IT Incident Response Playbook

A comprehensive training guide for responding to IT security incidents effectively

Why Incident Response Matters

This playbook outlines a structured workflow for responding to IT security incidents effectively. Each step is designed to minimize the impact of incidents while ensuring a systematic approach to resolution and recovery.

A well-prepared incident response strategy reduces downtime, protects sensitive data, and ensures business continuity during security events.

The Six-Step Response Framework

01

Preparation

Establish foundation with policies, procedures, and trained teams

02

Detection and Identification

Identify and classify potential incidents through monitoring

03

Containment

Limit the spread to reduce damage and preserve evidence

04

Eradication

Eliminate the root cause from the environment completely

05

Recovery

Restore systems and services to normal secure operation

06

Post-Incident Analysis

Review and improve future response processes

Step 1: Preparation

Establish a foundation for incident response. This includes creating and maintaining policies, procedures, and tools. Ensure team members are trained and have access to resources.

Develop an Incident Response Plan

Create comprehensive documentation outlining procedures, roles, and escalation paths for various incident types.

Identify Roles and Responsibilities

Assign clear ownership for incident management, technical response, communication, and coordination activities.

Conduct Regular Training

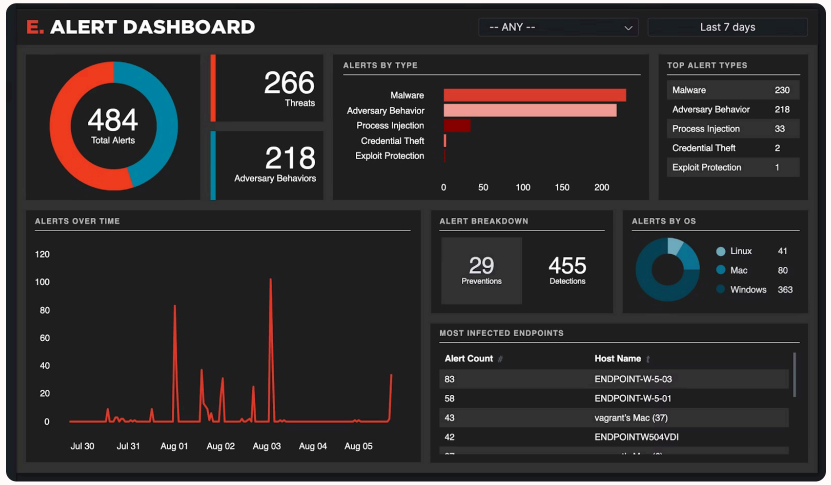
Run simulations and tabletop exercises to ensure team readiness and identify gaps in response capabilities.

Step 2: Detection and Identification

Identify potential incidents through monitoring tools, user reports, or automated alerts. Classify the incident type and prioritize it based on severity.

Key Actions

- Monitor systems using SIEM tools like Splunk or QRadar
- Analyze alerts and logs for suspicious activity
- Categorize incidents: malware, phishing, DDoS, data breach
- Prioritize based on impact and urgency



Step 3: Containment

Limit the spread of the incident to reduce damage. Choose between short-term containment for immediate response and long-term containment for system isolation.

Disconnect Systems

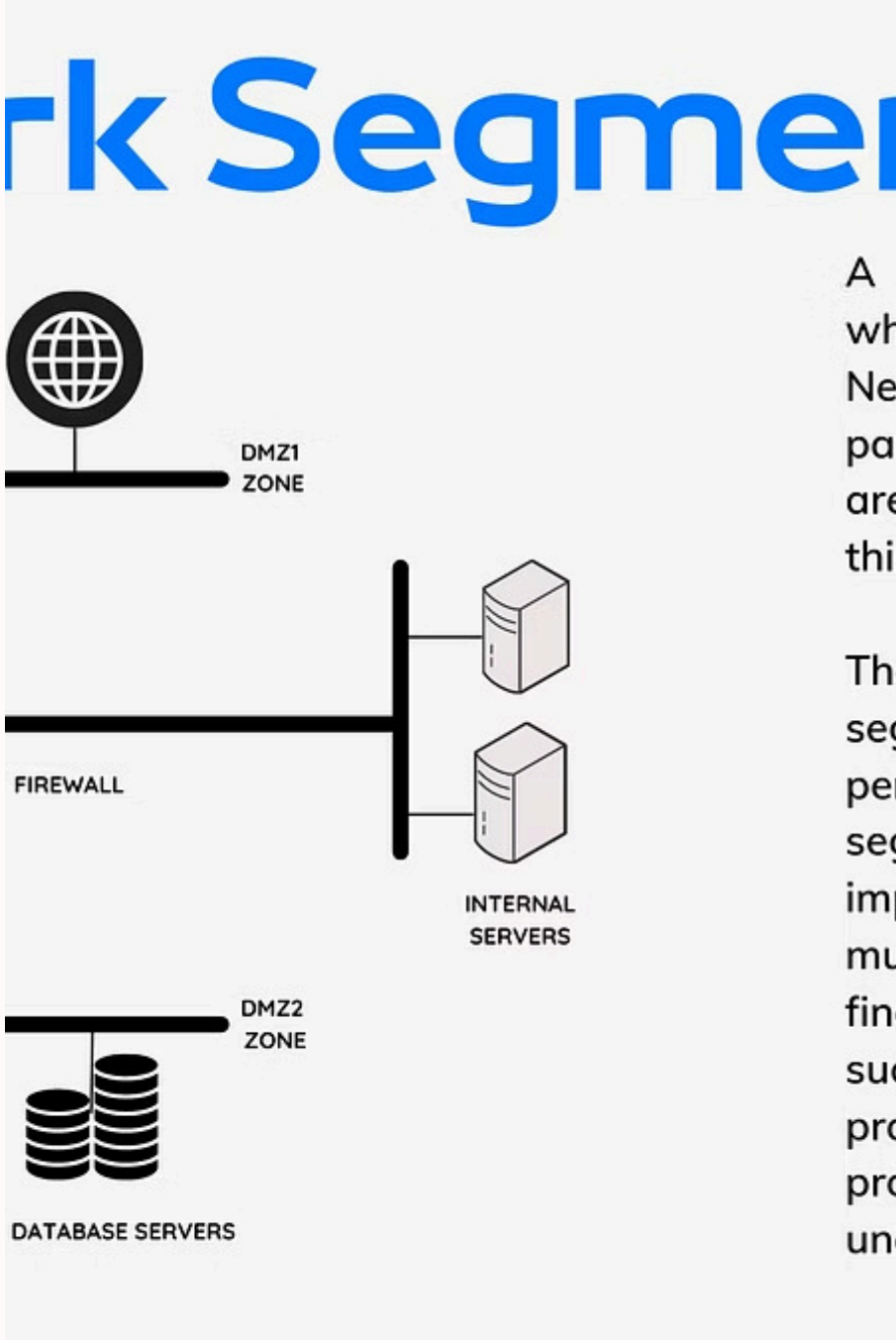
Isolate affected systems from the network to prevent lateral movement

Apply Firewall Rules

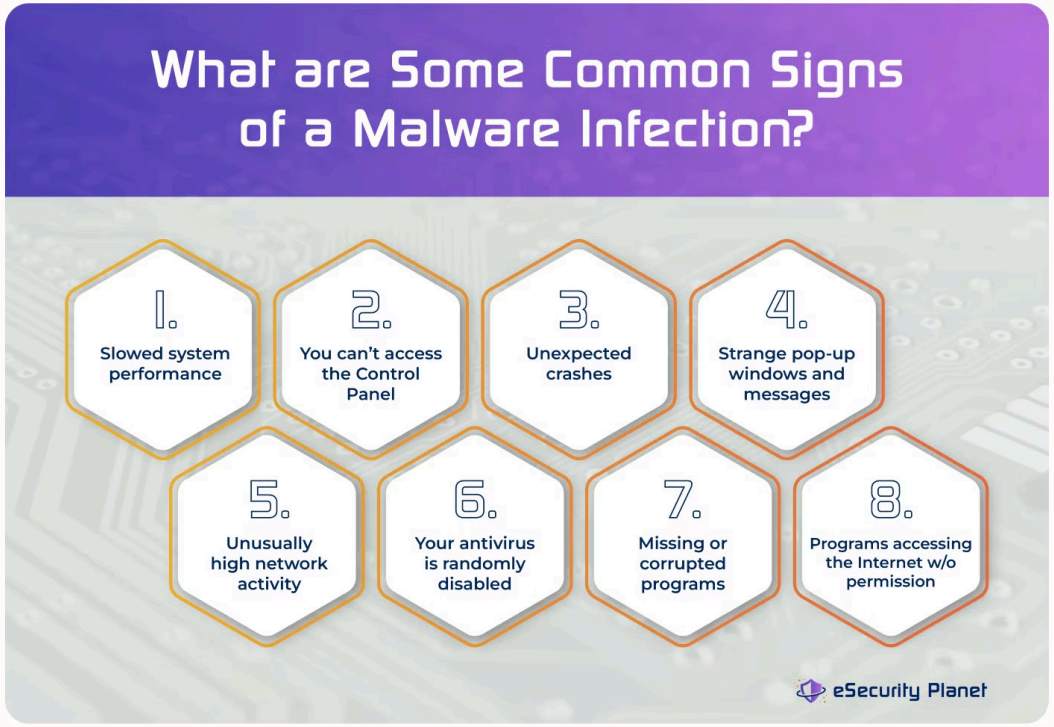
Block malicious traffic and IP addresses at the perimeter

Preserve Evidence

Capture logs, memory dumps, and system states for analysis



Step 4: Eradication



Eliminate the root cause of the incident from the environment. This step ensures the threat is removed entirely and systems are clean.

Critical Actions

1. Remove malware and close vulnerabilities
2. Revoke compromised credentials immediately
3. Patch systems and update antivirus tools
4. Perform thorough system scans
5. Verify complete threat removal

Step 5: Recovery

Restore affected systems and services to normal operation while ensuring they are secure and monitored for residual activity.

1. **Rebuild Systems**

   Reconstruct compromised systems from clean images if necessary

2. **Restore Data**

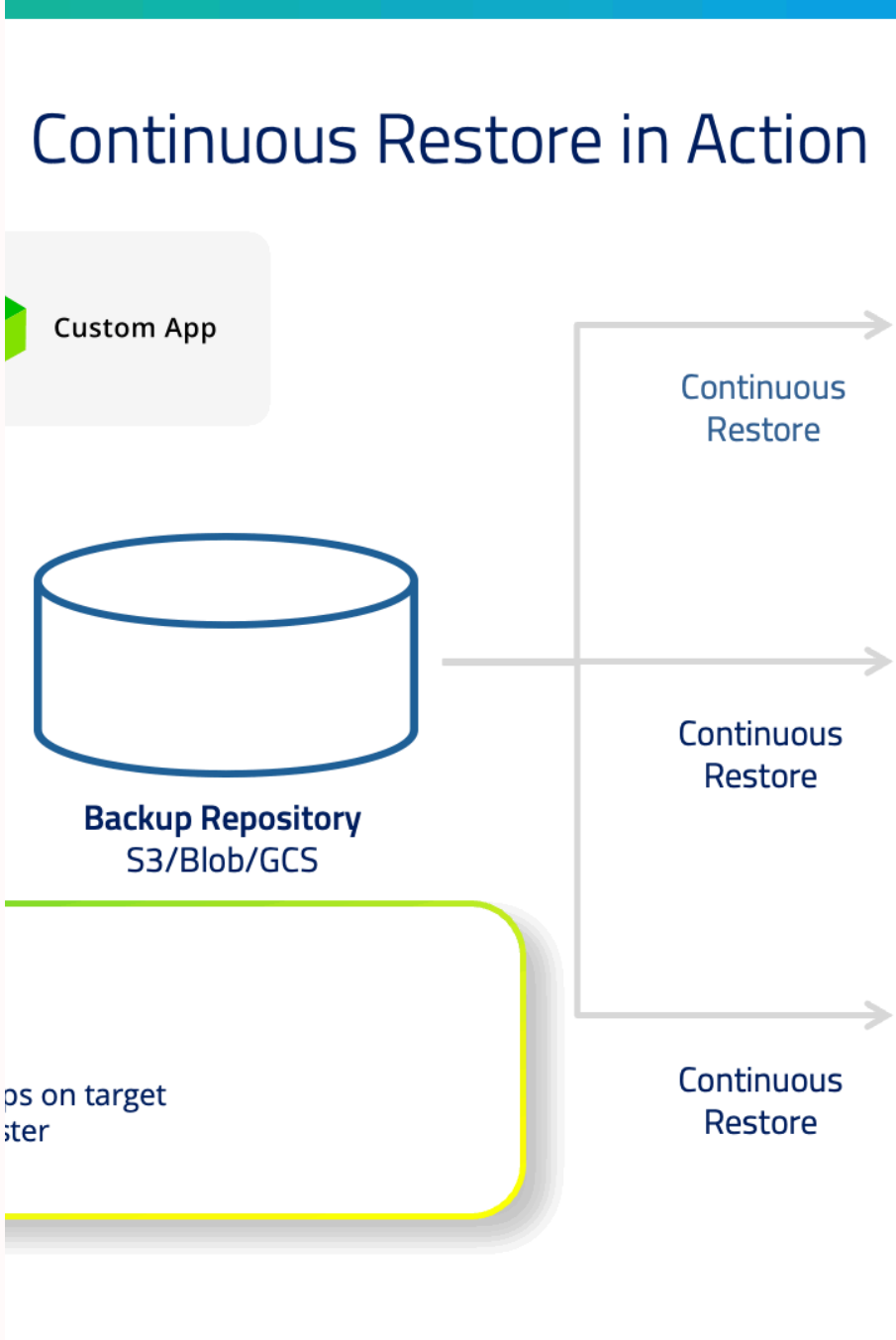
   Recover information from verified clean backups

3. **Monitor Activity**

   Watch for unusual behavior during recovery period

4. **Validate Security**

   Confirm all systems are secure before full restoration



Step 6: Post-Incident Analysis

Document Everything

Record incident details, timeline, actions taken, and outcomes for future reference and compliance.

Analyze Performance

Review what worked well and identify areas for improvement in detection, response, and recovery.

Update Procedures

Revise policies, playbooks, and training materials based on lessons learned from the incident.

Conduct a review meeting with the Incident Response Team to ensure continuous improvement and knowledge sharing across the organization.

Essential Tools for Each Step

Preparation

Policy documents, training platforms like Cybrary, incident response templates

Detection

SIEM tools, IDS/IPS systems, endpoint protection platforms

Containment

Firewalls, network segmentation tools, access control systems

Eradication

Antivirus tools, patch management systems, vulnerability scanners

Recovery

Backup solutions, system rebuild utilities, disaster recovery tools

Analysis

Documentation templates, analytics platforms, reporting tools

Incident Response Team Structure

A well-defined team with clear roles ensures efficient incident handling and minimizes confusion during critical situations.

Incident Manager

Leads response effort, coordinates resources, and communicates with stakeholders

System Administrator

Provides technical support, investigates affected systems, applies remediation steps

Network Administrator

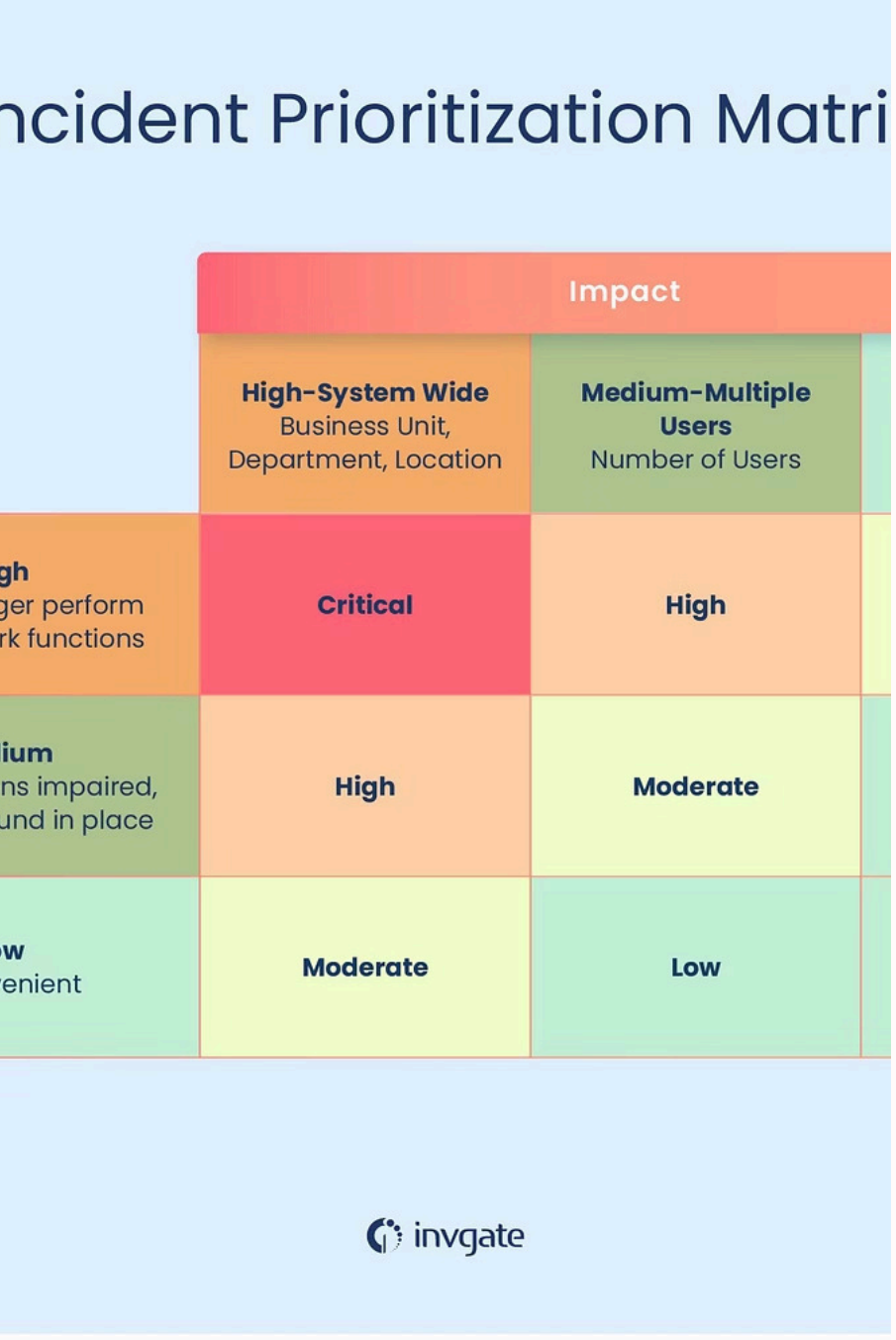
Assesses network activity, isolates affected segments, restores services

Security Analyst

Analyzes alerts, logs, and security tools to identify threats and patterns

Communications Lead

Handles internal and external communication, ensuring accurate and timely updates



Incident Classification Matrix

Prioritize incidents based on impact and urgency to allocate resources effectively and respond appropriately.

Low Priority

Minor disruptions, no significant impact

Examples: Phishing attempts without compromise, isolated policy violations

Medium Priority

Moderate disruptions affecting some services

Examples: Malware on non-critical systems, limited data exposure

High Priority

Major incidents with significant operational impact

Examples: Ransomware attacks, data breaches, critical system compromise

Communication Plan

Internal Communication

Notify relevant teams immediately upon incident confirmation:

- IT and security teams for technical response
- Management for strategic decisions
- HR if employee data is affected
- Legal for compliance requirements

Use secure channels and maintain clear documentation of all communications.

External Communication

Handle external stakeholders with transparency:

- Notify customers promptly if their data is affected
- Coordinate with legal and PR teams for regulatory reporting
- Prepare media responses if public disclosure is required
- Follow breach notification laws and timelines

Key Takeaways

Preparation is Critical

A well-prepared team with documented procedures responds faster and more effectively to security incidents.

Follow the Framework

The six-step process ensures systematic handling from detection through post-incident analysis.

Continuous Improvement

Every incident is a learning opportunity. Update your playbook regularly based on lessons learned.

Customize for Your Organization

This playbook is a starting point. Tailor it to your specific environment, risks, and business requirements.