CYE

CYE SERVICE DATASHEET

Incident Response & Digital Forensics

24/7 expert-led containment, forensics, and recovery when it matters most.

24/7 support is provided to ensure effective containment, remediation, and recovery during a breach. The service is designed to reduce response time and minimize business operational impact, with activities spanning forensic evidence collection, threat hunting, and reporting on the scope of damage.

Response **Methodology**

1. Preparation
2. Detection & Analysis
3. Containment, Eradication & Recovery
4. Post-Incident Activity

- Forensic evidence collection across affected systems, networks, and endpoints.
- Threat hunting to identify indicators of compromise and the scope of the incident.
- Reporting on the scope and extent of the damage caused by the incident.

Deliverables

Upon incident closure, Cye provides a detailed incident summary report including:

Executive Summary
A business-level overview of the incident, its impact, and Cye's response.

Investigation Findings
Methodology and investigation process — containment approach, IOC gathering, and forensic analysis methodology.

Root Cause & Remediation
Root causes, findings, and proposed remediations to strengthen defenses.

Prerequisites

- Completion of an incident readiness questionnaire

Customer Engagement

- Incident readiness workshop
- Full engagement and assistance during an incident

RELEVANT STANDARDS

NIST Cybersecurity Framework

SECURITY DOMAINS COVERED

Governance, Policies & Procedures

Security Operations, Monitoring & IR

Engage a Cye expert to activate 24/7 incident response and digital forensics for your organization.

Engage Us