

CYBERSECURITY SERVICES

Quickly and effectively respond to cyber incidents using trusted techniques and tools to assess, halt, and recover your organization from malicious cyber attacks.

INCIDENT RESPONSE

INCIDENT RESPONSE ACTION PLAN

Preparation: BlueSky's cybersecurity professionals will work with you to determine the scope of the incident, including any constraints or compliance requirements for your organization.

Identification: BlueSky's team will work to identify any active and potential threats to your organization, including infected machines, malicious insiders, network gaps, compromised credentials, and/or data exfiltrated.

Containment: Once the threats have been identified, BlueSky's Incident Response team will work to contain such threats with both short-term and long-term tactics. This containment involves quarantining of infected or compromised systems, access revocation of malicious insiders, limitation of data exfiltration, and more.

Eradication: After threats have been identified and contained, BlueSky's professionals will eradicate such threats from the environment with cleaning/purging of malware and rootkits, decommissioning of systems, removal of malicious artifacts, and more.

Recovery: BlueSky will help you through a seamless recovery with reconstruction of assets and post-eradication of threats. This includes the hardening of environmental gaps that have been identified as routes to compromise, re-imaging of systems, implementation of security controls to combat further related and unrelated threats, and more.

Our security team is experienced in the field of cyber-incident response and has responded to both small-and large-scale attacks. Contact us to get started.

