EITS
Enterprise IT Security

Incident Response

To beat an attack you must think like a hacker.

Incident response is a systematic approach to addressing the aftermath of a security breach or attack. The primary goal is to manage the incident in a way that limits damage to an organization, while reducing the time and costs associated with recovery efforts.

Why is Incident Response a Challenge?

The unpredictability and increasing volume of attacks and subsequent alerts make it impossible for your internal security team to monitor and investigate alone. It is not realistic or financially feasible for an organization to attempt to hire the problem away.

According to a survey by Enterprise Strategy Group, incident response efficiency is limited by the time and effort spent on manual processes.

Survey respondents stated they had big plans to increase the use of orchestration and automation for incident response, with 97% either automating some of their incident response plans already or planning to do so in the following 18 months.

Only one-third of survey respondents considered their automation projects "mature."

Prioritizing threats requires experienced security professionals to make educated decisions about what to address or ignore; without this expertise, it is often difficult to determine which elements are low-priority versus which should be investigated immediately.

24/7x365 Incident Response

The security experts at EITS are available 24/7x365. You never know when or how attackers will strike; EITS' readily accessible and experienced staff is always poised to respond with our unique incident response approach. Our average time to have incident responders on-site is less than 12 hours.

Total Business Coverage

Our security experts familiarize themselves with your network and business operations the day we partner with you to ensure the fastest-possible results. When we respond to an incident, we coordinate remediation efforts to address the full extent of the threat, not just individual symptoms.

Specialized Incident Response Team

Our security incident response team includes GIAC Certifi ed Incident Handlers to expertly manage remediation activities, threat intelligence experts to rapidly discover and remediate threats across your enterprise, and GIAC Certifi ed Forensics Examiners to ensure the fastest time to unravel what malicious activity occurred.

Custom Incident Response Plan

We work with your team to develop the fastest, most effective Incident Response Plan for your enterprise, customized according to your unique situation and needs. This Incident Response Plan will be communicated to you with regular updates to ensure rapid and effective deployment.

Defense Strategy

EITS' defense strategy involves both endpoint and network detection tools and techniques; this approach ensures that all malicious activity can be identified and averted.

Tailored Prevention Recommendations

EITS security experts will review each incident to make architectural recommendations that will limit the opportunity for future incidents.

(704) 900-8042 www.eits.com info@eits.com

A proven plan to neutralize the modern threat landscape

The Difference Is in the Eits Approach

Once engaged, EITS' average time to have incident responders on-site is less than 12 hours. Our unique approach utilizes cloudbased and on-premises response solutions so investigations can begin quickly.

Within hours, our security experts will coordinate with your team to develop a customized Incident Response Plan; this allows our responders to begin analyzing network traffic and endpoint artifacts as fast as possible. EITS has partnered with multiple threat intelligence partners, enabling our incident response team with the latest attack indicators of compromise (IOC) in addition to attacker tactics, techniques, and procedures (TTP).

The experts at EITS understand that an incident response engagement extends beyond just the technical investigation, which is why we assist with executive communication and crisis management; this can include legal, regulatory, and public relations considerations. Crisis management is critical for controlling reputational damage and legal liabilities.

EITS offers a security monitoring service that takes place in conjunction with the remediation phase. While your staff is recovering from the incident, our experts monitor your environment to ensure there is no new malicious activity; this allows EITS to ensure your company the smoothest return to business operations.

Our Process Provides Peace of Mind

EITS engagements include client, network, and behavioral analyses for a comprehensive assessment. Our response actions are tailored to help organizations respond to and recover from an incident, while managing regulatory requirements and reputational damage.

During engagements, EITS typically identifies:

- Total time of incident exposure
- Compromised systems, applications, and user accounts
- Malicious software
- Exploited security gaps
- Accessed and exfiltrated business documents

Real World Example of an Incident Response

1. Develop and document a detailed response plan based on the customer's environment.
2. Deploy the appropriate technology to ensure a fast and comprehensive incident resolution. Our team simultaneously investigates all leads while performing behavioral analysis to start building indicators of compromise that will identify attacker activity.
3. Work with executives, legal teams, business leaders, and senior security personnel to develop a crisis management plan.
4. Analyze the attacker's actions to determine the initial attack vector, establish timeline of activity, and identify extent of compromise.
   This can include:
   - Live analysis
   - Malware analysis
   - In-Depth Forensic analysis
   - Network traffic analysis
   - Log analysis
   - Browser analysis
   - Email analysis
5. Identify impacted systems, users, applications, and sensitive information. Develop a custom containment and remediation strategy based on the actions of the attacker that is tailored to the needs of the business; this will eliminate the attacker's access and improve the security posture of the environment to prevent reinfection.
6. Assist in developing a recovery plan; this includes training your staff on how to monitor any technologies used in the Inci-dent Detection process. EITS staff is also available to aid in the recovery process.
7. Provide security architectural guidance to minimize the risk of future attacks.
8. Offer security monitoring to give you peace of mind. Our security experts work with your team(s) to prioritize and provide guidance on new incidents.

Verified skills produce real results.

GCED GDSA GCWN GSEC GCIH GWAPT GPEN GCFE C|NDA Certified Network Defense Architect C|EH Certified Ethical Hacker

(704) 900-8042 www.eits.com info@eits.com