DATA SHEET

Incident Response Services

Rapid, Expert-Led Cyber Crisis Response When Every Second Counts

Deliverables

- Immediate remote triage and on-site dispatch of IR consultants where requires
- 24/7 incident hotline and rapid engagement SLA
- Threat containment, eradication, and recovery strategy
- Forensic imaging, malware reverse engineering, and root cause analysis
  - Coordination with legal, PR, and regulatory stakeholders
  - Full reporting: executive summaries, technical findings, and regulatory-ready documentation
  - Remediation roadmap and lessons learned workshop

Engagement Scope

Typical engagements range from a few days to several weeks depending on breach complexity. We work collaboratively throughout, aligning response with your business and compliance needs. Our team remains engaged until full recovery and closure are achieved or otherwise as requested by our clients.

Overview

Our Trellix Guardians' Emergency Incident Response (IR) services provide organizations with immediate support during active cyber incidents. We deliver expert-led, comprehensive containment and investigation using globally recognized frameworks such as NIST SP 800-61r3 and MITRE ATT&CK®. Whether facing ransomware, data breaches, insider threats, or cloud compromises, we act fast to minimize damage, ensure compliance, and recover operations.

Our Methodology

We use a five-phase approach tailored for high-impact incidents:

1. Detection & Triage – Validate the incident, establish scope and severity.

2. Containment – Stop threat actor movement, preserve evidence, implement tactical defenses.

3. Investigation – Perform deep-dive forensics, log analysis, malware reverse engineering.

4. Eradication & Recovery – Recommend removal of threats, harden systems, restoration of services safely.

5. Post-Incident Reporting – Deliver clear executive reports, technical evidence, and recommendations

Technology and Intelligence Enablement

Our Emergency Incident Response services are technology-agnostic and designed to integrate seamlessly with your existing infrastructure, regardless of vendor or platform. To support rapid and effective investigation and response, our consultants leverage a suite of advanced tools, including the Trellix™ cybersecurity platform for threat detection, forensics, and endpoint analysis. We also incorporate proprietary threat intelligence from our internal Threat Intelligence Unit to identify attacker tactics, techniques, and procedures (TTPs), enhance contextual analysis, and accelerate containment and remediation actions.

Why Choose Us

- Proven experience with global breach cases
- Certified forensic and IR consultants (GCIH, GCFA, CISM, etc.)
- Compliance-aware (PCI DSS, GDPR, ISO/IEC 27001)
- Seamless integration with MDR, SIEM, SOAR, and Cloud platforms
- Clear communication with executive-level reporting and regulatory support

Disclaimer

This Emergency Incident Response service is delivered based on the information and access provided by the client at the time of engagement. Due to the lack of prior visibility into the client's environment, security controls, or architecture, our findings, containment actions, and recommendations are made in good faith based on the best available evidence. While we strive for completeness and accuracy, the client retains full responsibility for validating results, implementing controls, and maintaining ongoing security governance.

If you experiencing a breach, contact our Incident Response Team at: hacked911@trellix.com & hacked999@trellix.com