FORENSIC INVESTIGATION

Certified Forensic Investigations for Legal Proceedings

What Is Forensic Investigation?

Certified forensic investigators identify, preserve, and document crucial evidence for insurance claims and criminal prosecution. This is done by reviewing data sources such as, security or audit logs, emails or chat communications, and files on storage devices. Information obtained during a forensic investigation is processed in accordance with proper evidentiary procedures for preserving original unmodified copies of the data. This requires maintaining documented chain of custody, necessary for findings to be admissible in legal proceedings and insurance claims.

Why Choose CISO Global?

Only certified cybersecurity forensic investigators are capable of assisting you with legal and insurance claims. Our team of certified forensic investigators have decades of experience assisting companies through the complex process of legal and insurance claims.

- Certified cybersecurity forensic investigators
- Experience with obtaining insurance payouts
- Experience with submission and acceptance of evidence by the FBI
- Over 20 years of experience conducting forensic investigations

CISO Forensic Process:

- **Discovery** - Map out systems and data to be included in forensic investigation and create copies of unmodified original sources and establish chain of custody.
- **Analysis** - Review identified data sources for evidence related to the investigation or other suspicious activities.
- **Documentation** - Create report establishing narrative of investigation along with key findings and timelines of activities observed.

Key Outcomes

Identification of Evidentiary Data

Preservation of Evidentiary Data

Documentation of Findings

CISO
GLOBAL

480-389-3444 | ciso.inc

The CISO Global Approach to Incident Response

Containment

Limits the spread of the attacker and disrupt command and control communication by resetting compromised user accounts or blocking access to threat actor infrastructure.

Forensic Investigation

Certified forensic investigators review systems and applications for evidence of compromise to determine scope of attack and preserve data for use in criminal and civil court cases as well as supporting insurance claims.

Eradication

Removes attacker's malware and back doors planted into live systems or backups.

Remediation

Applying of security patches or modification of configuration settings to prevent future attempts from using the same pathways.

Root Cause Analysis

Identification of the source of the security incident enabling a complete understanding of what went wrong and highlighting the steps necessary to prevent the organization from suffering a similar attack in the future.

CISO GLOBAL

480-389-3444 | ciso.inc

Optional Add-On Services

Awareness Training

When an incident is determined to be caused by employee error, CISO Global Awareness Training is the best way to educate your team on typical attack pathways and how to respond to them which is the best way to protect your organization from a future breach event.

Penetration Testing

Just because attackers found one way to breach the organization doesn't mean there aren't other vulnerabilities lurking in the shadows. Penetration testing will identify security issues that expose your organization to immediate risk before the attackers can find and exploit them.

Security Risk Assessments

A comprehensive review of your entire organization will help identify gaps in your security posture. This includes evaluation of your policy, personnel responsibility & training, depth of security controls, and 3rd party risk from vendors and contractors.

CISO-As-A-Service (CISOaaS)

Having an experience security leader to develop and execute an overall strategy for the organization's information security program will ensure that initiatives are prioritized for maximum impact.

Security Operations Center Monitoring (SOC)

Continuous monitoring to identify suspicious activities in real time can allow organizations to quickly identify and shut down initial attack phases before they develop into full-blown breaches. CISO Global's SOC monitoring capabilities provide experienced analysts to swiftly understand and escalate a cyber kill chain to protect you from imminent threats.

CISO GLOBAL

480-389-3444 | ciso.inc

ABOUT CISO GLOBAL

About Us

A leader in cybersecurity and compliance services, CISO Global brings together expert practitioners and thought leaders to provide tailored solutions that drive cyber resilience. The company's top-tier talent spans geographies, specialties, industries, regulatory frameworks, and focus areas and includes auditors, compliance specialists, certified forensics experts, ethical hackers, security engineers, and around-the-clock analysts.

To learn more, visit www.ciso.inc.

STRATEGY & RISK

- Gap Analysis
- Audit/Assessment
- Third Party Risk Management
- FedRAMP
- StateRAMP
- CMMC
- Advisory
- Virtual CISO
- Managed Compliance
- Managed GRC

CYBER DEFENSE OPERATIONS

- Extended Detection & Response
- Managed Detection & Response
- SIEM as a Service
- Threat Hunting
- Cyber Threat Intelligence
- Digital Forensics
- Vulnerability Management Program
- Attack Surface Reduction
- Cyber Incident Response

CISO

SECURITY ARCHITECTURE & ENGINEERING SOLUTIONS

- Secured Managed Services
- Advanced Firewall Management
- Identity & Access Management
- Cloud Security
- Data Protection
- Remediation

READINESS & RESILIENCY

- Penetration Testing
- Tabletop Exercises with Incident Response Retainer
- Training Programs

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations™

SOC 2® Type II Audited

CISO GLOBAL

480-389-3444 | ciso.inc