CYBERCLAN™

Incident Response Services

When a cyber breach occurs, every second counts. An effective response is crucial to thwarting threat actors and swiftly restoring your business and information security systems to their optimal state.

The Challenge

One of the biggest challenges companies face today is responding to cyber incidents quickly and effectively. Without a robust Incident Response (IR) plan, breaches can lead to prolonged downtime, financial loss, and lasting damage to reputation. The pressure to mitigate these disruptions while ensuring a secure future is immense.

Many organizations struggle to mobilize an IR team swiftly enough to reduce the impact of a breach. Time is critical—companies need experts who can jump into action and immediately contain the threat. Yet, even with the right people, businesses often find themselves without a clear, actionable roadmap, causing delays in recovery.

Our Solution

At CyberClan, we prioritize your security. Our global Incident Response (IR) team is committed to responding within 15 minutes of a breach notification. After our initial scoping call, you'll receive a clear and detailed statement of work within an hour, outlining our responsibilities and next essential steps.

Our Incident Response suite of services include:

Containment & Monitoring: Act quickly by identifying which systems or networks must be halted or quarantined. Activate the Endpoint Detection and Response (EDR) tool in our Security Operations Center for thorough monitoring, and our analysts will investigate and develop a targeted remediation strategy.

Breach Forensics & Root Cause Analysis: Investigate the network evidence from the breach by analyzing attack patterns and traffic data. Understand how it occurred and create strategies to prevent future incidents.

Business Email Compromise: Carefully review the email logs to construct a precise timeline of the incident, thoroughly investigate the audit logs, and uncover the method of access that was used.

Data Mining: Analyze Personally Identifiable Information (PII) and Personal Health Information (PHI). Our in-house data experts provide actionable insights and support throughout the investigation and remediation process to fulfill notification requirements.

Social Engineering Fraud Investigation: Carefully analyzing suspicious emails and attachments is essential for identifying threat actors and their methods. This proactive approach helps us detect potential malware or backdoors, safeguarding our systems and enhancing our security in a risky digital environment.

Threat Hunting: Conduct proactive threat hunting within the network environment to identify intrusions and malicious activities, revealing adversaries that may otherwise remain undetected.

Deep & Dark Web Monitoring: Continuously monitor cybercrime communities on the dark web using both current and historical data. Our proactive reports deliver valuable insights and timely alerts on significant events, empowering you with actionable intelligence to protect your interests.

Incident Response Retainer: A proactive solution that offers targeted support for network attacks and breaches at a lower cost than traditional insurance. Our retainers include forensic investigation, containment, monitoring, and IT restoration services.

Key Benefits

- Unparalleled speed, cost efficiency, with automation backed by manual validation to assure integrity.
- We deliver partial results when needed to expedite notifications and meet tight deadlines.
- Continuous monitoring ensures exceptional accuracy and accountability.
- Access to our team of global incident response and cybersecurity experts, ready to support you.
- Follow-the-sun, global capabilities for 24/7 support during active engagements.

CYBERCLAN™

Incident Hotline
US/CA 1 800 762 3290
UK 0800 368 8731
AU 61 1800 413 128
response@cyberclan.com

General Inquiries
US/CA 1 855 685 5785
UK 0800 048 7360
info@cyberclan.com