Secureworks®

WHITE PAPER

THE CLOCK IS ALWAYS TICKING: 24/7 CYBERSECURITY MONITORING TAKES ITS TOLL

Alleviate the Challenges of Around-the-Clock Cybersecurity

It's an unfortunate fact that cybersecurity attacks never take a break. The volume of malicious activity from a global network of threat actors means that 24/7 monitoring is mandatory for cybersecurity teams.

According to the PsyberResilience Project, "more than 700,000 professionals that make up America's cybersecurity workforce are increasingly being described as our digital-first responders—a first and unflinching line of defense against an unrelenting wave of cyberattacks against businesses, governments, and entire communities."[1]

Even with an ideal team and schedule in place, this intense level of monitoring for high- risk situations takes its toll on employees and can quickly lead to burnout, opening the door for human error in a threat detection environment, which leaves organizations vulnerable to risk.

Just as importantly, it leads to the possibility of losing strong employees and disrupting a cohesive security team due to workload creep, which can negatively impact the efficacy of a cybersecurity program and potentially lead to highly qualified security practitioners leaving the field altogether. A Forrester study found that 51% of cybersecurity professionals experienced extreme stress or burnout, with 65% saying they had considered leaving their job because of job stress.[2] Additionally, an ESG study discovered that 60% agree that a cybersecurity career can be taxing on one's work/life balance, and 38% agree that they often feel an unhealthy level of stress with their jobs.[3]

This paper will explore the issue of increasing demands on security practitioners and offer several avenues for automating and reducing workloads for team members, allowing them to work more efficiently and effectively to mitigate risk.

65% of cybersecurity professionals say they considered leaving their job because of job stress.[2]

38% of cybersecurity professionals agree they often feel an unhealthy level of stress with their jobs.[3]

[1] 10 Top Reasons for Cybersecurity Professional Burnout

[2] Forrester: Predictions 2022: Cybersecurity, Risk, and Privacy

[3] ESG Research Report, The Life and Times of Cybersecurity Professionals 2021, Volume V

A CLOSER LOOK AT THE DEMANDS PLACED ON CYBERSECURITY TEAMS

Starting with an honest account of the myriad demands placed on cybersecurity teams is an important first step. A successful cybersecurity program and team strives to balance the proactive tuning and management of existing platforms with incident response and steady state operations.

In order to achieve this, cybersecurity teams must handle the following challenges:

PROACTIVE VS. REACTIVE APPROACH

For many practitioners, security efficacy is not a point-in-time evaluation – new threats are developing and new responses are constantly deployed, requiring that practitioners attempt to maintain a proactive position on ensuring readiness and evaluating risk. They must also take a regressive approach, based on new information, of how to mitigate threats and look back at their environment to see if they've been compromised. This is the primary balancing act of those in the security position: an iterative approach that strikes a fine balance between offense and defense, with consideration for regression analysis and mitigation.

INCIDENT RESPONSE

In addition to monitoring and mitigating incidents, security teams must evaluate risks while providing the best protection possible for business assets. Business units outside of the realm of security, such as compliance officers, may put demands on the security team for audits and change controls, and professionals must be ready to deliver that information while at the same time dealing with the actual compromise. Meanwhile, they also need to document regulations, requirements, and more.

STEADY STATE

When maintaining a steady state, organizations face challenges that include the level of risk to the organization, the availability of funding, and any potential compliance requirements or regulations. For example, in the government sector, organizations need to adhere to government criteria and compliance requirements such as HIPAA and may need to evaluate exposure level based on those requirements. In this example, exposure is very great if personal information is revealed. No matter the cost, they need to invest in the people, tools, and processes to mitigate this exposure.

OUTSIDE INFLUENCES

The rapid shift to remote working in 2020 increased pressure on security teams. A lot of attention in this situation is focused on making tools available to employees to ensure they can continue doing their jobs uninterrupted and having a sound infrastructure to support access to the tools they need to maintain productivity.

However, confidentiality and integrity of information must also be considered on equal footing with availability; most remote workers don't reside in a location that will maintain confidentiality for information, and organizations may not have given as much concern to credentials for particular kinds of information or policies around external devices such as USBs and printers that could leave information vulnerable.

Some organizations have remained fully remote, while others have adopted a hybrid staffing model. These organizations should continue to analyze if there are any differences in monitoring the remote aspects of their infrastructure. They must ask themselves if there needs to be a deeper analysis of environments that the security team wasn't able to monitor during the remote period, which will create additional demands for the security team.

THE TOLL ON TEAMS

For most global organizations, there are no off-hours. There was a time when workforce management would have an ebb and flow, even if 24/7 monitoring was in place. Now as businesses – and threat actors – become more global, that is no longer the case, and teams are running at full speed year-round.

UNRELENTING THREAT VOLUME

As a result of this new normal, the sheer volume of alerts can contribute to team fatigue. Teams have no time to pause due to the unceasing wave of attacks - some organizations end up ignoring an estimated 30 percent of alerts due to excessive alert volume.[4]

LACK OF SINGLE PANE OF GLASS

In addition, customers want to focus on only the critical threats that have the highest risk to business and information assets. But there is no single pane of glass to be able to do this, so security practitioners use a conglomerate of tools that need to be leveraged to assess for high risk and high severity. Practitioners use these tools and processes in conjunction with their own experience, which requires continuous learning and development.

PROCESSES

Maintaining processes also contributes to burnout with its own set of stressors. Depending on the tools in place to document findings and follow through on actions, it may be confusing and time-consuming to ensure proper processes in the absence of a robust ticketing system.

[4] IDC, "In Cybersecurity, Every Alert Matters" Thought Leadership White Paper, October 2021

INTERDEPENDENCE

It's important to consider that security operations don't exist within a vacuum. Most businesses tend to separate infrastructure management and information security. The individuals responsible for maintenance and hardening of the information asset itself are not necessarily in the same organization or group as those responsible for providing security. When determining whether an agent can be deployed for incident response or steady state on a physical asset, it's not the individual working in the security space who will make that decision – it may be IT or IT services, which has its own chain of command and requirements. The security team relinquishes some control in these situations which can create delays and other issues.

"DIY" SECURITY PRESSURE

There is also a tremendous amount of pressure on organizations, due to budgets and data privacy demands, to maintain their entire security program in house. It can be very difficult for practitioners to understand from the inside which low-severity incidents may lead to a high-severity compromise and adjust workloads to focus on the key items putting the business at risk.

TECHNOLOGY AVAILABLE TO HELP

The good news is that there is help for security practitioners in the form of several technologies and accompanying services provided by cybersecurity vendors. These include:

XDR

Extended detection and response, commonly known as XDR, has become prevalent in the market as the next step from traditional managed security services. XDR is based on a SaaS-based platform that delivers security threat prevention, detection, and response. XDR platforms integrate with numerous types of security technologies, including endpoints, network, cloud, and other systems. Telemetry from these point solutions is pulled into a centralized location, where machine learning and curated threat intelligence are used to detect malicious activity and alert a customer's security staff.

MDR

A software product may not be enough for many organizations, who lack the staff, expertise, and time to get the most out of that type of solution. That's where managed detection and response, commonly known as MDR, comes in to provide the people power and expert human insights many organizations don't possess. MDR marries machine learning and advanced technologies of SaaS platforms with a robust, experienced team of security operations experts. Security analysts investigate, triage, and escalate alerts, plus incident response personnel are available for serious issues, and threat hunters proactively scour a customer's environment.

COLLECTIVE INTELLIGENCE

In a dynamic environment, we must consider both primacy (historical trends) and recency (new toolkits, root sets, etc.). Third-party cybersecurity experts are able to offer unmatched perspective on types of threat activity and solutions based on their years of experience with a diverse customer base. Leveraging the collective intelligence of a third-party expert allows for a holistic view of threats to the organization from the outside-in, which can then be layered with perspective on how the issue can be best solved based on their experiences with other organizations. This helps reduce workloads and provides greater insight that may otherwise be missed internally.

Because attacks are always occurring, a 24x7 cybersecurity approach is now mandatory. This is creating enormous pressure on cybersecurity practitioners who are reporting rising stress levels that are leading to an increasingly negative impact on mental health.[5] And there isn't relief coming soon, considering the global shortage of cybersecurity personnel is estimated at 2.72 million.[6]

60% of respondents agree that a cybersecurity career can be taxing on one's work/life balance.[5]

2.72M global shortage of cybersecurity personnel.[6]

Fortunately, there is help available from third-party vendors that will decrease workloads and streamline the efficiency of overburdened security teams, including XDR, MDR, and leaning into the collective intelligence of the industry itself.

Empowering security teams with outside perspectives and support will enable them to approach their work with new insights and energy, which will help create a more balanced workplace while further mitigating risk to the business.

[5] ESG Research Report, The Life and Times of Cybersecurity Professionals 2021, Volume V

[6] (ISC)² Cybersecurity Workforce Study, 2021

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