deepwatch

Alleviating Alert Overload: Reducing Noise for Better Security Focus

www.deepwatch.com

Introduction

Traditional alert monitoring is not working

Most enterprises see over 11,000 alerts per day from an average of 6.8 threat intelligence feeds, according to a 2020 Palo Alto networks report. Almost three-quarters of an analyst's time is spent "investigating, triaging, or responding to alerts, and most of these alerts must be manually processed, which significantly slows down a company's alert triage process." In 2018, Infosecurity Magazine reported, "alerts are on the rise, leaving today's security teams bombarded with 174,000 per week." That works out to a just shy of 25,000 per day.

Today, in 2022, it's fair to say that the daily volume of alerts is even higher. With these number of alerts, the traditional model of alert monitoring is not sustainable. The sheer volume of daily alerts leads to alert fatigue.

The traditional model of investigating alerts requires every alert be reviewed and responded to. With the overwhelming volume of alerts from various security tools, security analysts are unable to keep up with every new alert, are unable to thoroughly investigate all alerts and are challenged to prioritize the alerts. With the lack of prioritization, alerts can slip through the cracks, increasing the risk of irreversible damage.

Alert overload is not a new phenomenon. In 2014, **Target experienced a breach** due to alert fatigue. This attack resulted from Target's security team "reviewing and ignoring urgent warnings from threat-detection tools about unknown malware spotted on the network." The key takeaway is that no single solution or technology that is going to stop a ransomware attack.

Factors Contributing to **Growing Alert Fatigue**

While alert overload and resulting alert fatigue are not new, statistics show that they are getting worse. Research indicates that 90% of companies cannot investigate all the security alerts that they receive in a typical day. The Cloud Security Alliance found only about 23% of threat alerts were real, meaning that 77% were false positives, and according to the same survey, 32% of analysts don't pay attention to alerts due to the sheer number of false alarms, and 26% say they get more alerts than they can handle.

With so many false positives, it's no surprise that more than a quarter (28%) of all alerts are never addressed. Three main factors are contributing to this problem: an expanding attack surface, a growing number of security tools that need to be monitored and managed, and the cybersecurity skills shortage.

Expanding Attack Surface

As the volume and complexity of attacks faced by organizations continues to increase, so has the need to deliver rapid and proactive threat hunting. Threat detection is a data-heavy process demanding real time access to multiple sources of telemetry and a wide variety of logs (potentially spanning a wide time frame). In addition, with the move to the cloud and increased reliance on third parties, merely ensuring visibility across all vectors is increasingly challenging.

The dissolved perimeter due to the introduction and continual growth of cloud-based technology along with a remote workforce has increased complexity for security teams. With more endpoints across a wide range of locations to secure, from laptops to mobile phones to BYO technology, the risk of human error is greater than ever.

Representative Large Enterprise Attack Surface Statistics[1]

8,427	Hosts
1,967	Domains
5,422	Live Websites
777,049	Total Web Pages
3,609	Certificates
114,504	IP Addresses
76,324	Forms
2,841	Wordpress and Drupal Sites
45	Mail Servers
7,790	Cloud-Hosted Apps
1,464	Remote Access Service Instances
8,624	IoT Devices

Growing Number of Tools in the Security Tech Stack

Each prevention and detection tool deployed within a company's security tech stack generates alerts. Most platforms and solutions come with security analytics as a core part of the solution with a suite of prebuilt models and rule-based detections, all of which generate alerts. However, such capabilities are rarely tuned perfectly on an ongoing basis, increasing the likelihood of generating false positives which create more noise for security analysts to sift through.

Cybersecurity **Skills Shortage**

24/7 monitoring is needed to secure a company from the ever-growing attack surface. However, most security teams lack the skilled security staff for round-the-clock security monitoring. This lack of staff adds to additional fatigue felt from alert overload. Without enough experts to review and prioritize alerts identified by security tools in a timely manner, security leaders are faced with working extra hours, facing burnout and fatigue, increasing the risk of missing a critical threat.

The cybersecurity skills gap keeps increasing, with 60% of cybersecurity professionals believing that the cybersecurity staffing shortage is placing their organization at risk. (ISC^2)

Read our eBook titled "Bridging the Cybersecurity Skills Gap in Security Operations" to learn about:

- Security Staffing Is a Never-Ending Task
- The Challenges of Operating a Modern Day SOC
- The Skills Gap In Security Operations
- Operations Staffing for the Future

CLICK HERE TO READ

Impact of **Traditional Alert Monitoring Approach**

Alert fatigue resulting from alert overload decreases the effectiveness and efficiency of a security team.

- Triage becomes very difficult and laborious
- Investigating false positives takes time and attention away from analyzing the legitimate ones, or even finding them in the first place
- Critical threats that appear as low and medium severity alerts are likely to be overlooked

Alert overload costs companies more than you think. When more analyst time is spent sifting through alerts, valuable resources are diverted from other high priority or critical tasks. Spending time on false positives and generally slow investigation/triage leads to inefficient use of people and resources and adds to security risk.

Analysts faced with alert overload experience poor work-life balance due to the nature of their role, leading to burnout. This fact is especially true for smaller IT and security teams. Part of improving as an analyst involves building up a mental database of what attacks look like in real life and making them easier to spot in the future. When an analyst is constantly looking at unnecessary alerts, this can get in the way of the development process.

Burnout from alert fatigue also costs a company money by causing staff turnover. All companies understand the cost and struggle of hiring new staff constantly, especially in roles that impact a company's security.

Rethinking **Alert Management**

The traditional SIEM alerting model relies primarily on alert rules and correlation mechanisms. SIEMs do a decent job at alert correlation but the outcome falls short of security leaders' expectations about reducing alert volume. Assuming 25,000 alerts are generated daily, a 90% reduction in alert volume still leaves 2,500 alerts to be investigated daily. Some quick math shows the problem:

- It takes, on average, 10 minutes to investigate one alert. This does not include additional time needed to investigate complex alerts.
- At this rate, one analyst working solely on alert investigations can get through just under 50 alerts a day in a given shift.
- An organization would need over 50 analysts fully dedicated to alert management to get through the daily alert volume.

Given the large and rapidly growing volume of alerts being generated on a daily basis, compounded with the skills shortage, the traditional SIEM model does not scale to keep pace with today's expanding attack surface.

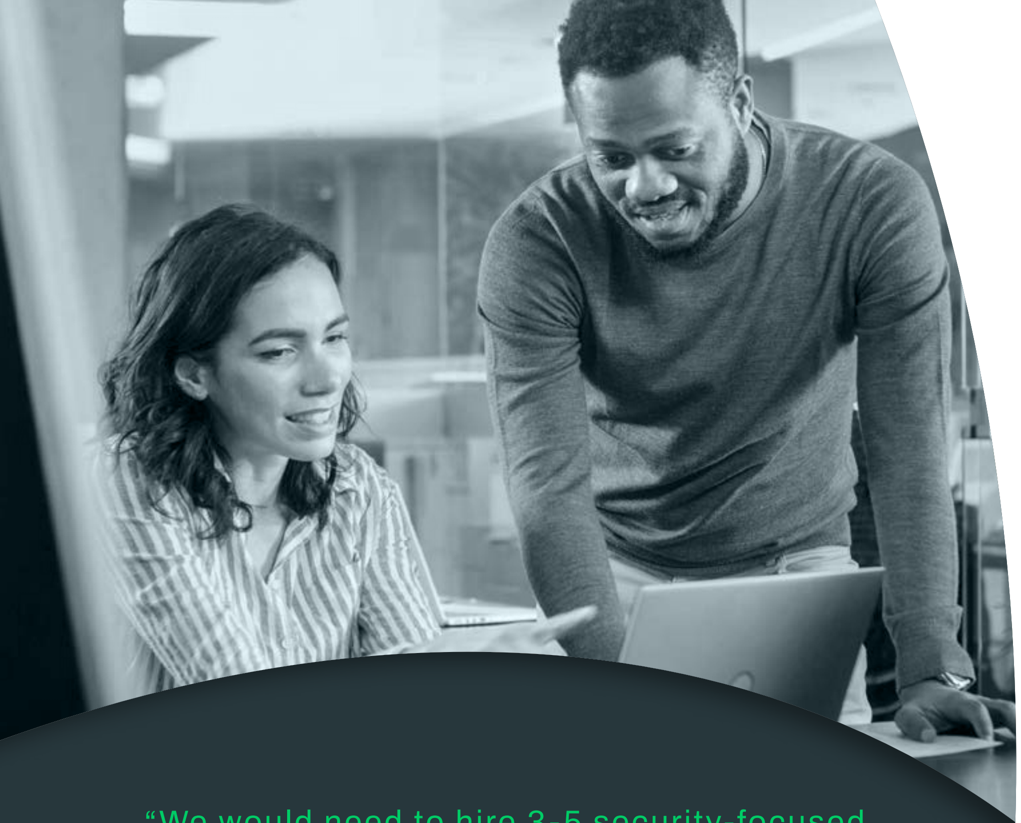
It's time to rethink alert management using a more intelligent approach, using correlations based on threat activity related to a given entity (assets and identity), enriched with contextual data.

> "We cannot solve our problems with the same thinking we used when we created them."
>
> – Albert Einstein

In order to reduce the volume of alerts while improving threat detection, a better approach to alert management should include the following:

- Data sources monitored should be prioritized based on asset critically.
- Alerts should be correlated with other detected anomalous activity.
- Alerts from multiple sources should be normalized in order to build a better understanding of risk over time.
- Low and medium severity alerts, and low-fidelity "informational" alerts should be used for better correlation and behavioral analytics and not discarded.

In addition, automated rapid response should be implemented for high risk alerts.



“We would need to hire 3-5 security-focused professionals to work overnight/in different time zones and try to keep them employed... in this career landscape where security professionals are burning out/leaving jobs in a few months”

John Woods
Global CISO at RJ O’Brien

Partnering with a managed security service provider can help alleviate some of the concerns with in-sourcing. However, not all managed security partners are created equal.

Rethinking **Security Operations**

There are several metrics to consider when deciding whether to maintain your own in-house security operations team or to outsource, as well as pros and cons to consider. The total number of employees needed is a key factor. In addition to headcount cost, additional recruiting and training costs must be considered. The average security staff turnover rate is 20%, so recruiting will be an ongoing activity.

Pros include keeping talent in house, with career growth opportunities for your staff. You have the ability to customize all the workflows and processes and procedures that may be needed.

On the flip side, building and maintaining in-house security operations means that certain areas of expertise are subject to the talent pool that is available in a given geography. You are also faced with personnel management issues, turnover, and continuing education

The Benefits of **Outsourced Monitoring** (MDR)

A recent Gartner study about managed security services highlighted that close to 90% of organizations looking to outsource at least some aspect of security will focus on detection and response services. Managed detection and response (MDR) is an outsourced service that provides organizations and security teams with additional resources and capabilities for threat hunting, advanced detection, and effective response and mitigation to threats. The most effective MDR providers act as an extension of an organization's internal team, providing value through technology management (i.e. managed SIEM and firewall) and 24/7/365 alert monitoring, validation, and escalation.

Working with MDR partner contributes to positive security and business outcomes:

- 360˚ visibility across endpoint, network and cloud
- 24/7/365 monitoring with a team of experts who augment your team
- Strengthen the ability to detect and respond to advanced threats
- Increase the value from existing security investments and tools
- Improve the efficacy of security operations

Take control of your alerts with Deepwatch MDR

Built on the Deepwatch SecOps Platform, Deepwatch MDR offerings benefit from platform capabilities including curated threat intelligence by customer industry, advanced threat analytics, malware analysis and machine learning to identify threats which evade detection tools.

Threat analytics is a dynamic alert correlation technology that normalizes all alerts from multiple technology types into a single Risk Object. Correlation across every transaction generates Threat Probability Value (TPV). All low and medium severity alerts aren't discarded but additional context on suspicious but non-alertable activity is preserved e.g. increased auth/ web activity.

Only the alerts that exceed the threshold of customer acceptable risk tolerance are escalated.

Deepwatch Threat Analytics and Threat Probability Value (TPV)

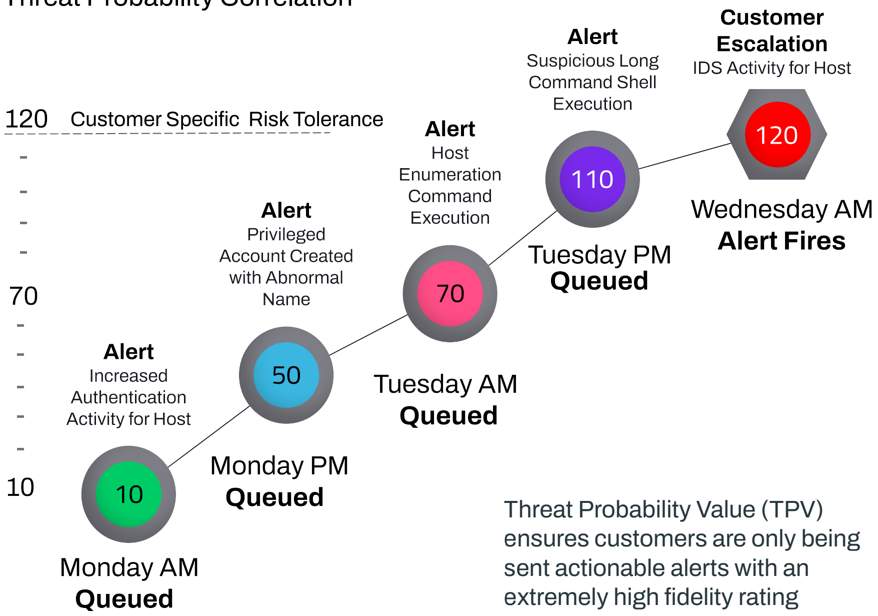
- Correlation of every transaction across an enterprise to generate a Deepwatch Threat Probability Value (TPV)
- TPV is a framework that allows for advanced correlation & enables dynamic assignment of risk values to every alert
- Alert generation is based on minimum risk value which is very closely tied to rule severity
- Customers see a drastic reduction of low/medium severity alerts while identifying high & critical threats 10x faster

98% reduction in alerts

This approach has proven to **reduce the number of alerts** in our customers' environments by over **98%**.

Platform: Threat Analytics

Threat Probability Correlation



120 Customer Specific Risk Tolerance

70

10

Alert
Increased Authentication Activity for Host

Monday AM
Queued

10

Alert
Privileged Account Created with Abnormal Name

Monday PM
Queued

50

Alert
Host Enumeration Command Execution

Tuesday AM
Queued

70

Alert
Suspicious Long Command Shell Execution

Tuesday PM
Queued

110

Customer Escalation
IDS Activity for Host

Wednesday AM
Alert Fires

120

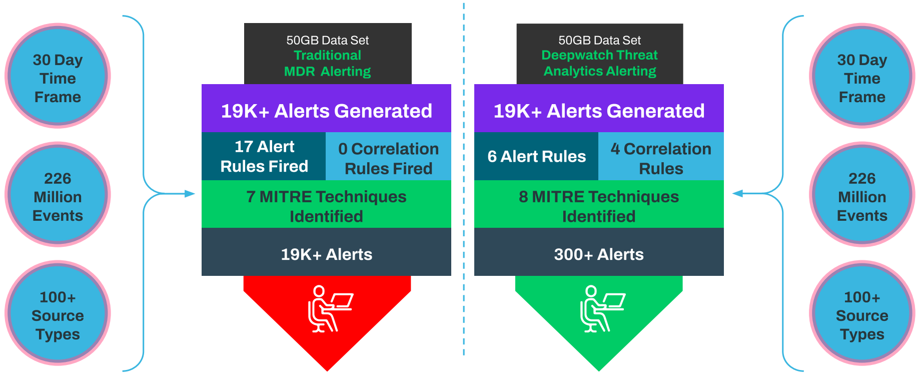
Threat Probability Value (TPV) ensures customers are only being sent actionable alerts with an extremely high fidelity rating

From **19k** down to **300 alerts**

Third-party testing proved that Deepwatch Threat Analytics technology was able to **reduce the number of alerts from 19K alerts** that a typical SIEM based MDR will report **down to mere 300.**

Platform: Threat Analytics

Outcomes



30 Day Time Frame

226 Million Events

100+ Source Types

50GB Data Set
Traditional MDR Alerting

19K+ Alerts Generated

17 Alert Rules Fired

0 Correlation Rules Fired

7 MITRE Techniques Identified

19K+ Alerts

50GB Data Set
Deepwatch Threat Analytics Alerting

19K+ Alerts Generated

6 Alert Rules

4 Correlation Rules

8 MITRE Techniques Identified

300+ Alerts

30 Day Time Frame

226 Million Events

100+ Source Types

deepwatch

ABOUT DEEPWATCH

Deepwatch helps secure the digital economy by protecting and defending enterprise networks, everywhere, every day. Deepwatch leverages its highly automated cloud-based SOC platform backed by a world class team of experts who monitor, detect, and respond to threats on customers' digital assets 24/7/365. Deepwatch extends security teams and proactively improves cybersecurity posture via its Squad delivery and patented Security Maturity Model. Many of the world's leading brands rely on Deepwatch's managed detection and response security.

Visit www.deepwatch.com or reach out to us at sales@deepwatch.com.

Conclusion

Alert fatigue resulting from alert overload is a clear signal that something needs to change. Traditional SIEM alert management met the needs of security information teams in the past. However, experience from the past decade has shown us that that approach is not scalable given the sheer volume of alerts that organizations see daily due to an expanded attack surface, growth in number of security tools used, shift to the cloud and cybersecurity skills shortage.

The solution lies in rethinking alert management and rethinking security operations. By partnering with an MDR vendor that has advanced correlation technology beyond the "alert everything" approach used by most managed security providers, organizations can reduce the alert fatigue plaguing their security team. By using correlations based on threat activity related to a given entity (assets and identity), enriched with contextual data, organizations can significantly improve threat detection while decreasing the volume of alerts.

To learn more about how Deepwatch can help improve threat detection while decreasing alert volume, visit **www.deepwatch.com**.

SOURCES

1. Analysis of attack surface (2021)
2. The Rise of Extended Detection and Response, Technology & Business Insight, 2021.
3. Alert Fatigue: 31.9% of IT Security Professionals Ignore Alerts, Cloud Security Alliance, 2017
4. 2020 State of Security Operations study from Forrester Consulting