Breach Response Services

APPALACHIA TECHNOLOGIES, LLC.

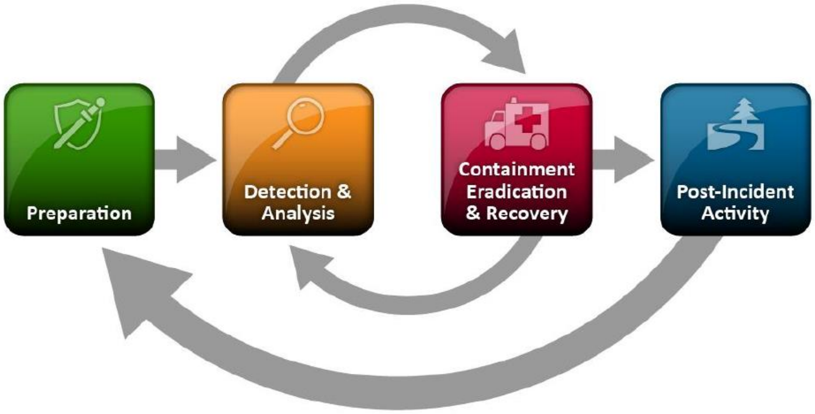
If you suspect your organization has been compromised, we can help. From rogue insiders to unknown outsider threats, Appalachia's Cybersecurity Breach Response establishes an efficient, effective and orderly response to a cybersecurity related condition(s).

The goal of Breach Response is to:

- Limit/minimize further loss of profits and information assets.
- Identify, contain, and rapidly respond to the condition(s) reported.
- Assess and ascertain the extent of the condition(s) reported quickly and effectively.
- Communicate our findings to the appropriate stakeholders within the Client's organization.

Our Approach

Appalachia's Incident Response service is based on the NIST 800-61 incident response procedures guidelines and follows this framework when conducting consulting services related to incident response including Preparation, Detection & Analysis, Containment Eradication & Recovery, and Post-Incident Activity. This approach allows Appalachia to give standardized response services in cases of a cybersecurity incident.



Preparation

- Gather All Information about Security Incident
- Review Reported Indicators of Compromise
- Conduct Interviews with Relevant Team Members

APPALACHIA TECHNOLOGIES, LLC.

Detection and Analysis

- Perform network packet capture as needed
- Analyze Network Traffic Data for indicators of compromise
- Analyze and Correlate Log Data
- Investigate any potentially compromised systems
- Analyze Systems for malicious activity
- Identify root cause of malicious traffic

Containment, Eradication & and Recovery

- Block, Prevent or Stop any current attack
- Implement Steps, including, but not limited to
    - Coordinated Shutdowns
    - Antivirus Scans and Updates
    - Firewall Changes
    - Security Application Service Changes
    - Assist in recovery efforts

Post-Incident Activity

- Appalachia will provide a formal report of findings.
- Recommended additional steps to remove/remediate the cause of the threat.
- Our determination of the impact of the exposed sensitive data where possible.
- Outline existing Client vulnerabilities (system, staff etc.) based on our findings.
- All raw information/data gathered.

Pricing

A one-time mobilization fee will be assessed, then an hourly T&M rate will be incurred for the actual number of hours worked. The Mobilization Fee is based on the Client's need for engagement of Appalachia resources. For Emergency-based mobilization, Appalachia will work around existing commitments to ensure the resources are assigned and equipped for immediate engagement.

Proactive vs Reactive

When it comes to your cybersecurity strategy, prevention is better than recovery! That's why Appalachia provides **24/7 Managed Detection and Response**.

Proactive Threat Detection

We monitor network traffic for suspicious activity or anomalous behavior.

Suspicious patterns are verified against known attack signatures and other indicators of compromise for early detection of active threats.

Threat Response

Our security analysts investigate events real-time to identify and alert you of potential threats in your environment.

Once confirmed, our team works quickly to isolate and eradicate threats before they can spread further within your environment, or worse… your clients.

Compliance

Stay ahead of compliance requirements and auditors with regular reports to show progress towards compliance as well as identify weak spots in your environment.

Meet compliance requirements such as PCI-DSS, NIST CSF, HIPAA, ISO 27001, CJIS, SOC 2, and more.

Contact us to learn more or to schedule a demo!