

Secureworks®

WHITE PAPER

# 9 KEY QUESTIONS TO ASK WHEN SELECTING AN INCIDENT RESPONSE SERVICE PROVIDER



Security incidents can interfere with business processes, compromise data integrity, and threaten an organization's reputation. Well-meaning but incorrect actions after an incident can destroy valuable evidence about how the attacker accessed the network and the extent of malicious activity, leaving the organization unable to assess impact or prioritize future investment.

Many people associate the term “incident response” with recovery efforts following a major security breach. However, effective incident response is not just reactive, nor is it confined to major incidents. An incident response (IR) provider can assist you with a range of prevention, detection, and response activities; for example:

- Creating and testing an IR plan
- Integrating your IR plan with your information security program
- Identifying risks and threats through threat hunting and threat intelligence
- Managing identified risks
- Maturing your security posture
- Meeting legal and regulatory obligations
- Investigating and recovering from a data, system, and/or network compromise

Secureworks® Incident Response Consulting has compiled a set of questions to help you evaluate and select an IR provider.

### QUESTION 1:

#### Why do I need an incident response provider?

An objective third-party provider can offer expertise with a broad scope of IR activities. Using experience gained from decades of working with various organizations, an external provider can help you guard against, identify, and mitigate incidents. The vendor should be able to provide forensic analysis and evidence.



The third-party provider should also understand applicable legal and regulatory requirements, such as standards established by the Payment Card Industry (PCI) Security Council, General Data Protection Regulation (GDPR), and the Health Insurance Portability and Accountability Act (HIPAA).

### QUESTION 2:

#### Do I need an internal IR capability? If so, can the external provider help me?

An internal capability can range from a formal, regularly tested IR plan to a dedicated IR team. An IR provider should be willing and able to evaluate the organization's concerns, needs, and resources to recommend appropriate proactive and reactive internal capabilities. The vendor should support your internal IR team by providing insights and expertise:

- A broader view of attacks and the threat landscape for better context
- A larger skillset, especially in specialized areas such as threat hunting
- Independent third-party support as required by regulatory and/or legal requirements

### QUESTION 3:

#### How long has the IR provider been in business? Has it always provided IR services?

Longevity can reflect a vendor's level of experience and rate of success. Some companies shift their focus over time, so it is important to determine how long the provider has offered IR services rather than relying on when the company was founded.

## QUESTION 4:

### What other services does the IR provider offer?

Many IR providers take a comprehensive view to security by offering additional services such as vulnerability scans, threat hunting, penetration tests and adversarial exercises, threat intelligence, endpoint, cloud and network monitoring, and log monitoring. Combining these types of services can reveal vulnerable systems or software, exposed access vectors that threat actors could exploit, and early indications of malicious activity.

In addition, most IR providers will offer proactive IR consulting and advisory services, as well as training services to provide coverage and support across all aspects of the incident preparedness lifecycle (figure 1). Outcomes and results of advisory and assessment services help facilitate alignment among board members, executive team and security staff. These activities can also be designed for their participation to help build broader organizational cybersecurity awareness.




Figure 1: The Preparedness Lifecycle

### QUESTION 5:

#### **How much experience does the IR provider have in my industry vertical? Does that matter?**

Although skilled IR analysts should be able to investigate incident activity regardless of vertical, understanding an industry's dependencies, regulations, unique attributes, and links to other industries can enhance analysis efforts.



Many threats are not confined to specific verticals, so it is important for the vendor to have broad visibility across the threat landscape. In addition, knowledge of threat behavior and threat actors' tactics, techniques, and procedures (TTPs) is critical for anticipating and recognizing malicious activity.

### QUESTION 6:

#### **How much experience does the IR provider have with the technologies in my network environment, including industrial control systems? What about experience with cloud or software as a service (SaaS) solutions?**

An IR provider's familiarity with your technologies and platforms is important for identifying specific attack vectors, as well as abnormal files or behaviors. As attackers and malware attempt to avoid detection, subtle nuances such as a misspelled filename may be critical to an incident investigation.

Evolving IT ecosystems means growing attack surface with more opportunities for threat actors to exploit. For example, the [Secureworks 2021 Learning from Incident Response: Year in Review](#) reminds us of several high-profile incidents involving opportunistic mass exploitation of popular third-party software.

### QUESTION 7:

#### **Will the IR provider supply engagement statistics and client references?**

The number of engagements per year can indicate the vendor's capacity for handling simultaneous engagements and the level of experience with various types of incident activity. Although some clients may be wary of discussing the details of a breach, a mature IR provider should be able to provide references who are willing to talk about their experience with the vendor.

### QUESTION 8:

#### **What support can the IR provider give for civil or criminal litigation?**

Security breaches could lead to legal action, so it is important to understand if and how the provider could contribute. For example, is forensic evidence collected and processed in a manner that can be used in court? Are the IR analysts willing and able to testify if necessary?

### QUESTION 9:

#### **What differentiators should I look for?**

When evaluating IR providers with comparable services, other factors might help you determine which vendor is the best fit. The ideal vendor should have the following characteristics:

- A desire to be a trusted security partner, not just a provider of services
- A presence in your geographic region to provide rapid local support
- Certifications and accreditations applicable to your industry and/or company requirements
- Experienced responders drawing on cross-functional, technical and non-technical skills to complement and guide response effort
- Experience in your industry vertical and other related industries
- A working relationship with law enforcement
- An analysis model that incorporates a combination of commercial and proprietary tools

### **About Secureworks Incident Response Consulting**

Secureworks Incident Response Consulting assists with the development of IR plans, offers IR workshops and exercises, conducts risk assessments, and provides rapid containment and mitigation of threats to minimize the duration and impact of a security breach. The team leverages elite cyber threat intelligence and global visibility to facilitate preparation, response, and recovery activities. Visit the Secureworks website for more information about [Secureworks incident readiness and response services](#).

# Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 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.

## CORPORATE HEADQUARTERS

### United States

1 Concourse Pkwy NE #500  
Atlanta, GA 30328  
+1 877 838 7947  
[www.secureworks.com](http://www.secureworks.com)

## EUROPE & MIDDLE EAST

### France

8 avenue du Stade de France  
93218 Saint Denis Cedex  
+33 1 80 60 20 00

### Germany

Main Airport Center,  
Unterschweinstiege 10 60549  
Frankfurt am Main Germany  
069/9792-0

### United Kingdom

One Creechurch Place,  
1 Creechurch Ln  
London EC3A 5AY  
United Kingdom  
+44(0)207 892 1000

1 Tanfield  
Edinburgh EH3 5DA  
United Kingdom  
+44(0)131 260 3040

### United Arab Emirates

Building 15, Dubai Internet City  
Dubai, UAE PO Box 500111  
00971 4 420 7000

## ASIA PACIFIC

### Australia

Building 3, 14 Aquatic Drive  
Frenchs Forest, Sydney NSW  
Australia 2086  
1800 737 817

### Japan

Otemachi One Tower 17F  
2-1 Otemachi 1-chome,  
Chiyoda-ku  
Tokyo 100-8159, Japan  
81-3-4400-9373  
[www.secureworks.jp](http://www.secureworks.jp)