

# Targeted Threat Hunting

## Find the Unknown Threat

### Hidden Network Threats

Whether leveraging malware or existing tools in your environment to float across your network, advanced cyber threat actors are cunning; their success depends on stealth. Detecting and identifying the scope of advanced threats in your environment is cumbersome, requiring specialized resources and budget. Without specifically designed intelligence, tools and expertise, your IT security personnel may be unable to take intelligent action.

### How Secureworks Helps

The Targeted Threat Hunting service is a comprehensive and intensive investigation of your environment to identify indications of hidden adversaries. Our team of elite security experts brings decades of combined experience countering targeted adversary tradecraft.

This human intelligence along with our proprietary hunting technology arms us to identify the presence of compromises and entrenched threat actors operating in your network.

### Our Approach

Our security experts collect data from your environment and use a battery of hunting tools and proprietary hunting technology to scan your environment.

Our researchers and incident response consultants screen for threat indicators across your firewalls, DNS and proxy servers. Utilizing our proprietary Threat Intelligence, our experts may scan your endpoints such as servers, desktops, or laptops, for indicators of an adversary's presence.

When a threat is detected, our experts will perform an in-depth analysis. Leveraging our unmatched visibility into the threat landscape across 4,400 clients and The Secureworks Counter Threat Platform™, we can then build context on the threat. This context provides insights into its tools, purpose, origin and possibly the agent behind the threat.

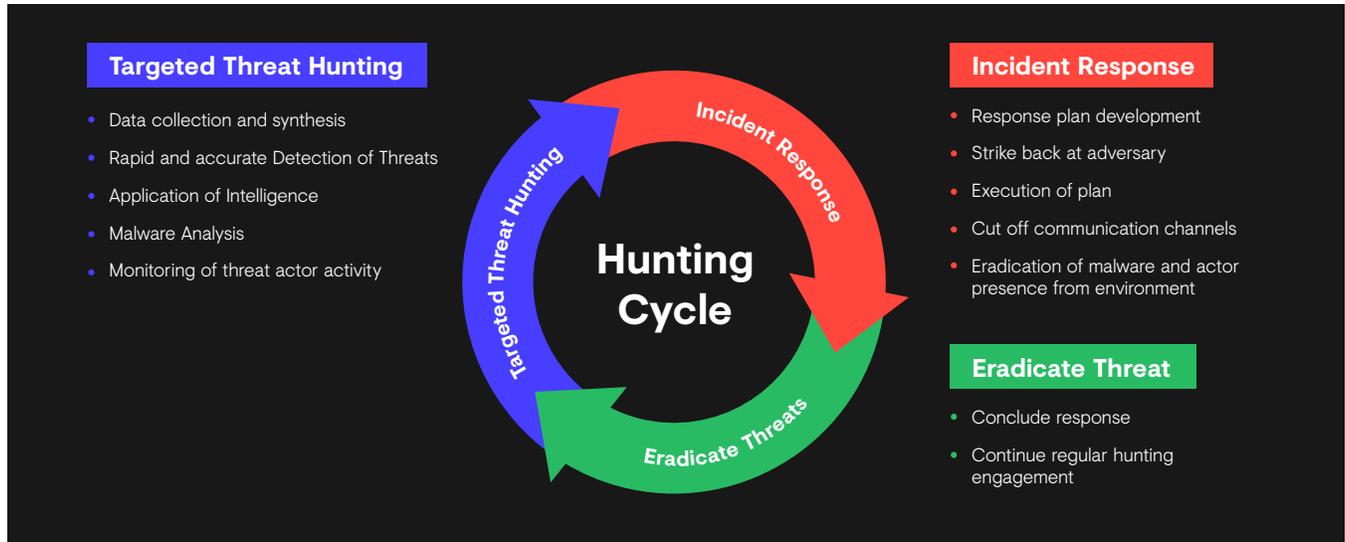
Based on investigation findings, the Secureworks researchers and incident responders will provide actionable guidance to your organization to improve your information security defenses and posture against targeted cyber threats. This guidance may address weaknesses in your information security architecture, policy and personnel that, when implemented, will help your organization predict and prevent similar IT security threats in the future.

### Client Benefits

- Determines if your environment has been compromised by a sophisticated adversary
- Increases your confidence in system integrity and data confidentiality
- Helps you understand the impact of any discovered breach
- Provides recommendations on security architecture, instrumentation and controls to make your environment more resilient
- Provides actionable guidance on next steps to respond to and eradicate the threat, offering seamless integration with Incident Response

---

**Secureworks provides end-to-end support before, during and after a security incident.**



*Targeted Threat Hunting & Incident Response*

**Incident Response**

In the event that malware or indications of a threat actor are found in your environment, the Secureworks team will provide specific guidance and recommend appropriate steps to contain and eradicate the threat actor from your environment.

**Why It Matters**

A targeted threat hunting engagement provides you:

- Unparalleled visibility and intelligence that outsmarts the adversary
- Faster recovery time that reduces impact to your organization, when a threat actor is identified
- Recommendations for enhancing the security of your network to eliminate gaps for cyber threats to enter

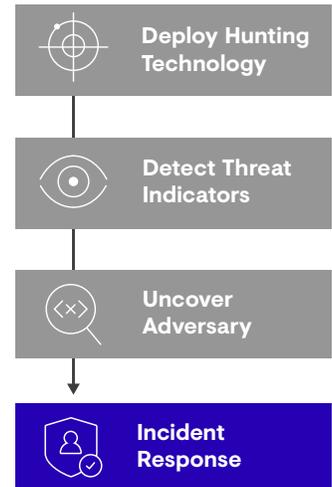
**About Secureworks**

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that keeps organizations safe in a digitally connected world. We combine visibility from thousands of clients, 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 clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

**Related Services**

Red Cloak™ is a proprietary Endpoint Detection and Response (EDR) technology invented by our Counter Threat Unit™ (CTU™) team and leveraged by our threat hunters. This technology is now available as an ongoing managed service to help identify threats that evade antivirus and other threat prevention technologies, even advanced threats or those that use little or no malware.

Our Advanced Endpoint Threat Detection (AETD) service with Red Cloak technology improves your security situational awareness by continuously monitoring your endpoints and alerting of potential compromise. AETD delivers CTU Threat Intelligence directly to the endpoint, providing valuable visibility, correlation and remediation guidance to help you determine the potential impact of a threat, while also reducing the time and effort to respond.





For more information, call **1-877-838-7947** to speak to a Secureworks security specialist. [secureworks.com](https://secureworks.com)