

Secureworks Elite Threat Hunting

A powerful add-on to Secureworks® Taegis™ solutions, Elite Threat Hunting provides ongoing proactive threat hunting and risk identification to uncover hidden threats in your environment. Partner with a designated threat hunter who gets to know your environment, meets with you every two weeks to review findings, and collaboratively explores ways to enhance your cyber resiliency and reduce your cyber risk.

Amplify Your Threat Vigilance

Elite Threat Hunting delivers comprehensive, personalized threat hunting that goes beyond the monthly threat hunting included as part of Taegis solutions. Threat hunts are based on vast research into new and emerging threats that can bypass traditional defenses, and the expertise from delivering thousands of incident response and red team engagements annually. Elite Threat Hunting takes threat hunting to a new level with a designated Secureworks resource to perform regular deep threat hunting and proactive risk identification activities throughout your environment.

Hunting goes beyond periodic ad-hoc searches and leverages our experience and insights into the global threat landscape, providing you peace of mind that hidden risks are not lurking in your environment. Discovered risks are escalated to our security analysts immediately, and your threat hunter meets with you every two weeks to talk through findings and provide guidance that improves your security posture.

CUSTOMER BENEFITS

Quickly identify elusive threats that can bypass traditional detection methods and gain a foothold in your environment

Enable threat hunting activities tailored to your unique environment and needs

Discover unknown security risks and configuration issues that expose potential attack avenues in your environment

Reduce the time a stealthy threat can dwell in your environment with continuous threat hunting activities

Enhance your organization with experienced threat hunting expertise without the challenge and expense of hiring specialized personnel

Enable proactive, continuous threat hunting for potential security risks, misconfigurations, and poor security controls, further fortifying your resilience

Elevate Your Defense Against Stealthy Threats

DEFINITION OF THREAT HUNTING

Proactive and iterative discovery of current or historical threats that evade existing security mechanisms, using that information to develop future countermeasures and increase cyber resilience.

WHAT WE DELIVER

Elite Threat Hunting focuses on swiftly responding to and stopping threats, while proactively hunting for unknown risks, allowing you to concentrate on strengthening your organization's security posture.



SECUREWORKS DIFFERENTIATORS

Knowledge fueled by decades of security insights, thousands of threat hunting engagements annually, and threat intelligence across the global threat landscape

A full team of dedicated threat hunters who understand how threat actors operate and apply that understanding to searching your environment using the latest hunting techniques

Threat hunts that encompass your entire environment, not just one particular type of technology

Elite Threat Hunting

Secureworks uses a wide variety of proven, expert-led methods to seek out stealthy threat actors:



Continuous Expert-Led Threat Hunting

Customer receives ongoing hunting activities performed by your designated Secureworks threat hunter who possesses years of expertise in threat hunting, incident response, data science, and adversary tactics.



Threat Hunting Baseline

Your designated threat hunter establishes a threat hunting baseline for your organization and works collaboratively with your staff to learn your environment and business priorities.



Proactive Risk Identification

Proactive searching for potential security risks, misconfigurations, and poor security controls, within an organization's IT environment before attackers can exploit them.



Artifact-Driven Threat Hunting

Hunting that focuses on specific artifacts, such as mailbox rules or persistent mechanisms to uncover potential threats. This type of threat hunting analyzes existing data to seek out known malicious activities.



Hypothesis-Driven Threat Hunting

Hunting activities involve forming hypotheses about potential threats based on knowledge of the environment and threat attacker behavior. Hunters design specific activities to test their hypothesis.



Threat Intelligence-Driven Threat Hunting

Hunters use indicators of compromise (IOCs) gathered by Secureworks Counter Threat Unit™ (CTU™) research team to search within the customer's environment for evidence of threat activity.



Tailored Threat Hunts

Elite Threat Hunting customers can request up to four tailored threat hunts per month, such as searching for presence of ransomware following a publicized attack.

MDR services built on the award-winning Taegis Platform

Taegis MDR	Taegis MDR Plus	Taegis MDR Enhanced	Add-Ons
<ul style="list-style-type: none"> • Taegis XDR Platform • 24/7 Triage, Investigation, & Response • 350+ Integrations • 1 Year of Data Retention • Advanced Detectors and Applied Threat Intelligence • SOAR & AI Engine • Taegis Endpoint Agent (EDR) • Unlimited Incident Response • Monthly Threat Hunts 	<p>Taegis MDR and...</p> <ul style="list-style-type: none"> • Weekly Threat Hunts • Custom Use Case Support • Custom Response Workflows • Custom Report Development • Named Taegis Support Engineer • Annual Taegis Health Check • 4 Secureworks Service Units 	<p>Taegis MDR Plus and...</p> <ul style="list-style-type: none"> • Designated 24/7 SOC Analysts • Monitored Phishing Inbox • SOC Analyst access to Customer Security Systems • Premium Governance, Reporting, and Advisory processes 	<p>Elite Threat Hunting</p> <ul style="list-style-type: none"> • Designated Threat Hunter • Hypothesis-driven Threat Hunting • Customer requested Threat Hunting • Bi-weekly Meeting <p>OT Support</p> <ul style="list-style-type: none"> • IT and OT threat monitoring, detection, investigation, & collaborative response • 24/7 rapid access to security experts and access to OT-focused experts • Integration with multiple OT toolsets <p>Secureworks Services</p> <ul style="list-style-type: none"> • Planning & Advisory Services • Testing & Validation Services • Workshops & Briefings

Secureworks® a SOPHOS company

Secureworks, a Sophos company, is a global cybersecurity leader that protects customer progress with Taegis™, an AI-native security analytics platform built on more than 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.



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