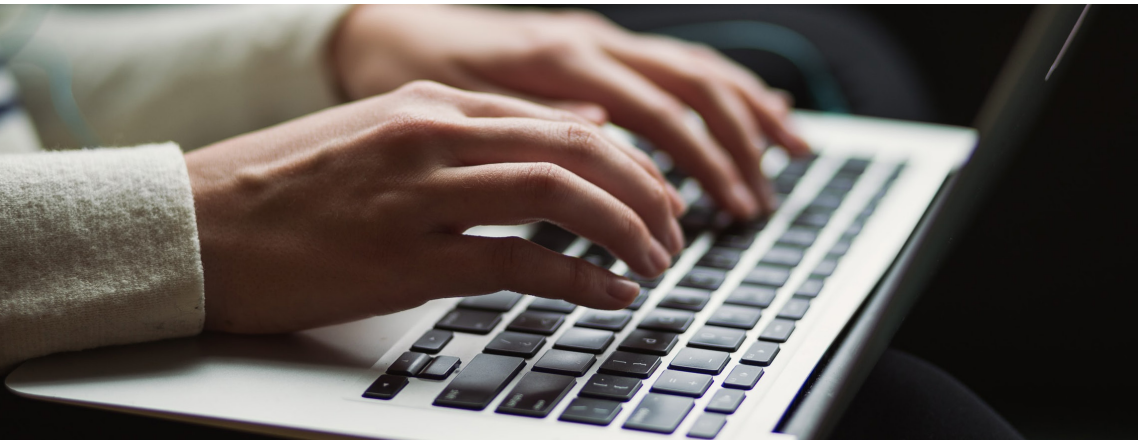
SOLUTION BRIEF

Secureworks

Transforming Incident Response for Readiness and Resilience



The Challenge

The pace and breadth of change today is unprecedented. Organizations are faced with increased cyber risks as they embrace technologies intended to enable business operations and transformations that are increasingly attracting the attention of motivated adversaries.

The Solution

The Secureworks Incident Management Retainer is designed to help organizations reimagine their approach to incident response, enabling a comprehensive and resilience-driven approach to elevate their cyber defense posture and providing support in the event of cybersecurity emergencies.

Cyber resiliency is defined by NIST as "the ability to anticipate, withstand, recover from, and adapt, to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources"[1], emphasizing the importance of moving beyond security prevention to a strategy that relies not only on detection but also on improving organization-wide response capabilities for more effective response and recovery.

New Business Realities

Cybersecurity leaders today need to balance cybersecurity and risk mitigation with business operations and transformation efforts. The accelerated adoption of new technologies has resulted in an increasingly complex IT ecosystem and a rapidly expanding attack-surface. Compound that with the industry-wide staff and skills shortages and fast-evolving, motivated adversaries, and it is clear why 76% of cybersecurity professionals indicated that threat detection and response is more difficult than it was two years ago[2].

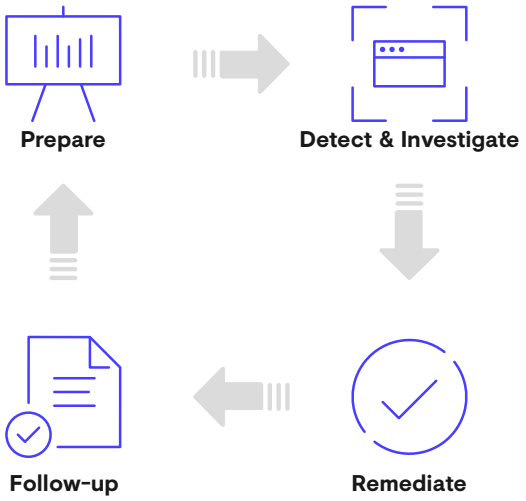
In this new business environment, recognizing that compromise or data breaches may be inevitable is a fundamental assumption to building a robust response program and achieving cyber resilience. The Secureworks Incident Response Life Cycle (Figure 1)

[1] https://csrc.nist.gov/glossary/term/cyber_resiliency

[2] ESG Master Survey Results, The Threat Detection and Response Landscape, April 2019

provides a framework for building an incident response program. It emphasizes the importance of coupling reactive and conventional response capabilities with a proactive and adaptive approach. Preparation and post-incident follow-up activities play a pivotal role in effectively managing cybersecurity risk and ultimately mitigating disruption and lasting business impact during and after material cyber incidents.

Figure 1. Secureworks Incident Response Life Cycle



Maturing Incident Response

As proactive incident response and preparation are recognized as critical components of an organization's cybersecurity program, incident readiness is becoming one of the biggest drivers for security spending[3]. However, a recent ESG survey suggests that organizations are less mature in incident readiness than they believe[4].

The survey shows that 92% of respondents feel "good to excellent" about their ability to quickly detect and respond to incidents, yet only 68% indicate they have an incident response plan in place, and fewer still regularly exercise that plan.[4] While readiness activities are taking place, the approach is often not optimal for building readiness and resilience. Further examination of incident readiness shows a tendency toward tactical activities, with regulatory compliance prevailing as one of the leading drivers for incident readiness.[4]

Organizations can mature their programs and gain more value from proactive incident response by increasing the frequency and expanding depth of readiness activities, while ensuring a deliberate, organized approach.

[3] ESG Research Report: Cybersecurity Services: omnipresent and heavily invested in, Dec. 2019
[4] ESG Master Survey Results, Incident Readiness Trends, Aug. 2020

How Secureworks Helps

Secureworks Incident Response has been responding to cybersecurity emergencies and helping customers prepare to respond for over 14 years. During this time, our incident response team has supported thousands of customer engagements globally. Our consultants leverage 20 years of company operational security expertise, visibility across over 4000 customers, and 20 years of attack data produced, analyzed, and validated by our Counter Threat Unit™ (CTU™) researchers and threat hunters.

Secureworks Incident Management Retainer

The Secureworks Incident Management Retainer is designed to enable a comprehensive and resilience-driven approach to elevate your cyber defense posture and to support you in the event of cybersecurity emergencies. Secureworks offers a tiered retainer model to accommodate your business objectives while advanced program management features provide the expertise to achieve and guide an effective proactive approach.

Proactive Consulting Services

The Incident Management Retainer provides access to a wide range of incident response and cybersecurity consulting services. Our consultants bring years of experience and a deep understanding of leading cybersecurity practices to mitigate risk and impacts. This expertise is enhanced by the collective knowledge from thousands of engagements, the very latest threat intelligence, proprietary cybersecurity analytics, and threat-informed methodologies. A suite of strategic, advisory, and technical services provides the building blocks to help build and tailor an incident response program and your cyber defense capabilities.

Incident Readiness & Advisory Services

Led by experts from our Incident Response and Security Advisory Services team.

Assess your current state to inform response planning and program design

Develop IR Plans, Policies and Procedures

Prioritize remediation and corrective action

Define cybersecurity roadmaps toward achieving target state

- **Incident Response Readiness Assessment**
- **Incident Response Plan Development/Review**
- Security Maturity Assessment
- Security Controls Assessment **based on proprietary Secureworks Information Security Assessment (ISA) framework**
- Cloud Configuration Review
- Cloud Security Architecture Assessment

Secureworks®

Workshops & Exercises

Led by our Incident Response consultants and elite researchers and hunters.

Learn about the threat and best practice

Train your teams in fundamental processes

Review lessons learned from past incidents

Practice through threat-informed scenarios and simulation

- **IR Fundamentals Training**
- **Lessons Learned Workshop**
- **Threat Brief**
- **Executive Brand Surveillance - Information Brief**
- **Tabletop Exercise**
- **Functional Exercise**

Testing & Validation Services

Delivered by our Adversarial Security Testing team and hunters from our CTU Special Ops and IR teams.

Test systems, applications, people, and teams

Identify the presence of existing threat actor

Remediate gaps and weaknesses

- Threat Hunting Assessment
- Penetration Testing
- Application Security Testing
- Red Team Testing

Program Management Features

In addition to enhanced Emergency Response SLAs, the Secureworks Essential and Essential Plus Incident Management Retainer tiers include advanced features geared toward helping to ensure and guide program advancement and governance. This includes both upfront workshops and regular touchpoints with Secureworks incident response subject matter experts to plan, track progress and review cross-organizational participation at all levels, before, during and after cybersecurity emergencies.

Through the **Annual IMR Planning Workshop,** Secureworks helps prepare for effective and efficient response with an upfront understanding of your organization's objectives and cybersecurity strategy.

- Emergency IR Fundamentals reviews the incident handling and escalation process, ensures alignment of the Secureworks response team to your existing plans and processes, and proactively identifies any areas that may hinder timely and effective response.
- Proactive Services Planning provides an opportunity to discuss your organization's objectives and cybersecurity strategy to collaboratively develop a proactive plan and a mutually defined roadmap for leveraging Secureworks proactive services.

Quarterly Service Reviews provide regular interactions with Secureworks Incident Response experts to review outcomes, provide recommendations and make any adjustments to the proactive services roadmap. Our Essential Plus Tier includes an Annual Executive Briefing delivered by a senior member of the Secureworks Incident Response team. This briefing is aimed at an executive audience to communicate insights, progress, and updates in the context of cyber risk

Emergency Incident Response

When a cybersecurity emergency does occur, the Incident Management Retainer provides SLAs to ensure timely support from global incident responders on standby to assist with a variety of cyber threat scenarios. Secureworks Emergency Incident Response provides support for a range of incident types – from small, single computer system concerns to large-scale, enterprise-wide crisis situations that significantly disrupt or impede business operations.

Our approach is collaborative and interactive. We work with your team to assess, understand, and handle the situation so you can take the right actions and minimize the duration and business impact of a cybersecurity emergency. Our team provides digital forensics, malware analysis and threat intelligence analysis capabilities, as well as guidance and assistance needed for rapid investigation, analysis, and remediation of threats.

Secureworks Incident Response is equipped to provide your organization with cross-functional incident command assistance to ensure all incident response stakeholders are coordinating their efforts and to lead all participants toward mutually defined response objectives.

To download a Data Sheet on the **Incident Management Retainer**, **click here**

If your organization needs immediate assistance, call our **24x7 Global Incident Response Hotline**: **+1-770-870-6343**

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

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