Cyber Incident Response **:** *We maintain incident handlers around the globe, enabling us to quickly provide support to you when time is of the essence.*

Cyber Incident Response

Forward Defense uses 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.

Forward Defense - Here 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.

Cyber Incident Response Services

The Forward Defense 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.

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. 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.

Cyber Incident Response : *We maintain incident handlers around the globe, enabling us to quickly provide support to you when time is of the essence.*

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.

Techniques

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.

Analysis of log data - this assists with the 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.

Network Security Monitoring - 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.

Contact Us

Each of our solutions is as unique as our customers. Please contact us to discuss the best way to meet all of your digital forensics requirements

www.forwarddefense.com
info@forwarddefense.com

Forward Defense Equipment and Services

51st Floor, Addax Tower City of Lights
Al Reem Island PO Box 47019 Abu Dhabi, UAE

+971 2 627 8921