Incident Response (IR)

Rapid Response and Recovery Against Advanced Cyber Threats

When advanced threats like zero-day exploits, social engineering, or malware attacks gain access to your environment, the clock starts immediately. Swift and efficient response is critical to limit data loss and get back to business.

Cyber Defense Group's Incident Response (IR) solutions offer comprehensive cybersecurity incident management to secure, analyze, and restore an environment as quickly as possible. This service guarantees prompt threat detection, active containment, and will accelerate forensic analysis of sophisticated cyber attacks. Our IR solutions are essential for efficient incident handling, minimizing downtime and ensuring compliance with regulatory standards.

$9.48 MILLION Average cost of a data breach in the United States.

75% INCREASE Due to lost business costs & post-breach response actions.

Cyber Defense Group incident response services are proactive and reactive

When a breach occurs, you need an incident response team to provide swift and strategic management of security incidents. Our experience during reactive IR engagements feeds into our preparation proactively.

Incident Response Emergency Reponse
Activate Cyber Defense Group experts for rapid response and crisis management and recover business operations after a breach.

Incident Response Retainer
Retain Cyber Defense Group experts to enable a faster and more effective response to cyber incidents **PROACTIVELY**.

Compromise Assessment
Verifies if your system is clean, using threat intel, analytics, and hunting techniques to find malware, attacker activity, misconfigurations, risks, and vulnerabilities.

Tabletop Excecises
Test threats on-site to assess your detection and response capabilities in a controlled setting. Develop scenarios, review outcomes, and receive actionable insights for your IR strategy.

KEY CYBERSECURITY INCIDENT MANAGEMENT CHALLENGES

Outdated incident response plans
Organizations may have a compliance response plan, but it sits unused and untested.

Immediate response pressure and recovery time
Lengthy recovery times strain budgets and resources, affecting business performance.

Legal liability
Many organizations are ill-prepared and face legal risks when breached.

Cyber insurance coverage issues
Claims may be denied due to policy exclusions, insufficient coverage limits, or disputes over the cause/extent of damage can delay claim processing.

Complex damage control
Addressing cyberattack and identifying the root cause is complex, impacting operations and customer trust.

System and data recovery struggles
Struggling to quickly identify breach causes due to limited investigative resources and expertise.

Inadequate post-incident security methods
Improving security post-incident is a common challenge, exposing companies to future attacks.

Methodology and Approach
How Incident Response Works

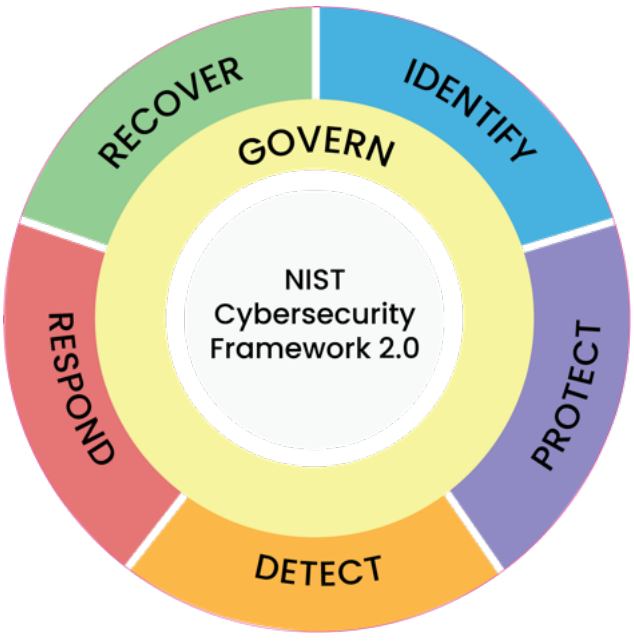
How it works

To stay ahead of advanced threats, you need a skilled team with access to top-notch experience against advanced attackers. Our incident response experts at Cyber Defense Group will help you understand and swiftly contain, remediate, and eradicate attacks. With a proven methodology and battle-tested tools.

It is evident that encountering a cyberattack on your organization is not a matter of "if," but rather "when." To attain cybersecurity readiness, a fresh approach to detection and response is crucial. This entails actively seeking out indications of existing or previous compromise.

Cyber Defense Group Incident Response steps to respond rapidly, mitigate impact, and restore operations

Cyber Defense Group's Incident Response soltuions align with the NIST Cybersecurity Framework and have been developed from extensive real-world experience investigating countless incidents. When incidents occur, we quickly respond to identify events, contain malware, eradicate threats, mitigate potential impacts and remediate and restore business operations. We prioritize your business's complete success and customer service from start to finish.



IDENTIFY
Detect and analyze the root cause of the breach to understand the point of entry and what data has been compromised.

PROTECT
Isolation of impacted systems and enpoints to prvent spread of malicious malware.

DETECT
Rapid containment of attacks and compromises are found and analyzed in the entire environment, including backups, privileged access, and security updates.

RESPOND
Actions are taken on eradicating attacks and compromises, taking steps to safely find and analyze the threat.

RECOVER
Focus is on restoring affected systems. Testing, monitoring, and verifying a clean operating environment to avoid future incidents and impact on business operations and reputation

GOVERN
An organization's cybersecurity risk managment strategy, expectations, and policy are established, communicated, and monitored.

Why Choose Cyber Defense Group?

Get back to business faster with Cyber Defense Group's expert solutions for Incident Response planning

Discover how Cyber Defense Group experts can enable your organization to quickly and effectively mitigate the impact of security incidents, minimize down time, financial loss, and reputational damage. Contact us to learn more about the benefits of proactive incident response planning.

CONTACT US FOR A CONSULTATION

About Cyber Defense Group

Cyber Defense Group offers mid-market to enterprise businesses bespoke cybersecurity programs, overcoming increased complexities and evolving threats. Our unique blend of strategic consulting and technology ensures business resilience and success at a predictable cost, setting us apart from traditional IT services and open-ended consulting engagements.

At Cyber Defense Group, your protection is not just our priority–it's our passion.

OUTCOMES-BASED SECURITY™ FOR ROBUST INCIDENT RESPONSE

Methodology and approach for swift incident resolution
Leverage our team's people and processes, recover faster from incidents, minimize breach impact, downtime, and data loss.

Expertise and skilled response
Leverage our team's wealth of expertise to swiftly investigate threats and implement effective counter measures, ensure your organization's security and peace of mind.

Efficient and Cost-effective
Save time and money by accessing expert responses without the hassle of recruitment, training, and cost of an internal team.

Comprehensive proactive prevention
Identify vulnerabilities, take preventive action to boost security, and avert breaches with end-to-end support.

Enhance preparedness and response capabilities
Comprehensive reviews and practical suggestions for your Incident Response Plan, with runbook templates and annual tabletop exercises.

Reduce legal liablity
Our method of response ensures the maximum amount of legal coverage, including working with outside counsel to preserve attorney / client privilege.

info@cdg.io www.cdg.io