IntegraONE | Incident Response

(484) 223-3480
(484) 223-3427 Fax
https://www.IntegraONE.com

IntegraONE offers comprehensive services for incident response. Our team of highly skilled engineers has expertise across many IT areas, including networking, storage, compute, virtualization and core security. We are here to help our clients through security incidents, restoring IT infrastructure and remediating the security issues that contributed to the breach or compromise.

Service Description:

Technology deployment / investigation of initial leads: Deploy the technology most appropriate for a fast and comprehensive incident response. We simultaneously investigate initial client-provided leads to start building Indicators of Compromise (IOCs) that will identify attacker activity while sweeping the environment for all indicators of malicious activity.

Crisis management planning: Work with executives, legal teams, business leaders, and senior security personnel to develop a crisis management plan.

Incident Scoping: Monitor real-time attacker activity, search for forensic evidence of past attacker activity to determine the scope of the incident.

In-depth analysis: Analyze actions taken by the attacker to determine the initial attack vector, establish the IntegraONE Advantage:

- Investigative Experience: IntegraONE investigators have honed their skills by conducting and remediating the some of the world's largest and most complex investigations.
- Threat Intelligence: Industry leading intelligence assembled from the frontlines of incident response, extensive attacker tradecraft discovery and research through third-party data sources, Threat Intelligence collected by IntegraONE teams and partnerships with other Threat Intelligence sources.

(484) 223-3480
(484) 223-3427 Fax
https://www.IntegraONE.com

- Technology: IntegraONE team members use the latest cloud and/or on-premises technologies, allowing investigations to begin immediately in conjunction with triage and forensic scripts and other tools as required. IntegraONE teams enable rapid response at scale through partnerships and internal expertise, providing visibility into traffic by review of logs and endpoints running Microsoft Windows, Linux and macOS X.
- Crisis Management: Our Incident response team and partners have years of experience advising clients on incident-related issues.
- 24/7 incident response coverage: 24/7 attacker activity analysis during investigation and remediation. Timeline of activity and identifying extent of compromise.

This can include:

- Live response analysis
- Forensic analysis
- Network traffic analysis
- Log analysis
- Malware analysis

Damage assessment: Identify impacted systems, applications and information exposure to extent possible.

Optional Services Extension:

Remediation: Develop and assist customer with containment and remediation strategy based on the actions of the attacker and tailored to the needs of the business in order to eliminate the attacker’s access and improve the security posture of the environment to prevent or limit the damage from future attacks.

Service Retainers:

Service Retainers for Incident Response and Remediation are available.