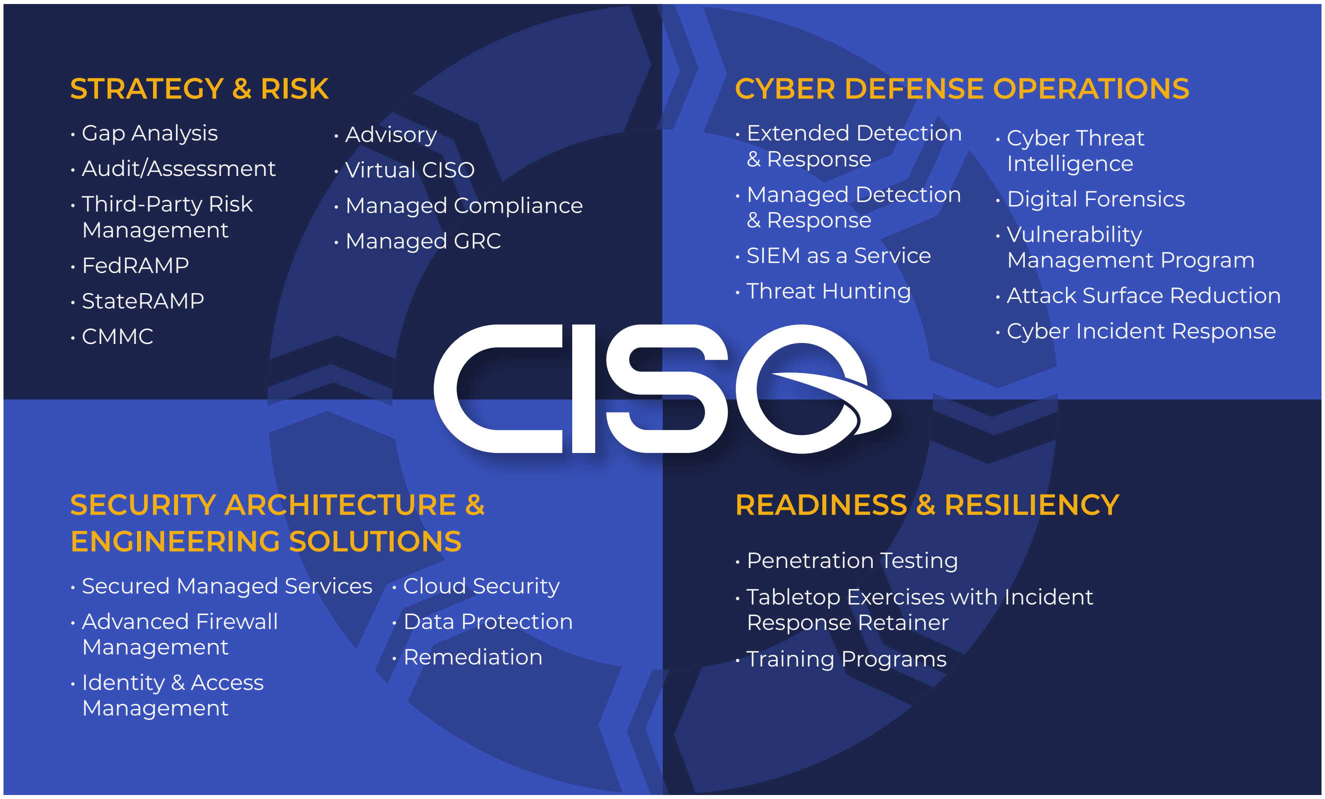
FULLY FEATURED XDR	TRADITIONAL SOLUTION
✓ Supports telemetry from a wide variety of sources	Often just monitors endpoints
✓ Automatically correlates and assesses alerts, highlighting and responding to significant events	Generates numerous alerts whose relationship to one another is often opaque, placing heavy assessment burdens on analysts
✓ Automates remediation and response capabilities	Relies on analysts for manual remediation and response, further burdening them
✓ Undertakes behavioral analysis, understanding normal user and system behavior and detecting anomalies	Lacks behavioral analysis capabilities, allowing covert attacks to be mounted using known good resources
✓ Employs fully automated playbooks for swift resolution of known threats	Requires analysts to execute playbooks manually when threats are detected

About CISO Global

CISO
GLOBAL

A leader in cybersecurity and compliance services, CISO Global brings together expert practitioners and thought leaders to provide tailored solutions that drive cyber resilience. The company's top-tier talent spans geographies, specialties, industries, regulatory frameworks, and focus areas and includes auditors, compliance specialists, certified forensics experts, ethical hackers, security engineers, and around-the-clock analysts.

To learn more, visit www.ciso.inc.



STRATEGY & RISK

- Gap Analysis
- Audit/Assessment
- Third-Party Risk Management
- FedRAMP
- StateRAMP
- CMMC
- Advisory
- Virtual CISO
- Managed Compliance
- Managed GRC

CYBER DEFENSE OPERATIONS

- Extended Detection & Response
- Managed Detection & Response
- SIEM as a Service
- Threat Hunting
- Cyber Threat Intelligence
- Digital Forensics
- Vulnerability Management Program
- Attack Surface Reduction
- Cyber Incident Response

SECURITY ARCHITECTURE & ENGINEERING SOLUTIONS

- Secured Managed Services
- Advanced Firewall Management
- Identity & Access Management
- Cloud Security
- Data Protection
- Remediation

READINESS & RESILIENCY

- Penetration Testing
- Tabletop Exercises with Incident Response Retainer
- Training Programs

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations

SOC 2® Type II Audited

© Copyright 2023 CISO Global. All rights reserved.