Secureworks®

WHITE PAPER

Reduce Alert Fatigue in Your IT Environment

How XDR combats cybersecurity noise to deliver a truly robust defense

Security teams are tasked with managing a huge volume of alert logs, and this noise can overwhelm any team – let alone an individual analyst. A recent study showed that 70% of SOC teams are emotionally impacted by their work managing IT threat alerts – and more than half said they aren't entirely confident in their ability to prioritize and respond.[1] All this noise makes it difficult to triage threats, which increases the risk of missing a real threat or potential breach incident. In fact, a recent Forrester study showed security teams are significantly understaffed when it comes to incident response, especially as they encounter more frequent attacks.[2]

70%

of SOC teams are emotionally overwhelmed by managing security alert volumes

As the cyber threat landscape continues to evolve and attack surfaces grow, what does this mean for security teams who are trying to sort through the noise to detect the real threats to their environment? Understanding the bigger picture of how the security landscape is progressing is a first step to addressing this ongoing challenge.

A Look Back

It's necessary to take a historical look at where the security industry began to understand how we got here and to shape where we want to go. Around 20 years ago, the security industry had standard firewalls for packet filtering, sniffing IDS for deep packet inspection, traditional AV alerts, and server logs. All of these were forwarded to a Security Information and Event Management (SIEM) system to be analyzed in real time. The problem was that every SIEM provider was looking to integrate more data sources to keep up with industry growth. As a result, next-gen firewalls, intrusion prevention systems (IPS), email security gateways, routers, switches, load balancers, and endpoint detection and response (EDR) were added to the mix. While these additional integrations were well-intentioned, they contributed to an increasing log noise and alert problem. Over time, the number of correlated log alerts increased on an exponential scale, exceeding what analysts could keep up with.

Contributions to a Noisy Environment

Today's security environments have become increasingly noisy, and both internal and external factors are to blame.

Internally, there are a few issues to consider. First, a larger attack surface and more technology gives way to an increasing number of alerts. The more endpoints an organization has to monitor – not only in the form of increased headcount, but additional devices per employee – the larger the attack surface. Further, the number of devices, the type of devices, and the tuning that has been done on those devices can all affect the alert volume for a security team.

The ever-growing attack surface and stretched perimeters have resulted in increased security controls. While these controls have been great for enabling the industry to adapt, they have also caused an influx of alerts. And, one incident an analyst reviews could require the use of multiple platforms or tools.

There are no signs that the growing attack surface will wane, in part due to the recent explosion of the Internet of Things (IoT). And with the variety of "smart" solutions available to businesses – employee badges, inventory trackers, barcodes, and so on – that growth is poised to continue its trajectory. The number of businesses that use IoT technologies increased from 13% to 25% from 2014 to 2019[3]. Further, a recent forecast estimates that by 2025, there will be 41.6 billion connected IoT devices, generating 79.4 zettabytes of data.[4]

41.6B

connected IoT devices will generate 79.4ZB of data by 2025

On top of a growing attack surface, the rise of cloud environments has also added to inbound noise and complexity within security teams. For many organizations, cloud adoption happened quickly, and with it came related noise. Amid the COVID-19 pandemic, companies found themselves moving from an on-premises network to working with cloud-native applications such as Microsoft Teams, Zoom, or WebEx. Without a doubt, adding these platforms creates another layer of complexity for security operations. Companies have many more questions to ask themselves about how their data is being transferred and stored. What used to be a piece of paper or conversation by a water cooler is now a digital file.

Complicating things even further, in the past, the industry reached a point with SIEMs where the common mentality was, "If it can generate a log, we can ingest it." However, while cloud security generates a large number of logs, that doesn't mean they are all valuable from a security perspective.

For example, some organizations want to monitor software development lifecycles using cloud-native services. Traditional SIEMs would not have monitored this type of activity – but with the evolution of cloud-native services, clients expect vendors to ingest these logs and provide context, even if in the end they have little security alerting value. As a result, organizations need to reconsider their strategy to avoid alert fatigue. The old way of thinking – that everything that could be monitored should be monitored – needs to be reconsidered.

There are also external factors that influence the amount of noise within an IT ecosystem. Changes in the threat landscape can expose new vulnerabilities for certain companies. For example, active phishing or malware campaigns may target specific verticals (financial, pharmaceutical), and as we saw with COVID-19, threat actors pivoted their focus to exploit the fear and uncertainty around the situation.[5] All of this contributes to additional alerts for a security team.

The Challenges and Consequences of Alert Fatigue

IT teams facing the everyday reality of noisy environments often deal with alert fatigue or analysis paralysis. Alert fatigue can be defined as the situation in which too many repeatable alerts occur that are non-actionable, false positives, or that the SIEM cannot diagnose as a true threat, so it falls to an analyst to manually review. Research from ESG reveals that 45% of daily alerts were ultimately determined to be false positives.[6] In this study, 75% of respondents say their organization spends an equal amount – or sometimes even more time – on false positives as on legitimate attacks.[6] Often, the sheer influx of noise results in analysts turning off the tools they use.

75%

of organizations say they spend an equal amount – or sometimes even more time – on false positives as on legitimate attacks

Undoubtedly, tracking alerts leads to “swivel chair” responses – a way to describe how analysts typically have to toggle between multiple security consoles in response to a single alert. At best, this workflow can cause analysts to burn out, and it commonly results in missed, or ignored, genuine alerts.

To get a well-reported, tangible understanding of the consequences of alert fatigue, we don’t have to look further than the infamous Target breach. During this high-profile incident – which compromised the credit card information of 40 million customers – the company’s malware detection tool did detect a threat and send an alert, but the security team ignored it because of the high volume of alerts they were used to and the frequency of false positives they received. The cost? All told, nearly $300 million in expenses to the retail giant.[7]

Getting Rid of Noise With XDR

As a security leader, how do you empower your teams to accurately decipher what is noise versus a real alert worth investigating? The good news is that the security industry has risen to the challenge of minimizing alert fatigue and optimizing intervention efficiency.

Whether approaching it from the SOC or Managed Security Services perspective, or using the development of EDR (Endpoint Detection and Response), vendors are creating new Extended Detection and Response (XDR) platforms. XDR platforms are an all-encompassing IT and business infrastructure security management tool (covering cloud, network, endpoints, and business applications). With the primary purpose of stopping attacks and threats through coordinated early prevention, XDR can also minimize the organizational impact of an attack incident, should one occur.

XDR is a purpose-designed tool aimed at improving the effectiveness and efficiency of security operations staff. It addresses the challenges that security analysts and operators face head on through the unification of the, on average, 45 security tools that often exist in Enterprise networks—condensing them down to one tool for all investigations. As a result, it eliminates operational complexities.

Research indicates that an average of 80% of successful breaches are new or unknown “zero-day attacks.”[8] To help combat these and other sophisticated "tradecraft" and threats, XDR adds powerful AI detectors and security analytics, combined with the latest threat intelligence, for efficient, effective responses that would otherwise seem impossible.

XDR also solves the overwhelming volume of alerts and false positives by selectively calling upon and correlating security telemetry data, which it then uses to validate and prioritize alerts, so security analysts and operations are truly focused on the real attacks occurring in their IT ecosystem.

What Should a Full XDR Solution Do for You?

As you are unifying your prevention, detection, and response in one place, a fully developed XDR platform needs to perform many roles. These are the ones we consider essential.

- **Correlation** – to bring together relevant security data from your existing systems.
- **Detection** – of known and unknown threats to automatically protect your entire environment from a wide range of threats.
- **Enrichment** – of data with relevant user and asset context to speed up decisions.
- **Mapping** – of threats and alerts to the MITRE ATT&CK framework to clarify where in the kill chain the attack was stopped.
- **Collaborative Support** – you don't want DIY XDR; you need to know that fast, expert support is on hand.
- **Automation** – of containment and prevention actions. (If this is left to humans, the reaction time is too slow.)
- **Intelligence** – added external counter threat intelligence and collective intelligence from other XDR platform users.
- **Focus** – XDR delivers security operators with "true positives" by providing in-depth alert validation.

In the end, XDR is designed to detect threats with speed and precision, combining prevention—to block attacks and provide valuable context for any later investigations – with detection that covers the entirety of attack surfaces and uncovers threats that would normally bypass prevention controls. (Note: Most of today's successful attacks are designed and tested to bypass prevention detection controls!) And, XDR offers response capabilities that provide the data needed to enable in-depth threat investigations and incident response actions across all attack vectors.

An effective and efficient XDR solution energizes your security operations and enables your team to stop attacks, minimize system and user downtime (think ransomware), and bring focus to help minimize incident response workloads.

Looking Ahead

As the cyber threat landscape evolves, workplace perimeters continue to dissolve and attack surfaces continue to grow. All signs indicate that overwhelming alert noise is here to stay and security leaders need to adapt a new approach to keep up. After all, the old SOC SIM/SIEM approach was never designed to be a single-pane-of-glass extended security detection, prevention, and incident response solution covering cloud, network, and endpoint IT infrastructure.

The move to adopt XDR may take time because many organizations are still committed to the "more logs are better" mentality. This is, in part, exacerbated by the number of tools and products available in the market to ingest more information. Compliance requirements have also led to a big data problem, significantly increased operating costs, and created a false sense of security – as there is often no security relevance to compliance logs or the alerts they generate. However, eliminating or tuning out too many logs may mean you eliminate something worth investigating. On the other hand, by not eliminating or tuning out enough, you're right back where you started – drowning in noise and false positives. Striking the right balance to manage both these risks should be top of mind for every organization, and XDR works by being able to use selective logs as needed, rather than create a data lake of barely touched information.

Security leaders need to conduct an urgent reevaluation of their security strategy to help analysts focus on the alerts that matter and find the most efficient way to protect their organization. Hybrid XDR models that include rapid access to security expertise – including incident response teams and fully managed XDR with internal teams focused on business security priorities – are now very viable options.

As Forrester so clearly points out[2], XDR presents security teams with a simpler and more effective way to address threats and unify security-relevant telemetry data—from both security and business tools across your IT environment. You can also harness XDR's cloud-native big data infrastructure, machine learning capabilities, and sophisticated security analytics, which all offer enhanced flexibility, scalability, and opportunities for automation. Plus, analytic capabilities and third-party integrations provide both the missing visibility and controls over all parts of the business to deliver the robust defenses organizations need in today's tough threat landscape by eliminating irrelevant cybersecurity noise.

Sources:

[1] Trend Micro, A global study: Security Operations on the backfoot

[2] Forrester, Adapt or Die: XDR is on a Collision Course with SIEM and SOAR

[3] McKinsey, Growing opportunities in the Internet of Things

[4] IDC, Worldwide Global DataSphere IoT Device and Data Forecast, 2019-2023

[5] DHS, CISA, NCSC, COVID-19 Exploited by Malicious Cyber Actors

[6] ESG, Reaching the Tipping Point of Web Application and API Security

[7] Infosecurity Magazine, Target Sues Insurer Over Data Breach Costs

[8] Ponemon-Sullivan Privacy Report, The state of endpoint security risk

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Otemachi One Tower 17F
2-1 Otemachi 1-chome, Chiyoda-ku
Tokyo 100-8159, Japan
81-3-4400-9373
www.secureworks.jp