WHITE PAPER

Information Overload: Making Sense of Security Data

Inefficiencies Increase While Risk Grows

Executive Summary

Time to response is a critical metric in determining the severity of a cybersecurity incident. The longer threats remain undetected and uncontained on an organization's network, so does the likelihood that their effects will be more damaging and costlier on the organization.

However, security teams face three major challenges that limit rapid and effective incident response. First, the vast amount of security data, and in particular alerts, makes it difficult to understand and prioritize threats. Second, the cybersecurity skills gap means that security leaders often lack the right talent to address that alert volume and make effective response decisions. Third, the need to demonstrate compliance with numerous data protection regulations diverts the security team's focus from identifying and responding to potential threats.

Nevertheless, as security leaders are measured both on their ability to contain cybersecurity risk and to demonstrate that they are doing so, they must prioritize overcoming these hurdles.

While an analyst can realistically investigate 20 to 25 alerts in a standard workday,[1] the average organization's SOC receives over 10,000.[2]

Introduction: When the Security Data Trove Becomes a Liability

Security teams operate in a highly asymmetrical threat landscape. For an organization to be secure, the security team must be able to identify and remediate every potential attack vector that could grant access to the network or allow the theft of its information. On the other hand, an attacker may only need to identify and exploit a single vulnerability in order to launch an attack or exfiltrate sensitive data.

This asymmetry means that security incidents and data breaches have become inevitable. Over the past year, 81% of security executives experienced at least one intrusion.[3] In the same time frame, 58% of firms admit that data has been exfiltrated from their networks.[4] Exfiltration of data can be performed in a matter of minutes, making rapid incident detection and response critical.[5]

As organizations mature in security awareness, strategy, and tactics, they focus on collecting the data needed by their security teams to make informed decisions (and take mitigating actions) about potential threats. By strategically deploying security devices and software solutions throughout the network, organizations provide the security team with both a range of controls and rich sources of data regarding activity across their organization and potential attack surface.

Because digital innovation expands the network attack surface, companies are deploying more security controls, which further increases the total volume of security data generated. At the same time, cybersecurity threats keep accelerating in quantity and are becoming even more sophisticated. Consequently, individual security devices collect more (and more kinds of) data than they did in the past, both to assist in threat detection and to enable a more detailed audit trail to support any potential response activities. The result of both these trends is that the sheer volume of security data makes its effective utilization extraordinarily difficult.

Compounding the effects of the information overload is a persistent cybersecurity skills shortage and the additional burden of regulatory compliance, which drains the already meager resources dedicated to threat detection and response.

Information Overload Impedes Threat Prioritization

When faced with an alert from security devices or software, security analysts need context in order to determine if the alert is a genuine threat or a false positive. To achieve this, they may need to collect and assimilate data siloed in multiple devices or tools.

On average, an analyst can realistically investigate 20 to 25 alerts in a standard workday.[6] However, the average organization's security operations center (SOC) receives over 10,000 alerts per day, and the biggest organizations can see over 150,000.[7]

Most organizations do not have security teams large enough to keep up with the number of alerts that they see every day. Nearly 40% of security leaders list missing malware and attacks as a top challenge.[8] This makes a lot of sense, considering that it takes an average of 4.35 days for a security team to resolve a security incident.[9]

The volume of alerts that the average security team sees means that many alerts must be ignored. In fact, overwhelmed security analysts often address only 10% of security alerts.[10] Even worse, 38% of security operations teams turn off high-volume alerting features,[11] leaving the organization vulnerable to attack.

With the growing risk posed by the evolving cyber-threat landscape, this practice of ignoring alerts is an unsustainable approach to security. A single alert may mean the difference between detecting a major incident and missing it entirely. While some security incidents may be difficult or impossible to stop, most are preventable or at least containable if the security team is looking in the right place at the right time. In order to be effective, security teams need more efficient means of triaging and investigating alerts that enables them to keep up with the deluge of security data.

Too Little Cyber Talent to Go Around

Theoretically, organizations could deal with the number of security alerts that they face if they had access to an infinite pool of security talent. However, the growing cybersecurity skills gap means that most organizations simply cannot acquire the cybersecurity talent that they need.

In 2018 over 2.9 million cybersecurity positions remained unfilled globally, and this number is only expected to grow.[14] One report reveals that 80% of organizations do not have enough security analysts to run their SOC.[15] It is no surprise that 59% of cybersecurity professionals indicate their organizations are at risk due to the lack of cybersecurity talent.[16] One source of concern is that other IT staff cannot easily step into the cybersecurity roles. Accurately differentiating between a true incident and a false positive can require extensive knowledge and experience, as sophisticated threat actors specialize in "low and slow" attacks that hide among false-positive alerts.

The cybersecurity skills gap is exacerbated by the fact that many organizations rely on manual processes for alert triage and remediation, which is a top concern for 57% of security executives.[17] Manual processes lead to long incident response times, which dramatically increase their organizations' risk posture.[18]

Compliance and Reporting Add to the Burden

Beyond the challenges of performing incident investigation and response, security teams are also responsible for demonstrating compliance with an increasing number of security regulations. The EU's General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS) are only two of many such data protection regulations.

Overwhelmed security analysts often address only 10% of security alerts.[12] Even worse, 38% of security operations teams turn off high-volume alerting features altogether.[13]

Only 28% of companies have an adequate level of cybersecurity staffing.[19]

Nearly half of cybersecurity professionals say that the skills shortage has resulted in an inability to fully learn or utilize some security technologies to their full potential. [20]

The challenges posed by these regulations are twofold. First, quarterly and annual auditing requires security teams to generate and collect detailed data demonstrating how their security controls meet a given regulation's requirements. This often involves mapping the general regulatory requirements to specific security controls on the company's network, and then gathering the data pertaining to those controls.

Second, mandatory breach reporting puts acute time pressures on the security team. For example, the GDPR requires an organization to report a data breach within 72 hours of its discovery. An accurate report requires a comprehensive investigation prior to the deadline. Each regulation has different reporting requirements and regulatory authorities, which can make manual breach notifications a complicated and time-consuming process.

Because of their legal and potentially material financial implications, compliance tasks often trump the day-to-day work of the security team. Any time spent researching a particular regulation, mapping security controls to regulatory requirements, and demonstrating compliance with the regulation takes away from the team's ability to identify and respond to security incidents.

The number and complexity of these regulations continue to grow. An organization may be responsible for compliance with regulations in every jurisdiction where it operates, and the growing list of state, national, regional, and industry-specific regulations makes achieving and maintaining compliance increasingly difficult.

Microsoft had 1,600 engineers working to achieve GDPR compliance.[21]

Conclusion

Security teams within most organizations are overworked and understaffed. As the cyber-threat landscape continues to accelerate in both volume and complexity, most security teams will struggle to detect and respond to the threats facing their organization until well after damage is done, while being required to keep pace in demonstrating compliance with ever-changing regulations.

Integration and automation of security information and event management (SIEM) can go a long way to prioritizing alerts and simplifying incident response, alleviating many of the other burdens discussed here. A key concern for security leaders, however, is the degree to which these functions, and the tasks in support of them, may be handed over to automated processes and systems. Although the answer depends on the nature of each organization and risk appetite of its leadership, security leaders must begin to leverage the capabilities of automation and other AI-driven innovations to shift the balance of network security in their favor.

[1] Moazzam Khan, "Security Analysts Are Overworked, Understaffed and Overwhelmed—Here's How AI Can Help," SecurityIntelligence, July 13, 2018.

[2] "How Many Daily Cybersecurity Alerts does the SOC Really Receive?" Bricata Blog, October 2, 2018.

[3] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[4] Patrick Spencer, "Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study," Scalar Security Blog, February 20, 2019.

[5] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[6] Moazzam Khan, "Security Analysts Are Overworked, Understaffed and Overwhelmed—Here's How AI Can Help," SecurityIntelligence, July 13, 2018.

[7] "How Many Daily Cybersecurity Alerts does the SOC Really Receive?" Bricata Blog, October 2, 2018.

[8] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[9] Kelly Jackson Higgins, "The SOC Gets a Makeover," Dark Reading, September 6, 2018.

[10] Roselle Safran and Utpal Desai, "Security Analysts Are Only Human," Dark Reading, February 21, 2019.

[11] DH Kass, "SOC Analysts Overwhelmed by Alerts, New Study Finds," MSSP Alert, September 2, 2019.

[12] Roselle Safran and Utpal Desai, "Security Analysts Are Only Human," Dark Reading, February 21, 2019.

[13] DH Kass, "SOC Analysts Overwhelmed by Alerts, New Study Finds," MSSP Alert, September 2, 2019.

[14] "Cybersecurity Workforce Study," (ISC)^2, 2018.

[15] Kelly Jackson Higgins, "The SOC Gets a Makeover," Dark Reading, September 6, 2018.

[16] "Cybersecurity Workforce Study," (ISC)^2, 2018.

[17] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[18] Patrick Spencer, "Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study," Scalar Security Blog, February 20, 2019.

[19] "Cybersecurity Workforce Study," (ISC)^2, 2018.

[20] Jon Oltsik, "The Life and Times of Cybersecurity Professionals 2018," ESG and ISSA, April 2019.

[21] Julie Brill, "Microsoft's commitment to GDPR, privacy and putting customers in control of their own data," Microsoft Blog, May 21, 2018.

October 18, 2019 8:59 AM

D:\Fortinet\Work\2019\October\1011819\wp-information-overload-security-data