

DATA SHEET

Threat Hunting Assessment

Prepare and Defend Against the Unknown Threat

Develop cyber resilience by identifying undetected threats, uncovering security control gaps, improving visibility, and reducing incident impact.

Hidden Threats and Risks

Threat actors operate undetected in organizations taking advantage of visibility gaps, misconfigured security controls, and information technologies. Detecting and finding hidden threats in your environment is cumbersome, requiring knowledge of attack patterns, skilled resources to identify and disrupt threat activity, and the right technology to conduct analysis at scale across on-premises and cloud environments. Without specifically designed intelligence, expertise, and technologies, cybersecurity personnel are unable to detect today's threats and implement effective security controls.

How Secureworks® Helps

The Secureworks Threat Hunting Assessment is a point in time 30 day comprehensive and intensive evaluation of your environment to identify unknown compromise activity and cyber threats that can evade your security controls. Our team of elite security experts brings decades of combined experience countering adversary tradecraft. This human intelligence along with our proprietary hunting technology and Secureworks advanced security analytics enables us to identify the presence of historical and active compromises entrenched within the environment.

Comprehensive Approach

Our security experts collect endpoint, network, and cloud telemetry across your environment to determine historical and active threats using a battery of hunting tools including proprietary and commercial hunting technology to scour your environment. The Secureworks hunting methodology goes beyond a simple scan of indicators of compromise in your environment. Instead, our approach is informed by over a decade of experience responding to cyber intrusions, and takes a focused, tailored approach for each engagement. The below represents the components of our methodology (Figure 1). A hunt is an iterative process.

Customer Benefits

- Build cyber resilience with focused, tailored recommendations on security architecture, instrumentation, and controls
- Reduce dwell time, increase mean time to detect and remediate threats
- Increase confidence in the confidentiality, integrity, and availability of systems and data
- Decrease the number and impact of security incidents with finding-based improvement
- Improve speed, efficiency, and accuracy of your incident response process

Enabling Response and Improvements

A Threat Hunting Assessment will help:

1. Identify Undetected Threats.

If threats are found, our experts will perform an in-depth analysis to help scope the situation and build context on the threat, including intent, opportunity and capability.

2. Discover Gaps in Security Controls.

The report supplies actionable guidance to improve your organization's information security defenses and posture against cyber threats. This guidance may address weaknesses in your information security architecture, policies, and personnel that, when implemented will help mitigate an active cyber threat or prevent similar cyber threats in the future.

3. Inform Incident Response.

Findings from the engagement can be used to inform the incident response team on current visibility gaps in your infrastructure and detection capability. Customers can use the findings to create new detection capabilities for their environments, decrease response time, and establish a baseline.

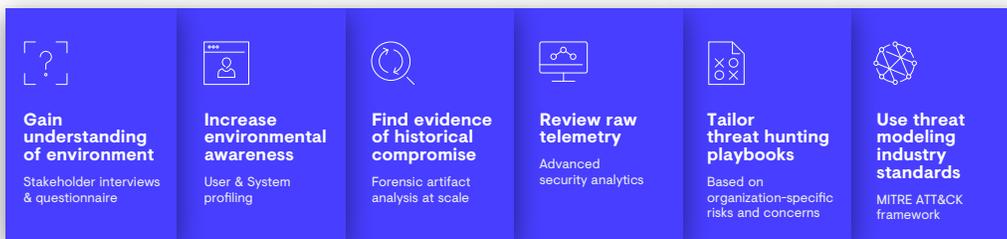


Figure 1. Components of the Secureworks Threat Hunting Methodology

About Secureworks

Secureworks® (NASDAQ: SCWX) a global cybersecurity leader, enables our customers and partners to outpace and outmaneuver adversaries with more precision, so they can rapidly adapt and respond to market forces to meet their business needs. With a unique combination of cloud-native, SaaS security platform and intelligence-driven security solutions, informed by 20+ years of threat intelligence and research, no other security platform is grounded and informed with this much real-world experience.

www.secureworks.com

Service Features

- Tailored to your organization's unique risks and concerns
- Performed by experienced, dedicated hunters backed by advanced security analytics
- Leverages endpoint, network, and cloud telemetry
- Report details visibility gaps, asset enumeration and profiling of system activity mapped to the Center for Internet Security (CIS) framework
- Quick Emergency Incident Response assistance can be provided if high-severity compromise activity is found
- Optional Attack Surface Analysis and Active Directory Assessment available



If your organization needs immediate assistance call our **Global Incident Response Hotline (24x7x365).**
+1-770-870-6343



For more information, call **1-877-838-7947** to speak to a Secureworks security specialist
secureworks.com