FORWARD
DEFENSE

Cyber Incident Response

Detailed Information Service Partnership

Cyber Incident Response

Your network is inundated with events that may seem suspicious, but when one of those turns into a declared security incident you need fast and effective incident response to mitigate the potential damage, determine the root cause, and prevent future problems. Our team has been conducting incident response for government and corporate clients for well over a decade. Our methodologies ensure that our response is technically sound, organized, and professionally executed. We maintain incident handlers around the globe, enabling us to quickly provide support to you when time is of the essence.

Detailed Information
Service
Partnership

Professional, effective, confidential response

The realization that an incident has occurred can inspire fear and even panic as stakeholders struggle to understand the damage, the attack vector, and their potential liabilities. Internal challenges frequently arise as blame is assigned and various units shuffle to isolate themselves from the fallout. None of these leads to effective response to the incident or to mitigation of any negative impact. Our team works in the time-sensitive environment of active incidents on a regular basis, allowing us to impartially and objectively evaluate the evidence at hand, unencumbered by preconceived ideas about the environment. This third-party insight is a valuable advantage even to organizations with a robust internal incident handling team, as extra eyes on the problem drawing from different bases of experience assist in understanding the incident as quickly as possible..

We use the latest in memory forensics, log analysis, network security monitoring, disk forensics, malware reversing, and proactive scanning techniques to ensure a comprehensive response to any network security incident. Working with your team to determine the root cause, develop containment and remediation strategies, and enhance defenses to prevent recurrence, our incident response service provides a turnkey solution to any security situation. Backed by our team of industry-leading partners, we have the capacity to address any incident regardless of size or geographic scope.

We are there when you need us

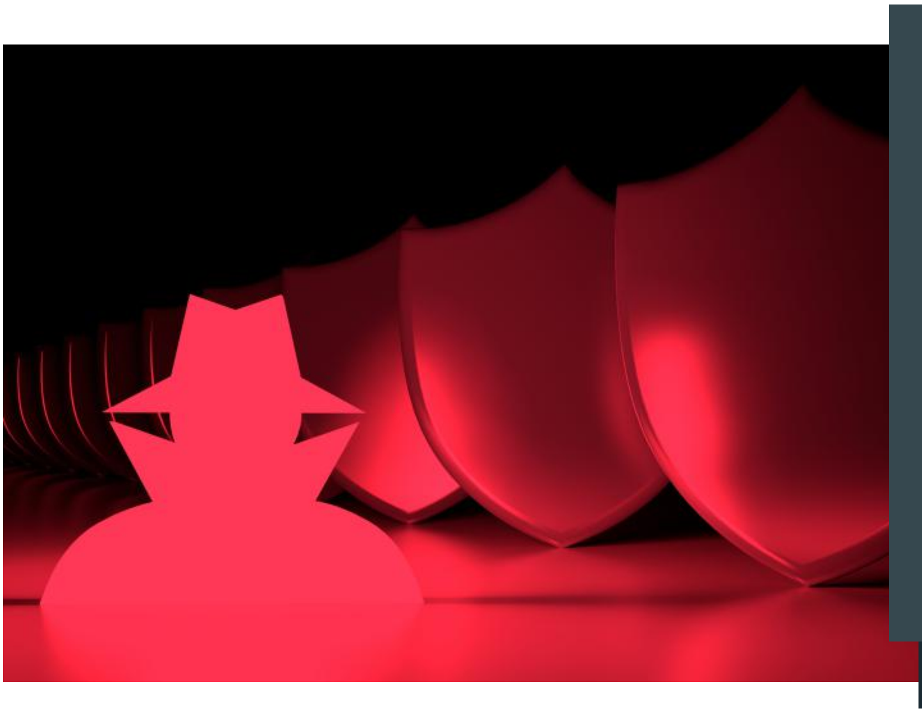
Our incident response service is offered as on an as-needed basis or on a retainer basis. Hours not used to respond to active incidents can be reallocated to pro-active threat hunting missions to help identify potential threats that may otherwise go undetected within your environment. We prefer that our customers also take advantage of our incident readiness services to ensure that their environment is capturing and retaining information to support effective incident response and investigation activities, but we realize that our expertise is often needed on short notice after an incident is detected. We are ready to offer our assistance to you at any time.

Service Overview

Incidents happen. No organization can protect itself from this reality, so it is incumbent upon every IT security executive to ensure that the organization has the capability to respond to incidents in an effective and efficient manner. When developing the internal capability to handle incidents is not possible due to business or financial constraints, outsourcing this capability is frequently the best solution. Our team maintains the skills, equipment and expertise to provide a thorough analysis of available data to analyze it for indicators of what occurred during an incident. All incident response services are offered on a time and material basis, with no guarantee of any specific findings.

Detailed Information   Service   Partnership

Incident Response Overview



In cases where our team is called to respond to an incident after it is detected, our response begins with offsite discussions with your onsite team to help direct collection and preservation of potential evidence related to the incident and formulate an initial strategy. An initial team of responders from our side will mobilize in accordance with available staffing and client requirements. This team will assist in collection and preservation efforts, following evidence handling best practices, and begin the triage analysis of collected data. Based on preliminary findings, additional senior response analysts, with specialized knowledge relevant to your situation, may be deployed to provide additional analysis and support. Our team will provide log analysis, digital forensic examination, vulnerability assessment, and other services as needed to investigate the incident.

Throughout the investigation, our team will liaise with your staff to obtain additional contextual information and make remediation and collection recommendations based on the most up-to-date analysis results. Incident response requires active and continuous communication with the IT and security staff of the client organization. Similarly, operational security must be reviewed and exercised to avoid leaking information about an ongoing investigation.

The final output of the investigation will be a report that outlines, to the extent possible, the root cause of the incident, the technical impact of the incident, recommendations for remediation of the incident and recommendations for improvements to security practices to reduce the risk of similar incidents in the future.

Detailed Information Service Partnership

Incident Response Methodology

Incident response is a constantly evolving discipline that must employ the latest technologies; however, the process of incident response remains relatively stable. Our methodology ensures that we conform to industry best practices and international standards. We draw upon a number of different standards to ensure that we provide a comprehensive, well documented, technically correct and procedurally grounded response. Our team relies on NIST SP 800-61 Revision 2, NIST SP 800-86, ISO 27035:2001, ISO 27037:2012 and ISO 17025:2005 to provide the basis of our incident response methodology.

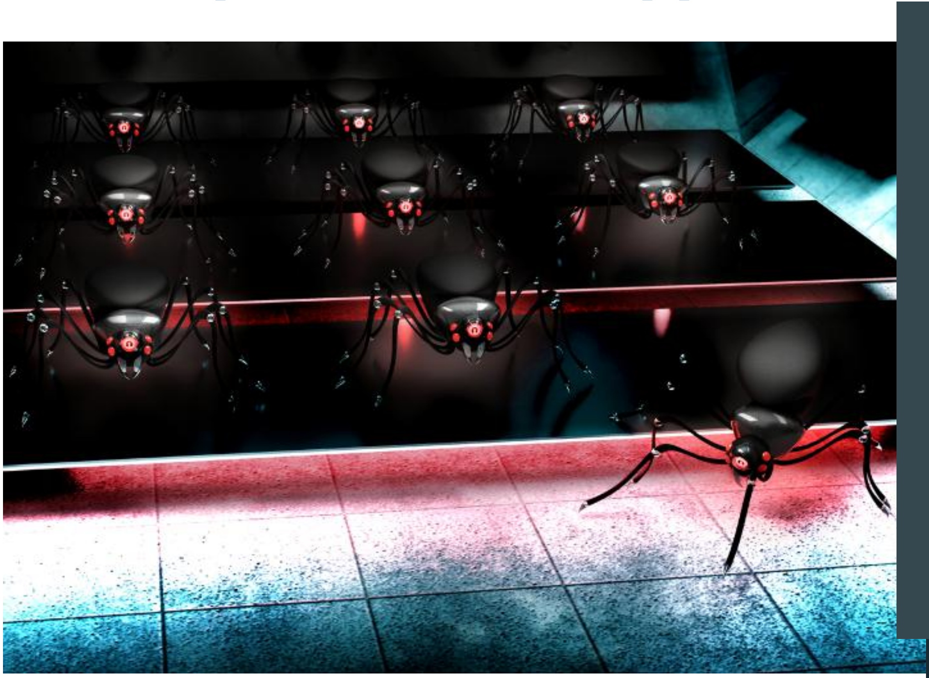
We recognize that incident response begins well before an incident is detected. Our team prefers to work with our clients to facilitate proper incident response preparation by helping to assess and improve our clients' incident readiness as well as proactively help strengthen your security and incident detection technologies and procedures. We therefore recommend that we work with you before an incident is detected to provide incident readiness assessments, vulnerability assessments, and recommend technologies and procedures to strengthen your network security and incident detection capabilities.

Once an event is determined to be an incident, our team will work side-by-side with your incident handlers, IT security team, and operational management to identify the scope of the incident and minimize its impact on operations. Incidents are dynamic events. We appreciate that a rapid analysis is needed to begin containment and that assessment and response must be continually updated as new information is discovered. As containment of the incident is achieved, our team will work with you to develop the best strategy for remediation and future prevention of similar incidents.

During the incident response, we will provide on-the-spot reporting as key activities are performed and actionable information is discovered. After the incident is controlled, our team will begin development of detailed documentation of the incident, our joint response efforts, remediation recommendations, and suggestions for future preventive steps that could be implemented to further harden your network and information resources. These documents will be delivered for review, approval, and subsequent action after the incident response is completed.

Detailed Information | Service | Partnership

Example Technical Approaches



While the key to any successful incident response is knowledgeable personnel, we can highlight some of the techniques that we employ on most of our incident response engagements. While each incident is unique and the techniques employed vary depending upon the nature of the incident, the following represent some of the techniques that we frequently deploy.

Many incidents involve the use of malicious software. As a result, memory forensics techniques are critical for identification and analysis of malware that may have been placed within a victim environment. Our experts use the latest in commercial and open source technologies to locate anomalies on running systems, identify indicators of compromise, and analyze the behavior of unknown malware.

When properly configured, event logs can be generated by a wide range of network assets. Analysis of this log data can help identify malicious activity and lead to discovery of attack vectors as well as lateral pivot activity within a network. Our experts use a combination of automated and manual analysis of log events to reduce false positives while surfacing critical events.

Forensic analysis of impacted systems can yield valuable information about the impact of an incident; however, our team recognizes that a complete analysis of all potentially impacted systems is rarely feasible. We employ a number of different triage mechanisms to identify systems of interest and target analysis of the areas of those systems most likely to contain information of evidential value to the incident. We therefore maximize the value of forensic analysis while controlling the associated costs.

In cases where an incident is ongoing, network security monitoring is a key component to a well-rounded response. By monitoring targeted network segments, our analysts are able to identify ongoing malicious activity and help monitor attacker response to ongoing containment or recovery efforts.

Many other techniques are employed by our team depending on the circumstances of the incident. These techniques include but are not limited to interviews of personnel, network security auditing, DNS traffic analysis, beacon detection and any other technique that may be applicable to the particular circumstance of the incident under investigation.