Secureworks

SOLUTION BRIEF

Incident Response Services to Help You Prepare for and Quickly Respond to Security Incidents

The Challenge

The threat landscape is always evolving and adversaries are getting harder to detect; and with that, cyber risk increases too. Incident Response experts require an increasingly sophisticated skill set, which makes hiring and retaining them difficult, yet you're expected to detect, investigate and respond to threats daily to defend your organization today, as well as ensure you mature processes and resiliency to prevent more in the future.

Seasoned Secureworks Incident Response subject matter experts leverage their experience and purpose-built response technologies enriched with years of proprietary threat intelligence to help you prepare for and respond to cyber incidents to mitigate cyber risk efficiently and effectively.

Increased Risk

Research shows that 1 in 4 organizations will experience a data breach in the next 24 months[1], yet 54% of companies still don't have an incident response plan.[2] Incident response involves a level of business risk that shouldn't be left to last minute planning or "winging it" through a crisis. Unfortunately, Secureworks found that 71% of organizations surveyed say their company's incident response capabilities are focused on reactive measures, and 42% either limit them narrowly to the security team or don't do security exercises at all.

Even if you do have a plan, you may not have the resources to fully protect your organization. The threat landscape is always evolving. Increasingly sophisticated adversaries are now living off the land in your environment, using legitimate credentials and native tools in your environment to make detection difficult without advanced technologies driven by behavioral analytics and the latest threat intelligence.

A recent survey revealed that 66% of enterprise respondents feel they do not have enough employees to address the increasing level of threats coming their way.[3] Digital forensics experts are especially difficult to hire and retain. More than most other security specialists, incident responders require hard to find skill sets like reverse malware engineering and analysis. With a lack of experienced resources comes a lack of insight—you don't always have the resources or perspective to take the right action to resolve security incidents quickly and prevent the adversary from re-entering your environment in the future.

Detection, investigation and response actions have to become a daily habit to mature your incident response program. Orchestrating these activities seamlessly across your security operations helps resolve incidents quickly, efficiently and scales response to the speed of digital business.

Incident Response Plan Review/Development

Secureworks Incident Response security consultants help you develop an effective response plan, also known as a Cybersecurity Incident Response Plan (CIRP), based on IT security best practices. We know every organization is unique and we tailor each plan to fit the requirements of your organization. Your response plan or CIRP will detail what needs to happen so you and your team can respond quickly and effectively during a cyber incident, and minimize the impact to your organization. In addition, your response plan or CIRP will reflect the latest intelligence we've discovered that addresses the types of threats and scenarios of greatest concern to your organization.

Incident Response Readiness Assessment

Secureworks Incident Response Readiness Assessments help gain a comprehensive picture of your cybersecurity Incident Response capabilities to inform tailored recommendations to enhance your plans and help ensure that your organization is ready when an incident occurs. Secureworks Incident Response consultants leverage their experience and expertise along with best practice methodologies to assess strategic and tactical effectiveness via documentation reviews, as well as workshops, tabletop exercises and interviews with key personnel to identify gaps and exposure areas. Based on these findings our consultants help prioritize recommendations for your plans, and to help enhance cybersecurity response practices overall.

Incident Response Workshops and Exercises

While the development of a sound plan is a critical step, testing the plan is necessary to determine how well you will react and respond to an active incident. Secureworks can facilitate exercises and training to mature your incident response program.

- **Tabletop Exercises**
  Tabletop exercises are designed to validate roles, responsibilities, coordination and decision-making. Our Incident Response security experts will design and conduct plausible simulated exercises to evaluate your team's performance. After discussing how your team would respond to the simulated scenario, our consultants will provide detailed feedback and recommendations for improvement.
- **Functional Exercises**
  Functional exercises allow personnel to validate their operational readiness for incidents by performing their duties in a real-life simulated manner. Functional exercises are designed to exercise the roles and responsibilities of specific team members and procedures in one or more functional aspects of a plan.
- **First Responder Training**
  First Responder Training instructs your first responders in carrying out processes to preserve evidence, utilize proper documentation procedures, and establish the necessary cadence with Secureworks towards resolving the incident and collaborating throughout the Incident Response Lifecycle. These workshops are designed to train your employees to enable your organization to quickly preserve and transfer critical disk images and RAM to enable timely and efficient analysis.

- **Briefings and Workshops**
  Briefings and workshops help you review lessons learned from previous incidents, the overall preparedness of your Incident Response program, or provide guidance on topics of interest that fall within the domain of Incident Response Services. We work with you to determine relevant content to cover during these sessions. This ensures your team gains insights on specific actions recommended to protect your unique environment.

Incident Management Retainer

To ensure your organization has the right resources, with the right expertise in place should a security incident occur, the Incident Management Retainer guarantees fast availability of our elite Incident Response team to help you contain, mitigate and recover from the incident.

The service provides immediate support through our Security Operations Center (SOC) and onsite support unmatched globally:

- Arrival in less than 36 hours onsite U.S. and U.K.
- In-transit within 48 hours for international clients

The retainer service is not just an insurance policy that guarantees you the top expertise is available when you need it; it's an opportunity to heighten the capabilities of your Incident Response team. The retainer service provides access to a team of seasoned incident response consultants and subject matter experts to advise and assist across the Incident Management Lifecycle. Whether you need assistance with cyber incident preparedness of response, invoke the Incident Management Retainer for any Incident Response Service at any time during the contract term*.

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

* Retainer balances can be applied toward all IR services at any time during the contract term, contingent on a sufficient balance to cover the price of the requested service or the approval to be billed for the difference.

Sources:

[1] 2017 Cost of Data Breach Study: Global Overview, Ponemon Institute, June 2017

[2] The Global State of Information Security Survey, PWC, 2018

[3] Global Information Security Workforce Study, Center for Cyber Safety and Education and (ISC)2, 2017

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the 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.™

Secureworks®