REDEFINE SECURITY OPERATIONS WITH XDR

Don't Get Stuck with Endpoint Detection and Response

Introduction

The goal of any security team is to defend an organization's infrastructure and data from damage, unauthorized access, and misuse. Security architects and engineers typically take a layered approach to prevention. As attacks have become more automated and complex, this approach has grown to include layered visibility in the form of detection and response products, such as endpoint detection and response (EDR), network traffic analysis (NTA), and security information and event management (SIEM).

This layered visibility comes at the cost of time and expertise. Disparate detection and response products create additional alerts, requiring a greater skill set to solve and increasing the interminable cycle: an endless stream of events, more tools and information to pivot between, ever-longer time to detection, and a security team that faces burnout, all while security spend never seems to be enough. The more we react, the farther behind we get.

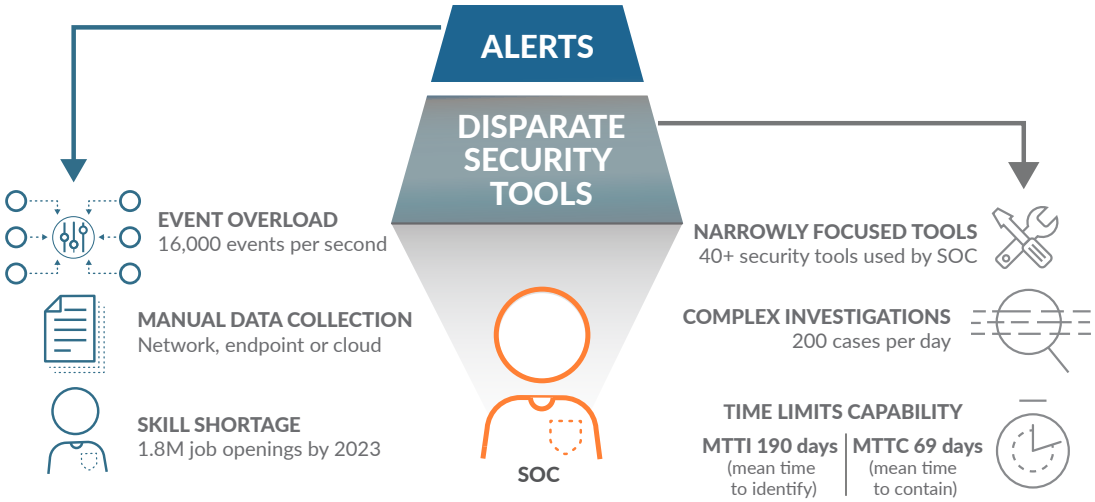


Figure 1: Network, endpoint or cloud

Many organizations like yours are battling with the same question: How can we shift away from reacting to inbound alerts and toward an active defense posture that can improve threat prevention?

It's time for a different approach—one that benefits the entire security team rather than burdening it, simplifies operations, and provides the means to rapidly detect and respond to the most sophisticated threats across the entire ecosystem.

Today's Approach: Solving One Problem Creates Others

Security teams work hard to keep their organizations secure but face difficulties in their efforts to prevent data breaches. The top five challenges include:

- Event overload
- Too few security analysts
- Narrowly focused tools
- Lack of integration
- Lack of time

Figure 2: SOC teams face five primary challenges

Let's explore each in some detail.

1. Event Overload

Security analysts see too many events to deal with them all effectively. 55 percent of security teams or security operations centers (SOCs) receive more than 10,000 events daily on average.[1] However, not all events are equal—most need to be prioritized, correlated or normalized, and added to the alert pool. Even with SIEM to help the SOC team comb through this mass of data, a security analyst must still expend manual effort to gather data, perform analysis, and weed out false positives—and quickly, lest they miss the most critical alerts. All too often, analysts fall victim to "alert fatigue," wherein they filter out alerts based on prior assumptions or the sheer mass of data. Due to alert volume, 54 percent of security professionals ignore alerts that should be investigated.[2]

2. Skills Shortage

Many organizations are trying to overcome increasing workloads by hiring more people, but there is a worldwide shortage of trained security professionals that analysts predict will reach 1.8 million by 2022.[3] It is especially difficult to find specialists with network or endpoint forensic experience, or both. As a result, security teams are overburdened in terms of alert triage as well as investigation and response. They spend an inordinate amount of time on tedious tasks, such as data collection, manual analysis, and incorporating intelligence, or trying to embed automation, causing additional strain. This also serves to curtail learning and sharing as knowledge and historical activity remain siloed and unavailable to other groups.

The combination of too many alerts, complex investigations, and too few analysts leads to human error and create a snowball effect downstream. Alerts are de-prioritized or falsely escalated due to lack of information, causing more work for members of the incident investigation team, who need help from hunting teams to handle the workload.

3. Disparate Tools with Too Narrow a Focus

The addition of tools is one way to overcome other challenges while enabling faster, more informed decisions, but there is such thing as too many tools. Most security tools have been developed to address specific technology gaps without consideration for how the tools should work in an operational environment, and often work against the security team's goal of providing holistic prevention and visibility. Operating in silos, lacking integration, and ingesting data from only a single source, these tools bring value only to those with specialized skill sets on the security team while providing no value to, and even serving to overburden, others.

Some tools commonly used in detection and response are valuable but limited:

- **EDR** can shorten investigation time for experienced incident response teams, but it is limited to data from endpoints on which you can install an agent. EDR can also drastically increase the volume of alerts, and it requires customized development to enable basic automation, burdening other parts of the team at the same time.
- **NTA** requires proper sensor placement to avoid missing volumes of traffic, rarely includes response, and doesn't incorporate endpoint data as a factor in anomaly detection or threat investigation.
- **UEBA** (user and entity behavior analytics) is largely focused on log data and misses key details from deep analysis of the network, not to mention the endpoint and the cloud. Additionally, UEBA has a high rate of false positives, further adding to analysts' workloads.

These tools all help with visibility, but because they introduce new problems, they still require specialized skill sets to render actionable results.

4. Swivel-Chair Syndrome for Investigations

Detection of sophisticated attacks requires data to be correlated from anywhere within the digital domain. As most tools that aid detection and response are based on only one data source, such as the endpoint, they miss important clues from other crucial sources, leaving security teams to do the heavy lifting in threat validation. With a typical large organization's SOC using more than forty tools, each operating independently, SOC analysts find themselves in "swivel chair" mode: they switch from screen to screen, trying to piece together conclusions from relevant information so they can mitigate real threats. If the data were correlated, it could provide a holistic view of the environment—but that would require normalization, date/time/event matching, and an understanding of investigative techniques in multiple areas, such as the network and endpoints. It's not an easy proposition, and today, it must be done manually.

1. "Survey: 27 Percent of IT professionals receive more than 1 million security alerts daily," Imperva, May 28, 2018, https://www.imperva.com/blog/2018/05/27-percent-of-it-professionals-receive-more-than-1-million-security-alerts-daily/.
2. "2017: Security Operations Challenges, Priorities, and Strategies," ESG, March 2017, http://resources.siemplify.co/hubfs/PDF%20Downloads/ESG-Research-Insights-Report-Siemplify.pdf?hsCtaTracking=4303efc5-9f7b-4a8a-9438-263c0588b898%7C6043fb9a-2881-4940-9a0e-6239a8686b81.
3. "2017 Global Information Security Workforce Study," Frost & Sullivan, accessed January 8, 2019, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf.

5. Time Is the Enemy

The greatest commodity of all is time. The more quickly a threat can be identified, the greater the chances of containment. As teams struggle with event overload, resourcing issues, and lack of correlation, they risk missing nondescript alerts that become major incidents and have trouble allocating the time to find unknown threats. On average, we see more than six months between when a data breach happens and when it is first identified,[4] and this "dwell time" is getting worse. Mean time to identify (MTTI) rose from 190 days in 2017 to 197 days in 2018, and response times—measured as mean time to contain (MTTC)—rose from to 66 days in 2017 to 69 days in 2018.[5]

This is all occurring at a time when organizations are embracing EDR, NTA, and UEBA, and reassessing SIEM while spending almost 60 percent of IT budgets on security.[6] Even with these tools, analysts spend significant amounts of time on manual tasks, such as writing queries, correlating alerts with log data, and piecing together information from disparate sources. With a constant array of work, it's no wonder few security teams have time to focus on critical tasks, such as hunting for sophisticated threats, doing more in-depth thinking, and solving obscure security problems that clever programs and automation are unable to unravel.

The SOC Deserves a Better Approach

The SOC team needs an approach that effectively addresses the aforementioned issues. This calls for a new approach that can aid the SOC in all stages of operations—alert triage, incident investigation, and threat hunting—and help conclude investigations quickly, regardless of threat type. In practical terms, the ideal approach would:

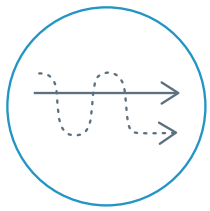
- Track activity across your network, endpoints, and clouds for the purposes of detection, alert triage, investigation, and response.
- Integrate with tools that generate alerts or provide intelligence to automatically present information, derive conclusions, and even take action where possible.
- Use large-scale analytics to correlate data from all sources, allowing automated or manual detection of hard-to-find threats spanning multiple data sources, with few false positives.
- Simplify investigations to aid less-experienced analysts and reduce the burden on experienced personnel, drastically improving time across all stages of SOC operations.
- Ensure that intelligence from every investigation can be quickly converted to improve defenses, such as by adding context to future investigations, reducing the number of alerts, and closing newfound or known vulnerabilities.

This would notably reduce mean time to detect and respond to threats (dwell time) as well as help move security teams away from being reactive to security alerts and toward defending the network proactively.

XDR Takes Detection and Response to a New Level

Palo Alto Networks is introducing a breakthrough approach to security operations by increasing visibility as well as the speed of threat detection, investigation, and resolution. It's called XDR, an evolution of the detection and response category. The "X" stands for any data source, be it network, endpoint, or cloud, with a focus on force-multiplying SOC productivity though automation. Complete visibility provides a holistic picture of the organization's activity by linking data from multiple sources so there's no more manual data correlation and nowhere for threats to hide. Integration pulls data from external sources, such as

Find stealthy threats faster with analytics across network, cloud, and endpoint



Simplify investigation and response to known and unknown threats

Radically improve security operations and return on security investments

Figure 3: Three key benefits of XDR

4. "2018 Cost of a Data Breach Study," Ponemon Institute, May 2018, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&.
5. Ibid.
6. "Infographic: 2018 IT budgets are up slightly; spending focus is on security, hardware, and cloud," ZDNet, October 2, 2017, https://www.zdnet.com/article/infographic-2018-it-budgets-are-up-slightly-spending-focus-is-on-security-hardware-and-cloud.

security alerts and global threat intelligence, to add insights. Automation merges critical data onto a single pane of glass while drawing conclusions for security analysts, doing in seconds what normally takes hours with years of experience. The result is simplified investigations across security operations, reducing the time it takes to discover, hunt, investigate, and respond to any form of threat.

XDR ushers in a new era of heuristics, analytics, and modeling, applying artificial intelligence and machine learning to rapidly detect and stop the most sophisticated threats. As it tracks threats across any source or location in an organization's infrastructure, XDR can automate containment, reconstruct each step of an attack to provide a clear sequence of events, apply threat intelligence, and close gaps for future prevention. This speeds time to resolution and frees analysts from intensive investigation. Importantly, XDR should be delivered as a complete cloud offering to ensure ease of deployment.

XDR Detection and Response Benefits

XDR is designed to work for and with the SOC. It delivers three significant benefits: unlimited visibility, simplified security operations, and radically increased return on security investment.

Unlimited Visibility to Find Stealthy Threats Faster

XDR uncovers anomalous activity by correlating the behavior of users, entities, and actions across all data sources. It reduces threat hunting complexity by providing powerful search capabilities, rich attribution, and data correlation. XDR automates the discovery of active or past threats using big data analytics across endpoint, network, cloud, and third-party intelligence, converging unknown threat discovery to one location for the SOC.

Simplify Security Operations in Triage, Investigation, and Response

XDR accelerates and simplifies investigations by visualizing the activity chain for any event to automatically reveal root causes and provide actionable forensic detail for all security analysts. It eliminates alert fatigue by correlating investigation results with all security alerts from any technology, allowing less-experienced analysts to do more, faster. XDR responds to active threats and prevents future successful attacks via coordinated enforcement across your network, clouds, and endpoints, freeing analysts from manual work and allowing more time for threat discovery.

Radically Increase Return on Security Investments

XDR acts as a force multiplier for the security analyst team, streamlining workflows as well as reducing the time and complexity of event triage, incident investigation, response, and hunting. It enables security tools to work together to automatically address problems, making use of rich data and threat intelligence. XDR strengthens prevention by applying the knowledge gained from each investigation to improving defenses and preventing additional alerts, or similar threats, tomorrow.

How Could XDR Benefit Your SOC?

XDR complements your prevention-first approach with a detection and response technology that helps convert your security operations from reactive to proactive. Complete visibility across all data sources and the right focus on process, from alert triage to threat hunting, will help you drastically improve security operations.

You'll be able to make alert fatigue a thing of the past, empower your security analysts to filter out false positives and make decisions in record time, free up your skilled analysts from manual investigation and remediation, give threat hunters the ability to find unknown threats, and be ready for known threats in the future.

By giving you automation and a big-picture view of security, XDR holds the promise of unleashing the full power of your SOC. If you're looking into detection and response technologies, ask your vendor about the X, because one view of your environment is no longer enough.

paloalto NETWORKS®

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

redefine-security-operations-with-xdr-wp-012219