

Incident Response: How to Handle and Mitigate a Cyber Attack

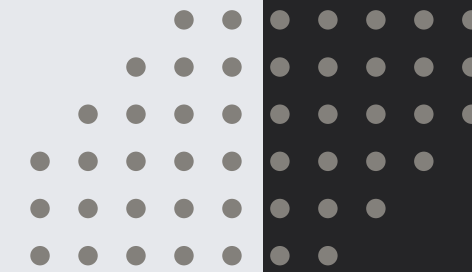
GROUP
6424e

PRESENTED BY

Presented by [Esmer
Seyidova]



AZERBAIJAN
TECHNICAL
UNIVERSITY



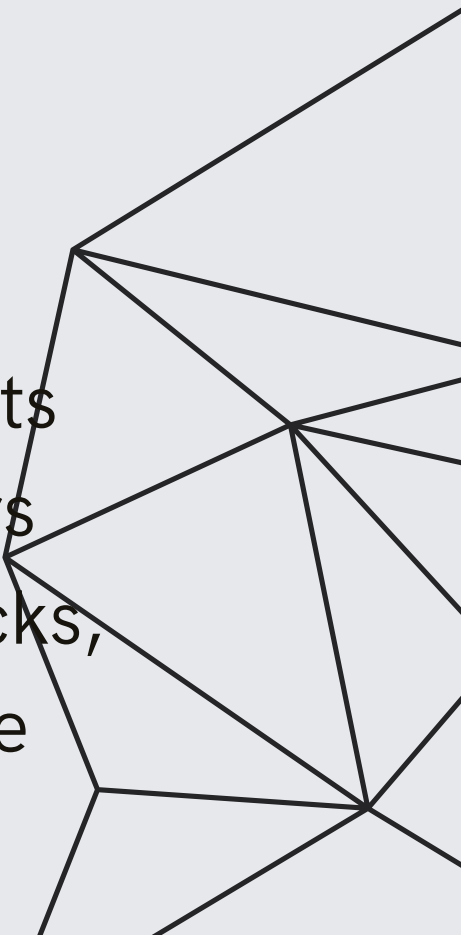


Introduction



In an era where digital connectivity defines the operational backbone of organizations, cybersecurity has become an essential priority. The increasing frequency and sophistication of cyber threats demand a structured approach to incident response (IR)—a comprehensive strategy designed to detect, respond to, and recover from cyber attacks effectively. Without a well-defined incident response plan, businesses risk substantial financial losses, reputational damage, and regulatory consequences.

Cybercriminals employ various attack vectors, including ransomware, which encrypts files and demands ransom payments; phishing, where malicious actors deceive users into disclosing sensitive information; and Distributed Denial-of-Service (DDoS) attacks, which overwhelm networks, rendering them unusable. These threats underscore the importance of incident response in today's digital landscape.





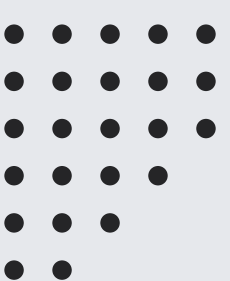
What is Incident Response?

Incident response refers to the structured approach organizations take to identify, contain, and mitigate security incidents. It plays a pivotal role in cybersecurity strategy by ensuring rapid action during a breach.

Objectives of Incident Response:

- Minimize damage caused by cyber attacks
- Reduce recovery time and costs
- Preserve trust and reputation

A well-executed IR process safeguards digital assets, preventing disruptions that can cripple businesses.





The Cyber Attack Lifecycle

Cyber attacks follow a systematic progression:

Reconnaissance – Attackers gather intelligence on their targets.

Intrusion – They exploit vulnerabilities to gain unauthorized access.

Exploitation – Malicious actors leverage compromised systems.

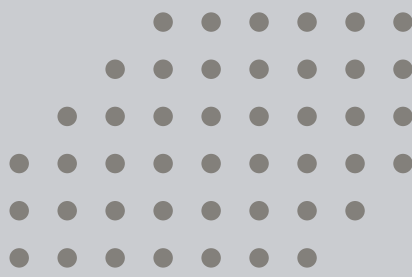
Command & Control – Remote control over infected devices.

Actions on Objectives – The final execution of malicious intent, such as data exfiltration or system disruption.

Understanding these stages helps organizations prepare effective countermeasures

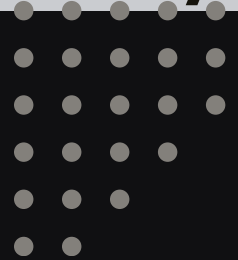


Why an Incident Response Plan Matters



A well-structured IR plan is essential for organizations to act decisively during cyber incidents.

Key Benefits



Quick decision-making



Enables timely and informed responses.

Regulatory compliance



Aligns with legal obligations (e.g., GDPR, HIPAA).

Preserves brand reputation



Ensures customer trust is maintained.

Without an IR plan, organizations may struggle to contain threats efficiently, exacerbating security risks.





Key Components of an IR Plan

An effective IR plan consists of four critical phases:


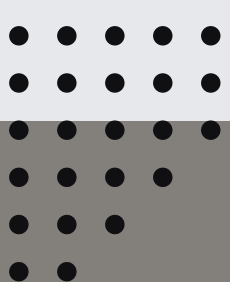
Preparation– Implementing preventive measures and training personnel.

Detection & Analysis – Identifying attack indicators and assessing impact.

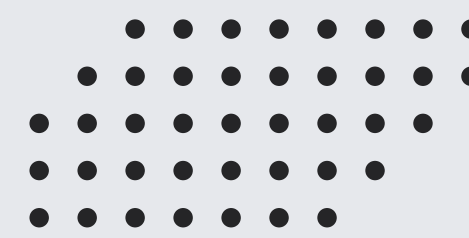
Containment, Eradication, Recovery – Neutralizing threats and restoring operations.

Post-Incident Activity – Learning from the breach and refining response strategies.

Each phase is instrumental in ensuring long-term cyber resilience.



Preparation Phase



Organizations must proactively equip themselves for cybersecurity threats. **Preparation** includes:

Defining roles and responsibilities within the IR team.

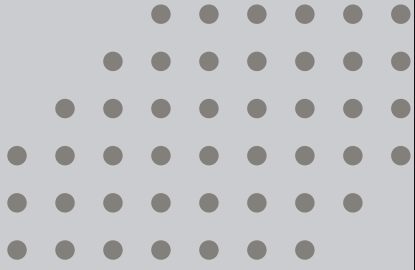
Training incident response teams to react efficiently.

Developing policies, procedures, and technologies for threat mitigation.

A well-trained team enhances the speed and effectiveness of response efforts



Detection & Analysis



Quick and accurate threat detection minimizes cyber attack damage.

Signs of Compromise:

Unexpected system behaviors.
Irregular network traffic or unauthorized logins.
Security alerts triggered by monitoring tools.

Security Tools:

Security Information and Event Management (SIEM) for threat analysis.
Intrusion Detection/Prevention Systems (IDS/IPS) to monitor vulnerabilities.
Endpoint detection solutions for identifying malware infections.

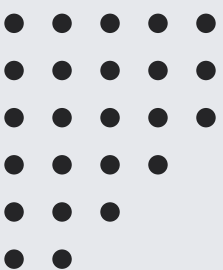
Timely detection ensures attackers are stopped before significant harm occurs

Containment Strategies

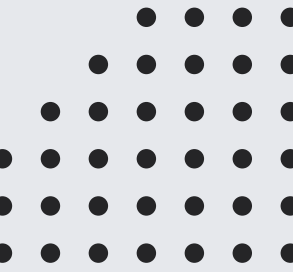
Containment prevents the further spread of cyber threats.

- Short-term containment – Immediate system isolation.
- Long-term containment – Structured efforts to secure affected assets.

By limiting attacker movement, organizations regain control over compromised systems.



Eradication



Threat actors and malicious software must be removed entirely.

Steps in Eradication:

Eliminating malware infections.

Patching system vulnerabilities.

Strengthening security defenses to prevent future breaches.

Secure systems reduce the risk of repeated attacks.





Recovery

Post-eradication, organizations must ensure business continuity through secure recovery processes.

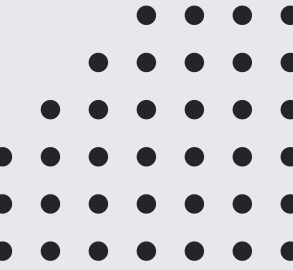
Recovery Measures:

- Restoring systems from backups.
- Monitoring for residual threats.
- Conducting integrity verification tests to confirm system security.
-

Proper recovery ensures uninterrupted operations following an incident.



Post-Incident Activity



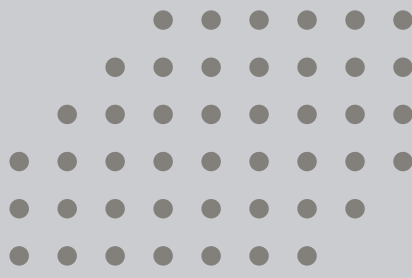
Once an incident is resolved, reflection and refinement are crucial

Recommended Actions:

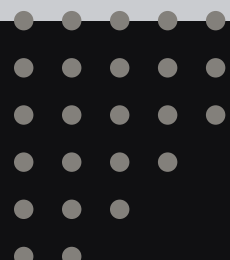
- Conduct **lessons-learned meetings** for continuous improvement.
- Update **IR policies and procedures** based on findings.
- Report security breaches to **stakeholders and regulatory authorities** as required.

This ensures that past mistakes are mitigated in future responses.

Building the IR Team



Incident response requires collaboration among various specialists:



Incident Response Manager

**Oversees
cybersecurity
operations.**

Security Analysts

Investigate and
neutralize threats.

**Legal, Public Relations, IT, and HR
experts**

Manage compliance
and communications.

Some organizations rely on external cybersecurity firms to supplement internal response capabilities.





Communication During Incidents

Transparent communication prevents misinformation and panic.

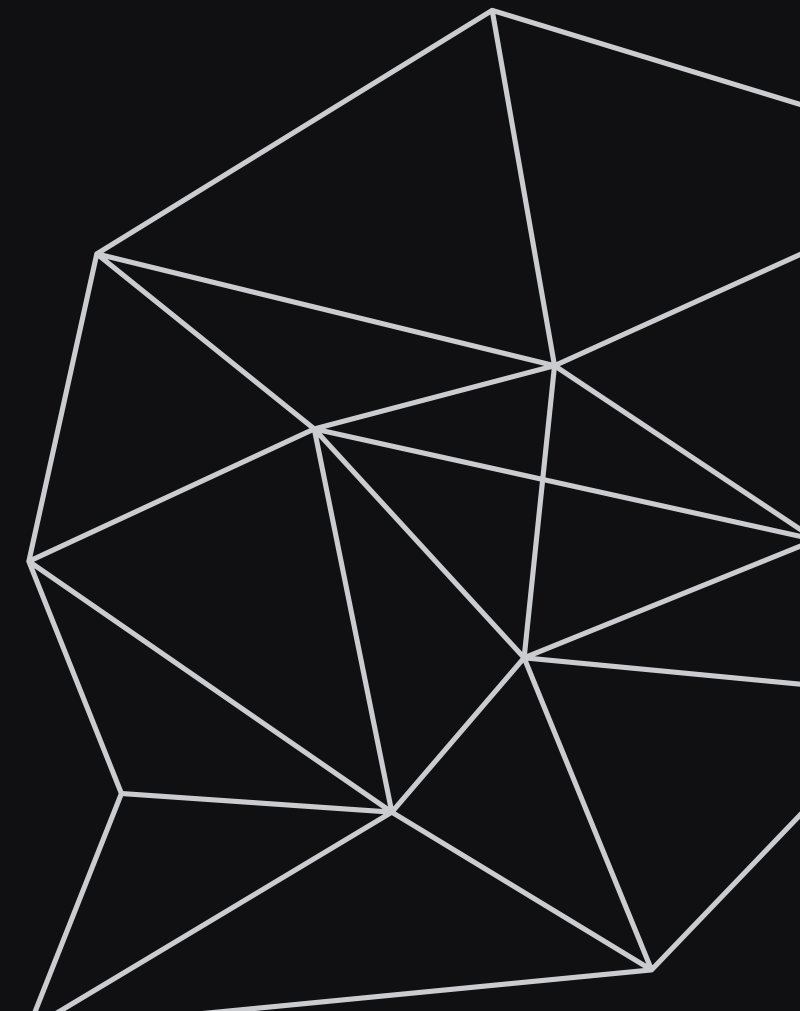
Key Communication Areas:

Internal coordination between response teams.

External messaging for customers, partners, and media.

Legal compliance reporting for regulatory transparency.

Clarity ensures trust and minimizes reputational damage.



Real-World Example: Notable Cyber Incidents

Studying past incidents enhances response preparedness:

Equifax Data Breach (2017): Poor patch management exposed personal data.

SolarWinds Hack (2020): Supply chain attack infiltrated major organizations.

Target Breach (2013): Attackers exploited third-party access credentials.

Each case highlights the importance of **proactive cybersecurity defense**.



Tools & Technologies for IR

Reliable cybersecurity tools streamline incident response:

SIEM Platforms: Splunk, QRadar.

Endpoint Detection & Response (EDR): CrowdStrike, SentinelOne.

Incident Ticketing Systems for tracking investigations.

Technology-driven solutions enhance security monitoring capabilities.

Common Mistakes in IR

Organizations must avoid critical IR failures:

- Lack of preparation before incidents occur.
- Delayed response leading to prolonged damages.
- Poor documentation preventing future improvements.
- Failure to involve legal teams early.

Avoiding these mistakes ensures efficient cyber defense operations.

Metrics to Measure IR Effectiveness

Performance tracking improves cybersecurity strategies.

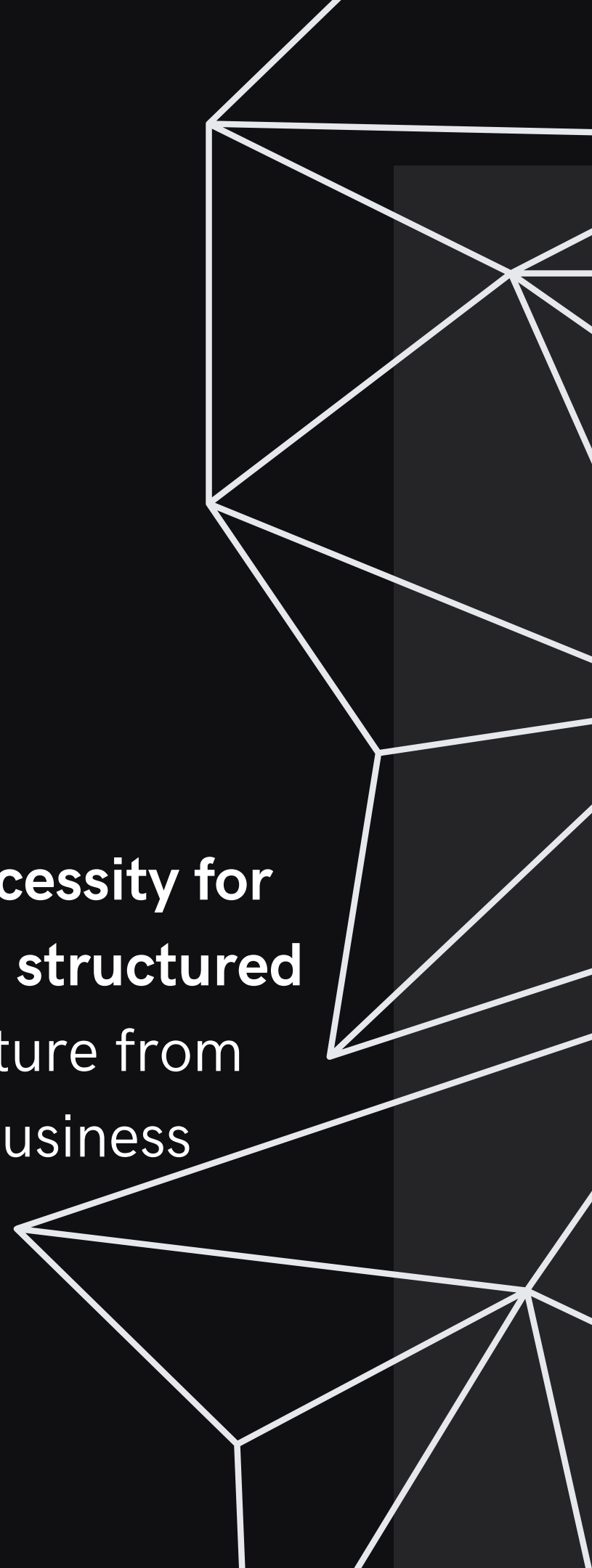
Key Metrics:

- Mean Time to Detect (MTTD) – Speed of attack identification.
- Mean Time to Respond (MTTR) – Efficiency of containment measures.
- Incident resolution rate – Number of successfully handled cases.

Data-driven insights enhance future security improvements.

Conclusion

Incident response is not merely a security protocol—it is a **fundamental necessity for cybersecurity resilience**. Organizations must prioritize **proactive planning, structured training, and continuous improvement** to safeguard their digital infrastructure from evolving cyber threats. Investing in cybersecurity readiness today ensures business continuity and trust in the long run.



**thanks for your
attention**

