Secureworks®

WHITE PAPER

9 Key Questions to Ask When Selecting an Incident Response Service Provider

Secureworks® Incident Response Consulting helps organizations of all sizes and across all industries prepare for, respond to, and recover from even the most complex and large-scale security incidents.

On average, targeted threats remained undetected in compromised networks for 221 days.[1]

Security incidents can interfere with business processes, compromise data integrity, and threaten an organization's reputation. Well-meaning but inappropriate 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 offers expertise with a broad scope of IR activities. Using experience gained from 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.

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:

The 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).

[1] Secureworks Incident Response Insights Report 2019

- 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, penetration tests, threat intelligence, endpoint 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.

Some vendors also offer consulting services, such as executive advisory support, security program assessments, and evaluation of security controls to meet legal and regulatory requirements. The outcomes of advisory and assessment exercises can help facilitate alignment among your board members, executive team, and security staff on what priorities need to be addressed.

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.

As a technology becomes more popular, it is often exposed to more threats. For example, the Secureworks Incident Response Insights Report 2019 revealed that incidents that traverse cloud infrastructure are generally becoming more common.

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?

Some security breaches 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?

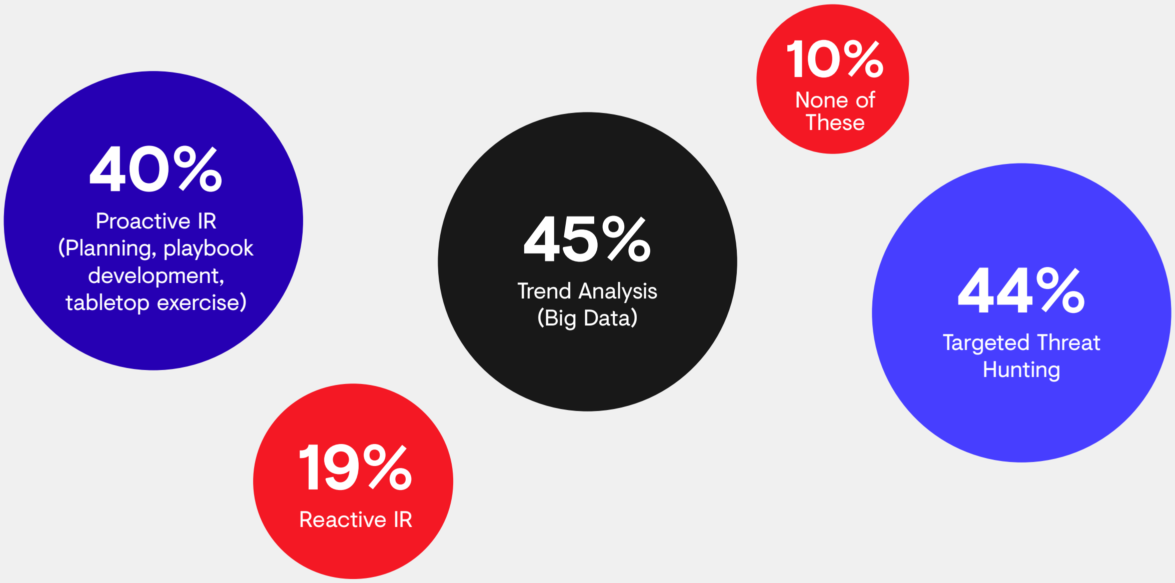
Question 9: What differentiators should I look for?

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 your 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
- 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

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 response services.]

What Type of IR Services Do You Have on Retainer with an External Vendor Today?



Snapshot of how companies are currently investing in IR retainers.

Source: Secureworks 2018 Security Leaders Survey

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

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
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp