

INCIDENT RESPONSE

When you are under attack, we bring structure, experience and technology to help you contain the attack, regain control of your systems, and get back to business as quickly as possible.

Our incident response teams and specialists include engineers from elite cybersecurity teams within the US Government. We have a deep understanding of emerging and veteran threat actors' tactics, techniques and procedures, and apply this knowledge to handle your incident quickly and efficiently.

Cyber attacks can damage more than just your technical or data- they also impact your reputation, customer confidence and liabilities. Consequently, in addition to technical investigation, containment and recovery, our incident response services include a full suite of crisis management support options, critical for assisting with executive communication and crisis management.

MOBILIZATION AND PREPARATION

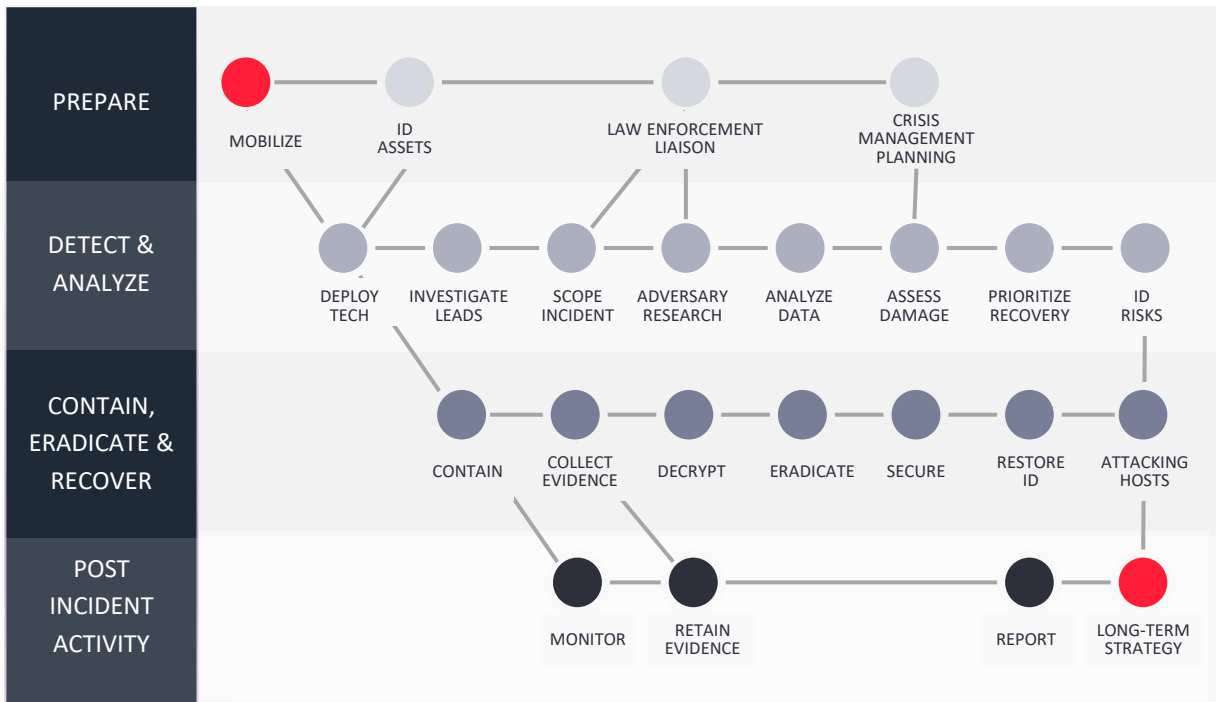
When you are under attack, every second counts. We immediately mobilize a multi-functional team of experts to start managing the incident with your internal team. Your Loki IR team includes experienced cybersecurity engineers, malware engineers, encryption specialists, intelligence analysts, threat hunters, security operations engineers, testing specialists and infrastructure architects.

In addition, our team includes liaison officers for IR interfacing with law enforcement to ensure you get every available assistance, insurance specialists, legal advisors and your executives and other stakeholders. It also includes security and trust restoration specialists to assist you build a proactive PR strategy and communication plan, as well as a longer term security strategy to rebuild trust with your various stakeholders.

INCIDENT RESPONSE SERVICES

- **24x7 incident response coverage** and threat monitoring across all platforms through our inhouse security operations center
- **Malware analysis**, cracking & decryption research
- **Threat intelligence** including OSINT adversary research, vulnerability research and security assessments
- **Breach containment** and isolation, and asset recovery and remediation
- **Investigations and analysis** including hunting for existing vulnerabilities and potential backdoors, and full forensic investigative processes
- **Ransom and extortion** management and negotiations where appropriate
- **Recovery and remediation** including developing parsers, decoders and other automated tools designed to efficiently clean and recover your assets
- **Security strategy** including network hardening advice, architecture review, and solution sourcing
- **Crisis management support** including emergency planning, communications, public relations, disclosure support
- **Key stakeholder liaison** support including law enforcement, insurance and legal liaison services





DETECTION & ANALYSIS

We deploy cloud and on-premise technology solutions and endpoint agents where appropriate to enable detection and analysis to commence almost immediately. We investigate the telemetry from these solutions, as well as your other devices, to begin to analyze the source, scope and vectors of the attack. Threat intelligence specialists and liaison officers engage with threat databases, law enforcement and other sources to build a profile of the attackers and their likely tactics and techniques. We then assess likely damage, agree with you an appropriate recovery plan.

While this is going on, our security assessment specialists analyze your network and proprietary code for other vulnerabilities that these or other attackers could exploit, while hunters look for potential backdoors left by attackers.

CONTAINMENT, ERADICATION AND RECOVERY

While analysis is ongoing, we work with you to contain the attack while collecting evidence for forensic purposes. Our malware engineers write automation tools to rapidly apply available decryptors and eradicate malware in your network, while also assisting with data restoration.

POST INCIDENT ACTIVITY

Our 24x7 security operations center maintains constant vigilance on your network, while incident response leads package evidence and complete necessary incident response reports for your executive, insurance and other third-party purposes. Finally, our security architects and strategist work with you to develop a long-term security strategy, and deliver tasks to restore trust with your customer, employee, and financial stakeholders.

Loki Labs Inc

13431 Heswall Run, Orlando FL 32823
 888.565.4522 / 888.LOKI.LABS
 info@lokilabs.io

A service-disabled veteran owned small business.

