BINARY DEFENSE

Incident Response Service

Rapid Response by Experienced Responders for Swift Remediation.

When an incident occurs in your environment, our experienced responders bring a proven playbook and work as an extension of your team to contain and eradicate malicious actors from your environment. When the security incident is remediated our responders provide mitigation and strategic recommendations to strengthen your security posture against future threats.

Rapid Response

With 24x7x365 response capabilities, we ensure that no matter the time or day of a security incident, our team is standing by and ready.

Experienced Responder

Our Incident Responders have years of experience remediating a wide range of attacks and environments. They are mission-focused on rapidly restoring your operations.

Proven Playbook

When an incident occurs, our responders act swiftly, armed with a tried and tested set of documented procedures and processes that are customized to your environment and incident type.

Active Cyber Defense

The responders are not the only team you have access to during an incident. Our service includes a team of dedicated analysts and an in-house Threat Intelligence Platform to drive rapid insights and response actions.

600 Alpha Parkway
Stow, OH 44224
binarydefense.com
sales@binarydefense.com

Incident Response Playbook:

Be ready when an attacker strikes. The right partner is the best defense.

Plan

Our goal is to be an extension of your team. Incident Responders work with your team to understand your environment and customize our proven playbook of procedures and processes to ensure that when a security incident occurs, a rapid response action plan is already established.

Detect

Threat Actors can hide within your environment without you knowing for days or weeks. Our Managed Detection & Response solution is built from an attacker-mindset to detect even the stealthiest of attacks.

Contain

If security tools have not already contained the threat, our Incident Responders and Threat Hunters quickly work to detect and contain the threat to prevent further damage.

Investigate

A complete investigation of the incident is conducted to determine the severity and scope of the attack. Incident Responders will document the investigation using both Cyber Kill Chain and MITRE ATT&CK frameworks to build a replica of the attack lifecycle and identify Indicators of Compromise.

Remediate

Leveraging the intelligence gained from the investigation, Threat Hunters diligently hunt through your entire environment looking for any hidden exploits or payloads while Incident Responders work directly with your team to eradicate the attacker from your environment and help restore the affected systems.

Strengthen

With the attacker eradicated from your environment and systems restored, our team provides a detailed report of the incident with tactical and strategic recommendations and guidance on strengthening your security posture and attack surface. These include new or tuned detections, security controls and more.

BINARY DEFENSE

600 Alpha Parkway
Stow, OH 44224
binarydefense.com
sales@binarydefense.com