Secureworks®

WHITE PAPER

How Secureworks Addresses Top Cybersecurity and IT Analyst Challenges

On the front lines of protecting companies, cybersecurity practitioners maintain a crucial role. Adversaries constantly seek to exploit weaknesses in the company infrastructure, repurposing malware and introducing new avenues of exploitation. Analysts work long hours under constant pressure to shield the business from these constantly evolving attack vectors.

Security analysts, as the last line of defense, continually strive to detect, prevent, and respond to incidents to protect business assets. Analysts must be well supported with the most current tools, information, and processes. In this way they can apply their skills to maximum effect.

Secureworks understands the challenges security practitioners face. As a partner to over 4,000 companies and by extension, tens of thousands of security analysts, we have a deep understanding of the daily frustrations and obstacles to success analysts must navigate. The most consequential obstacles fall under three common groupings.

83%

of businesses around the world believe they are most at risk because of organizational complexities.[1]

1. Increased Complexity of Company Infrastructure

Cybersecurity practitioners are tasked with defending a company environment that continually gains in complexity. Sensitive data is spread across individual devices, cloud, and on-premise servers. According to Ponemon Institute research, 83% of businesses around the world believe they are most at risk because of organizational complexities.[1]

Additionally, new technologies layered upon legacy systems can create security gaps that allow threats to dwell for hundreds of days. Continuous monitoring of these security systems is essential to balance threat prevention and detection. But even as companies procure new security tools, there is exponentially more data to process from year to year. 24x7 monitoring can stretch even the most committed IT and security teams.

Companies also find that aggregating various tools from multiple vendors creates complications when it comes to normalizing indicators of compromise for behavioral analytics. With each vendor classifying uniquely for threats and countermeasures, association of these threats is challenging. The result: More time is spent on detection than prevention.

Secureworks simplifies this complexity with a full suite of solutions and services that protects your business from endpoint to network and within the cloud. Our Red Cloak™ Threat Detection and Response (TDR) security analytics software uses machine learning to apply our threat intelligence to your telemetry to help you detect and eradicate advanced threats. Our Managed Detection and Response (MDR) powered by Red Cloak™ service offers all the benefits of Red Cloak TDR with our expert analysts operating the software. Both these solutions offer a fully connected, correlated monitoring environment with immediate contextual information and the choice to automate containment actions.

[1] Ponemon Institute, The Need for a New IT Security Architecture

For organizations with security investments that need optimizing, Secureworks offers orchestration and automation capabilities that harmonize disparate parts of the security stack. With everything working in concert, security practitioners have all the information they need to make sound decisions.

2. Limited Resources

Most security teams perform their jobs with limited resources at hand. With the global cybersecurity workforce gap estimated at over 4 million and the U.S. shortage over 500,000, many companies lack the security headcount they really need.[2] With top talent demanding top dollar in the market, companies often struggle to hire the right expertise and the required depth of experience. In addition, the top talent is in high demand so can be tough to retain.

Security teams are making decisions based on limited information. Any team only has access to their own environment, plus whatever information their peers share at CISO forums or industry events. Security practitioners are mostly only exposed to the experiences of friends and former colleagues in different companies, and sometimes through channels online. This means they may not always know the impact of a potential threat or how to handle it, despite the need to immediately respond.

Budget constraints are always a factor in why security teams often opt to use free threat intelligence available on the open market. Such a practice can lead teams down the wrong path. It's hard to validate the quality of free threat intelligence, not to mention that advanced threat actors often monitor free threat intelligence so they can see when they need to adjust their attack vectors.

Secureworks helps company resources go further with fully managed services to complement and augment your security teams. Our MDR offering includes security analytics software, 24x7 support, threat hunting, and incident response in a single solution. Secureworks has multiple security operations centers around the globe, which allows us to provide expert protection around the clock.

With limited staff, each business must assess which security events they trust automation to handle, and which events need expert attention. Secureworks works with companies to understand their security teams' levels of expertise and skill to arrive at the escalation model that works best for their capabilities. At the same time, we offer mentorship and training so together we arrive at the best solution for the incident at hand and your team can learn from each experience. For TDR and MDR customers, your team has access to a chat box in the software which gives access to our experts 24x7. Analysts can use the box to ask advice, validate their conclusions and any other security concern they might have.

Budget constraints are always a factor in why security teams often opt to use free threat intelligence available on the open market.

[2] (ISC)2, (ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide

Working with Secureworks ensures your company will realize the benefit of our more than 20 years of experience in the security industry, and our proprietary threat intelligence applied to your environment using supervised machine learning techniques. This combination of human and machine intelligence protects your business and helps your operation evolve.

3. Limited Time

Many security analysts deal with a high volume of alerts, many of which require manual investigation. Organizations that can't process this workload have no choice but to ignore a considerable portion of alerts. One survey found that 42% of cybersecurity professionals said their organization ignores a significant number of security alerts because they can't keep up with the volume.[3] Other research reveals that up to 25% of an analyst's time is spent chasing false positives.[4]

Time spent investigating inconsequential alerts would be better spent on more proactive activities that would help improve the organization's security posture. With too many benign alerts demanding their attention, practitioners risk missing truly credible alerts that represent actual intrusions.

In addition to managing the volume of alerts for analysis, security practitioners are also expected to respond immediately to alerts for the protection of organizational assets. This often means analysts are forced to make rushed decisions, or inform management based on initial reports that later investigation reveals is inaccurate.

Secureworks helps analysts manage and reduce time pressure with our Red Cloak TDR security analytics software and MDR services, which employ advanced behavioral analytics and integrated threat intelligence to escalate only the alerts that matter. When Secureworks escalates a threat to your team, our experts have already investigated and verified its severity. For customers who use Red Cloak TDR in-house, the software will alert you to suspicious activity that needs attention, while also allowing you to prioritize your investigation and response based on level of criticality.

42%

of cybersecurity professionals said their organization ignores a significant number of security alerts because they can't keep up with the volume.[3]

Our Offerings in Detail

Secureworks offers the full spectrum of services and solutions for companies of all sizes. First-rate threat intelligence based on more than 20 years in the industry assures practitioners they are getting the best threat information from experts who can provide rich context around each critical alert. Managed services assist companies in need of top tier expertise and support from dedicated cybersecurity specialists. Scalable software solutions enable companies with adequate staff resourcing to leverage Secureworks' advanced analytics and machine learning techniques.

[3] ESG, Dealing with Overwhelming Volumes of Security Alerts

[4] Security Boulevard, Every Hour SOCs Run, 15 Minutes Are Wasted on False Positives

Secureworks®

Threat Intelligence

Producing accurate, timely intelligence is difficult. Real threat insight comes from meticulous analysis of network and host data types, adversary tools, direct observation of intrusions, as well as attempting to understand the economic and geo-political perspective of the adversary. At Secureworks, we believe threat intelligence must be accurate, in context, and immediate.

Accuracy: Precision is paramount. Security teams need to be able to trust that the alerts they receive are truly impactful, and not a waste of already-stretched time and resources.

Context: Good threat intelligence is more than just producing a hash/IP address/domain. The right data combined with expert analysis provides predictive information about the adversary, such as how they will gain access, pivot within the compromised network, and exfiltrate data. Our broad customer base affords us visibility into threats across the landscape and in specific verticals. This comprehensive view, combined with our constant tracking of threat groups and malware families, enables us to provide our customers context for where else a threat has been seen, whether it's a historical threat or new, how it was developed and by who, and more.

Immediacy: Our Counter Threat Unit™ (CTU) is comprised of over 70 expert researchers who use a wide variety of commercial and proprietary tool sets to produce, analyze, and validate threat intelligence. Their latest findings are quickly applied to security device signatures and policies, attacker blacklists, event correlation, threat analysis, and response procedures. These experts constantly track 135 threat groups and manage and update over 52,000 unique threat indicators daily.

The experts in our CTU author their own countermeasures, which move from research to production with zero latency, in the blink of an eye. These countermeasures are productized and used by analysts in making assessments for vulnerabilities Secureworks customers might face. That means by the time a threat has hit the mainstream media, Secureworks customers are already protected from it.

Managed Services

For companies who need more support, Secureworks security analysts are available to serve as an extension of your team to monitor and detect threats across your environment.

Secureworks offers advanced MDR built on the powerful Red Cloak TDR security analytics software, 24x7 support, threat hunting, and incident response in a single solution. Our teams rapidly detect and respond to advanced threats for our customers using embedded proprietary threat intelligence to automatically correlate endpoint, network, and cloud activity, and identify which events require action. Additionally, your in-house analysts get access to the TDR software.

Our MDR service reduces adversary dwell time on your behalf. Security analytics correlate threat knowledge from our CTU researchers and incident response team to your telemetry to quickly identify stealthy threat behavior and malicious activity. Plus, our security analytics software dramatically reduces false positives, so you spend more time on what matters. Find known and unknown threats using constantly updated detection use cases and machine learning trained datasets.

Secureworks offers advanced MDR built on the powerful Red Cloak TDR security analytics software, 24x7 support, threat hunting, and incident response in a single solution.

Scalable Solutions

Secureworks has obsessively studied threat actor tactics since 1999 and to understand the hallmarks of even the stealthiest of attack techniques. We aggregate threat intelligence from activity in our base of over 4,000 customers and apply it to our solutions with minimal latency, so your organization is protected.

Red Cloak TDR uses advanced analytics technology to analyze data from your environment against our threat intelligence. If TDR detects suspicious activity, investigation is simple and collaborative to help you reach a resolution fast. When an incident requires a response, you can automate actions to contain incidents with minimal effort and maximum speed.

Our endpoint solutions enable you to protect, detect, and respond to endpoint threats, even those designed to evade traditional security controls. Our network protection solutions fortify defense capabilities throughout your network, allowing you to establish a solid fundamental security posture that guards your firewall, IDS/IPS and server technology.

Incident Response

Our accredited incident response (IR) teams help resolve complex cyber incidents at scale. We provide proactive planning in addition to rapid containment and eradication of threats. Our vast operational experience in responding to security breaches minimizes the duration and impact of an incident that threatens your sensitive customer data, patented trading algorithms, and proprietary financial services processes.

Backed by proprietary Secureworks threat intelligence and purpose-built response technologies, our global IR teams take our customers from the earliest stages of breach discovery and identification to the final stages of eviction and closure. With Secureworks, you can expedite your response, reduce impact, and thoroughly remediate to get back to business as fast as possible.

Let Secureworks Extend Your Capabilities

Every security team needs a provider that understands both the requirements of their business and the challenges of their mission. With vast experience across industries and decades helping security practitioners defend their organizations, Secureworks is that partner. We know what it's like to be on the front lines defending critical assets. With a powerful combination of AI technology, threat intelligence and global visibility across thousands of customers, Secureworks simplifies security so you can focus your time on priority initiatives that keep your organization protected.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

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
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp