EMERGENCY INCIDENT RESPONSE SERVICE

# Emergency Incident Response Service

CISO's Emergency Incident Response team follows best-practice processes described in NIST 800-61r2, focusing on first understanding the scope and scale of the incident, affecting containment and eradication, then supporting the business to achieve recovery of critical business process. During the incident and in the subsequent Incident Summary Report, lessons learned and observations for effective, long-term remediation is always shared with the intention of reducing incident frequency and severity.

Our team has decades of experience working both published and unpublished incidents of all sizes around the globe. We are experts in digital forensics, ransomware, ransomware actors, and have rare and extensive access to threat intelligence, including the darknet.

Additionally, our cloud forensics capabilities on all major platforms capitalizes on using cloud-native tools to rapidly gain perspective on endpoint, network, weak configurations, and suspicious activity to achieve rapid containment and root cause determination.

The team also has extensive experience working alongside cyber insurers and third-party legal practices to maximize the possibility of being covered for the unforeseeable and often catastrophic expense of a cyber-attack.

## OTHER INCIDENT RESPONSE SERVICES

### Post-incident Monitoring

We will take the environment and security control data to provide an immediate, advanced XDR/SOC service to ensure that even a determined adversary does not get back in. Our analysts know how to deal with sustained attempts to inflict ongoing damage as many Ransom-as-a-Service adversaries do.

### Encryption Key Recovery Services

CISO leverages various techniques and lab setups to recover encryption keys to be able to decrypt encrypted data.

### Threat Hunting

Utilize commercial, open source, and proprietary tools to discover Indicators of Compromise (IoCs)/Indicators of Attack (IoAs) on assets within a target environment. For the network and security controls, the team analyzes logs (firewall, e-mail, windows, linux, proxy, and application) and network traffic to determine if malicious actors are communicating with the environment using known Command and Control (C2) hosts or if other suspicious traffic is present.

CISO GLOBAL

480-389-3444 | ciso.inc

# PROJECT HIGHLIGHTS:

## Typical IR Clients

- Insurance Providers
- Government Site
- Non-profits
- Oil and Gas (IT/OT)
- Retailers
- Online vendors (“cloud-first”)
- Critical infrastructure (IT/OT)
- Banking and finance
- Insurance
- Managed Service Providers
- Manufacturing (IT/OT)

## SOC/IR Metrics and Reporting

It is impossible to manage what cannot be measured. The Emergency Incident Response (EIR) team has extensive experience assessing and measuring security operations to ensure excellent performance in key metrics, like: time-to-detect, time-to-contain, alert fidelity, and detailed measurement reporting.

## Operational and Crisis Response Threat Hunting

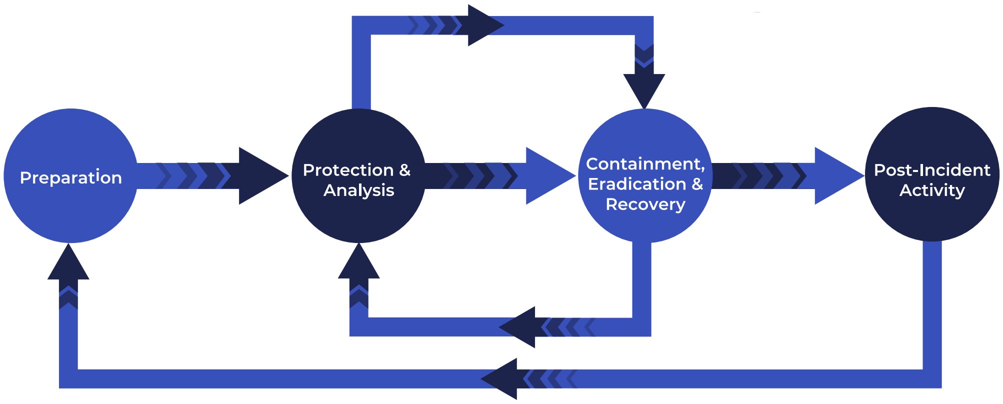
- Operational/day-to-day analysis of an environment
- Hunting adversaries live in an Emergency Incident Response scenario
- Rare and Proprietary Threat Intelligence (including darknet). Insight into the underworld that very few have access to.

## Threat Intelligence

- Curated, proprietary database with extensive surface and darknet feeds
- Darknet presence and HUMANINT
- Extensive ransomware expertise and adversary knowledge
- Ransom key recovery services. Excellent results for recovering ransomware keys; almost 100%

# METHODOLOGY

CISO GLOBAL uses an Incident Response Life Cycle (IRLC) framework that is capable to respond to any security incident. This IRLC is accepted by General Data Protection Regulation (GDPR) and the US government’s National Institute of Standards and Technology (NIST) Special Procedure (SP) 800-61.



## The four key steps are:

- Preparation – can you detect and respond? (hunting and SOC/EIR Program assessment and development)
- Protection and analysis – determining the scope and nature of the incident (emergency incident response)
- Containment/eradication and recovery – re-establishing the perimeter and drive the adversary out
- Post-incident activity – lessons learned from the incident; how did we get here?

# LEAD INCIDENT RESPONSE CONSULTANT

CISO's Head of Incident Response has conducted and led hundreds of advanced cybersecurity programs, assessments, and large-scale incidents over an illustrious career spanning more than 20 years.

A seasoned consultant with deep expertise in emergency incident response, digital forensics, threat intelligence, threat hunting, ransomware/leakware (malware/actors/TTPs), network forensics, security architecture, and an expert in all the major cloud platforms. Working with and for companies of all sizes across a wide array of industry verticals and has been part of the security community for decades.

## Skill Summary

Expert in Ransomware Remediation/Forensics, Darknet, Security Architecture, Advanced Red Teaming, Cyber Forensics, Cloud Security (Azure, AWS, GCP, Digital Ocean), Zero Day Threat Prevention, IoT Infrastructure, Wireless Security, Phishing Prevention/Forensics, advanced scripting (PowerShell, Python).

## Past Roles

- Forensics and Red Team Lead (2019 - Present)
- Chief Cyber Security Officer (2019-Present)
- Vice President of IT & Security (2017-2019)
- CISO and VP of Infrastructure (2012 - 2017)
- VP of Infrastructure and Security (2011-2012)
- Director of IT Security (2009 - 2011)
- Security Manager (2006 - 2009)
- Director of Security (2002 - 2006)

## Certifications

- Certified Ethical Hacker (CEH)
- Certified Expert Pen Tester (CEPT)
- Certified Forensic Hacking Investigator
- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- Certified PCI 3.2 Professional
- Certified Penetration Tester (GPEN)

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