Secureworks®

Emergency Incident Response

Comprehensive Full-Service Incident Response Assistance – from Investigation to Recovery

Addressing urgent cybersecurity incidents requires speed, efficiency, cross-disciplinary skills, and expertise. It also requires visibility into and knowledge of an increasingly complex threat landscape, threat actors, and their evolving tactics and techniques.

During a security incident, understanding the nature, scope, and risk of the compromise is critical to inform the right, timely actions and to reduce both immediate and lasting impacts to the business. Full-service incident response focuses on understanding the cause of the incident, restoring business operations, monitoring for additional activity, and preparing for future incidents. That said, the right information, approach, resources and expertise will enable a more comprehensive response that ties recovery objectives into the response results. This will assist in the long-term improvement of your cybersecurity posture.

CUSTOMER BENEFITS

Supplement and extend your team with cross-functional incident response capabilities and expertise

Reduce impact of an incident and the risk of recurrence due to incomplete mitigation

Expand visibility, obtain facts and determine answers fast to help you and your advisors take the right actions

Why Secureworks®

Secureworks® has been responding to cybersecurity emergencies since 2007. We have extensive experience providing full-service incident response assistance to a wide range of organizations, across verticals and incident types - from small, single computer system concerns to enterprise-wide crisis situations that significantly disrupt or impede business operations.

Our seasoned incident response team leverages expertise and backgrounds spanning national, military, organizational Computer Security Incident Response Teams (CSIRTs), law enforcement and intelligence agencies. They combine hands-on understanding of key cybersecurity practices with front-line incident response, threat intelligence, and security analytics to accelerate investigations and recover with confidence.

1,400+	20+	155+	Secureworks Taegis™
IR Engagements annually	Years of producing, analyzing, and validating attack data	Threat groups monitored	SaaS-based, open XDR Platform

By our Secureworks
Counter Threat Unit™ (CTU™) research team

Secureworks Approach

Secureworks' approach is collaborative and interactive. We work with your team to quickly assess, contain, understand, and remediate the situation. Our Secureworks team provides digital forensics, malware analysis, threat intelligence, ransomware negotiation, and monitoring capabilities. Secureworks engages with numerous partners to provide recovery and hands-on remediation services, supplementing and enhancing your internal capabilities. During an incident response engagement, we use cross-disciplinary subject matter experts (e.g., penetration testers and threat researchers) and trusted partners to ensure comprehensive risk mitigation and recovery across the Incident Response lifecycle.

Secureworks Incident Response Lifecycle Actions

DETECT & INVESTIGATE

INITIAL CONTACT & INVESTIGATION

Within moments of contacting, Secureworks takes immediate action to simultaneously ensure the right next steps are followed, the correct incident responders are engaged, and the necessary resources are assigned.

Remote IR assistance is provided to capture and collect existing forensic data, start initial analysis, develop containment actions, and deploy any additional engagement technology and analytics needed to quickly expand visibility throughout your engagement.

DEEPEN INVESTIGATION

Data Capture: Assets, services affected, business impact, other attack vectors.

Iterative Forensics & Threat Analysis: Researchers, hunters, penetration testers and analysts help gain a full understanding of the threat.

Remediation Planning: Start planning for remediation, in parallel and in concert with the investigation.

Attack Surface Reduction: Secureworks Adversary Group can provide interactive threat actor insight to validate controls and identify additional re-entry points for comprehensive risk mitigation.

Ransomware Negotiation: Experienced ransomware negotiators leverage deep knowledge of ransomware threat actors to ease negotiation and offer guidance to recover data safely and in a cost-effective manner from ransomware actors.

REMEDIATE

SECURE & VALIDATE

Focused Security Hardening: The IR team guides and supports tactical security control hardening efforts that will prevent re-entry by the threat actor.

Containment: Cutting off the command and control of the threat actor.

Threat Actor Eviction: Evicting the threat actor from a contained network requires the orchestrated elimination of their tradecraft and resetting of compromised domains. Secureworks Adversary Group helps validate containment actions.

RECOVER

System and Data Recovery: To help rebuild systems, sanitize data and put systems back into production, the IR team works with trusted partners to provide recovery services seamlessly and securely.

Host Validation: Using Secureworks Taegis™ Endpoint Agent, we help ensure that restored hosts are ready for production.

Monitor for Threat Actor Re-entry and Malicious Activity: Minimize the likelihood that the threat actor does not re-compromise the environment.

FOLLOW-UP

IMPROVE

Secureworks leverages lessons learned through the thousands of engagements we have performed to guide recommended response process improvements as well as strategic recommendations to help drive a security transformation roadmap.

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

SERVICE FEATURES

- Remote and on-site technical, incident command and advisory capability
- Seasoned and accredited global incident response team experienced in common and uncommon cyber threat scenarios
- Incident-specific threat intelligence and insights into current adversary tradecraft
- Quick deployment of technologies and Secureworks security

Secureworks®

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of over 4,000 organizations around the world who use its advanced, AI-driven capabilities 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