🛟 Incident Response Plan

capybara Unlimited

INCIDENT RESPONSE PLAN

An **Incident Response Plan (IRP)** provides a structured approach for detecting, responding to, and recovering from cybersecurity incidents. Below is a detailed IRP tailored for a cybersecurity team associated with Capybara Unlimited, a medium-sized organization.

By integrating this detailed IRP, cybersecurity teams can ensure they are prepared to handle incidents efficiently and minimize their impact on the organization.

🏆 I. Objectives

I Objectives

I.1 Minimize Impact:

The Capybara Unlimited IRP is designed to provide an effective initial response to any unplanned business interruption. Its main goals are to protect critical data, reduce operational and financial losses, minimize system damage, improve recovery time, identify key stakeholders, and reduce negative publicity.

I.2 Restore Operations:

A successful recovery from a disaster requires total coordination of all incident management and recovery activities. The following steps outline the process:

1. **Isolation and Containment:** Immediately disconnect or isolate affected systems to prevent further spread of the threat.

2. **Damage Assessment:** Investigate the incident to determine its scope, identify what data or systems were compromised, and find the root cause of the attack.

3. **Identify and Secure Backups:** Verify the availability of clean, unaffected backups from before the incident occurred.

4. **Test Restoration:** Conduct a test restore in an isolated environment to ensure data integrity and confirm that no threats are reintroduced.

5. **Systematic Restoration:** Once the test is successful, restore full operations using the verified backups.

6. **Apply Patches and Updates:** During restoration, apply all necessary security patches, software updates, and adjust access controls to strengthen defenses.

7. **Monitoring and Validation:** Continuously monitor the restored systems for anomalies or signs of persistent threats.

8. **Post-Incident Review:** Analyze the incident's impact, evaluate the response effectiveness, and document lessons learned to improve future recovery procedures.

I.3 Enhance Security Posture:

Capybara Unlimited experienced several vulnerabilities, including untested backups, the absence of an incident response retainer, lack of a clear chain of command, failure to regularly review and test the IRP, and weaknesses in data protection and confidentiality.

To improve its defenses, the organization should invest in specialized cybersecurity expertise, ensure rapid response capabilities, maintain cost-efficient solutions, and implement continuous 24/7 monitoring.

A robust and effective incident response plan is essential for safeguarding digital assets and maintaining business continuity. The key to effective incident response is not only having a plan in place but also **proactively testing, evaluating, and refining it** to stay ahead of evolving cyber threats.

I.4 Meet Regulatory Requirements:

To maintain compliance, the cybersecurity team will review Capybara Unlimited's existing policies and align them with the **NIST Cybersecurity Framework (CSF)** standards. After an incident, all critical systems will be restored from **verified backups**, and business operations will resume only after confirming that the environment is **secure, stable, and fully compliant** with regulatory and organizational requirements.

🔭 II. Scope

II Scope

The Incident Response Plan (IRP) applies to all information systems, networks, applications, and data managed by Capybara Unlimited. It covers internal staff, third-party vendors, and cloud service providers who handle or have access to company data. The plan includes all departments and business units to ensure that cybersecurity incidents are detected, managed, and resolved consistently across the organization.

🕵️ III. Roles & Responsibilities

III Roles & Responsibilities

The Incident Response (IR) Team at **Capybara Unlimited** is composed of designated personnel with defined roles, responsibilities, and authority to ensure a coordinated, timely, and compliant response to cybersecurity incidents. Each team member is accountable for specific functions throughout the phases of incident detection, containment, eradication, recovery, and post-incident review.

III.1 Incident Command

The **Incident Commander** serves as the overall lead and primary decision-maker during an incident.
Responsibilities include:

- Directing and overseeing all incident response activities across teams.
- Ensuring that all response actions align with the organization's strategic objectives, security policies, and risk management framework.
- Prioritizing tasks and allocating resources to ensure efficient incident containment and recovery.
- Coordinating communication between internal teams, executive leadership, and external stakeholders.
- Approving official public statements and ensuring that legal, technical, and communication activities remain synchronized.
- Authorizing the closure of the incident once full recovery and validation have been achieved.

III.2 SOC Analysts

SOC Analysts are the first line of defense, responsible for continuous monitoring and detection of potential threats.

Responsibilities include:

- Monitoring network and endpoint activity through tools such as SIEM, EDR, IDS/IPS, and log management systems.
- Identifying anomalies, suspicious behaviors, or confirmed indicators of compromise (IOCs).
- Performing initial triage and categorization of alerts to determine severity and potential business impact.
- Escalating verified incidents to the Incident Commander and coordinating with forensic and IT teams for further analysis.
- Maintaining accurate, timestamped incident records and evidence logs for audit and compliance purposes.

III.3 Forensic Specialists

Forensic Specialists are responsible for the technical investigation and evidence handling of incidents.

Responsibilities include:

- Conducting detailed forensic examinations of affected systems, networks, and endpoints to determine the root cause and attack vector.
- Collecting, preserving, and securing digital evidence in accordance with chain-of-custody and legal admissibility standards.
- Supporting law enforcement or regulatory investigations when necessary.
- Providing technical reports and detailed findings to guide containment, eradication, and future mitigation strategies.
- Assisting in post-incident analysis to identify weaknesses and recommend improvements in security controls and procedures.

III.4 IT Administrators

IT Administrators play a critical role in executing containment, remediation, and recovery efforts.
Responsibilities include:

- Isolating compromised systems or network segments to prevent further propagation of the threat.
- Implementing eradication measures, including removal of malicious files, user accounts, or unauthorized access mechanisms.
- Restoring affected systems and services from verified clean backups while validating integrity and performance.
- Collaborating with SOC Analysts and Forensic Specialists to verify that no residual threats remain.
- Documenting all recovery steps taken to ensure repeatability and compliance with change management protocols.

III.5 Legal and Compliance Team

The **Legal and Compliance Team** provides oversight to ensure that all actions taken during incident response comply with applicable laws, regulations, and organizational policies.
Responsibilities include:

- Advising the Incident Commander on legal obligations related to data protection, privacy laws, and breach notification requirements.
- Determining when and how to report incidents to regulatory bodies, law enforcement, or affected customers.
- Reviewing communication materials to ensure no legal exposure or violation of confidentiality occurs.
- Maintaining detailed records of all legal correspondence and decisions for audit and compliance verification.
- Supporting the post-incident review by identifying compliance gaps and recommending corrective measures.

III.6 Sales and Marketing

The **Communications Officer** manages the internal and external flow of information during an incident to maintain transparency, trust, and brand integrity.
Responsibilities include:

- Developing and disseminating consistent, accurate, and approved messages to employees, customers, partners, and the media.
- Working closely with the Incident Commander and Legal Team to ensure that public communications comply with legal and regulatory requirements.
- Coordinating internal briefings to ensure staff are informed of relevant updates without disclosing sensitive or classified details.
- Managing inquiries from external entities, including journalists and stakeholders, in a controlled and professional manner.
- Assisting with post-incident reputation management and reinforcing public trust in the organization's cybersecurity resilience.

III.7 All Employees or General Workforce

All employees play a critical role in supporting Capybara Unlimited's cybersecurity posture. Their actions before, during, and after an incident directly impact how quickly and effectively the organization can respond and recover.

Responsibilities include:

- **Awareness and Prevention:**
  Employees must stay informed about cybersecurity best practices, such as identifying phishing emails, using strong passwords, and following company data-handling policies. They are required to complete periodic cybersecurity awareness training provided by the organization.

- **Incident Detection and Reporting:**
  Any employee who notices unusual system behavior, suspicious emails, or potential security incidents must immediately report it to the **IT or Security Operations Center (SOC)** using the company's established reporting channels (such as email, hotline, or ticket system). Quick reporting helps the IR team contain threats before they spread.

- **Cooperation During Investigation:**
  Employees must cooperate with the Incident Response Team by providing accurate information, logs, or details about their recent activities if requested. They should avoid deleting, modifying, or sharing any evidence related to the incident.

- **Post-Incident Participation:**
  Employees are encouraged to take part in post-incident reviews and follow-up awareness sessions to learn from the event and reinforce stronger security practices.

This shared responsibility builds a culture of transparency, accountability, and trust. When employees actively participate in incident reporting and response, Capybara Unlimited can reduce damage, restore operations faster, and strengthen its overall security posture.

🌱 IV. Incident Response Lifecycle

IV Incident Response Lifecycle

Follow the **NIST Cybersecurity Framework's Incident Response Process**:

IV.1 Preparation

IV.1.1 Develop policies

Define incident types, severity levels, and escalation paths.

IV.1.2 Train personnel

Regularly conduct training and tabletop exercises to ensure readiness.

IV.1.3 Implement tools

Ensure availability of SIEM, IDS/IPS, forensic tools, and reliable backup systems.

IV.1.4 Create playbooks

Tailor playbooks for specific incidents (*e.g.*, malware incidents, phishing, DoS attacks).

IV.2 Detection and Analysis

IV.2.1 Identify incidents

Monitor systems for suspicious activity using:

IV.2.1.a SIEM

SIEM dashboards for anomaly detection.

IV.2.1.b EDR

EDR alerts for malware or endpoint compromise.

IV.2.1.c Network logs

Review logs for unusual or unauthorized network traffic.

IV.2.2 Classify incidents

Classify incidents in terms of **severity** and **type**.

IV.2.2.a Severity levels

- Low
- Medium
- High
- Critical

IV.2.2.b Type

- Malware
- Phishing
- Insider threat
- DoS/DDoS
- Data Breach

IV.2.3 Collect evidence

IV.2.3.a Logs

Logs (system, application, network).

IV.2.3.b Malware

Malware samples for forensic analysis.

IV.2.3.c Email headers

Email headers for phishing attempts.

IV.2.4 Decision points

IV.2.4.a Escalate to leadership

Escalate high-severity incidents to leadership.

IV.2.4.b Scope-based containment

Determine containment steps based on the scope of the incident.

IV.3 Containment

IV.3.1 Immediate steps

IV.3.1.a Affected systems

Isolate affected systems from the network (do not keep them connected) to prevent lateral movement, but maintain power to preserve forensic evidence.

IV.3.1.b Affected accounts

Quarantine or disable compromised user accounts.

IV.3.1.c Firewall rules

Block malicious IPs, domains, or URLs at the firewall level.

IV.3.2 Short-term actions

IV.3.2.a Disable infected devices

Disable infected devices but preserve forensic evidence.

IV.3.2.b Redirect to alternative systems

Redirect legitimate traffic away from targeted systems.

IV.3.3 Long-term actions

IV.3.3.a Patch management

Patch vulnerabilities identified during investigation.

IV.3.3.b Network segmentation

Strengthen network segmentation to limit lateral movement.

IV.4 Eradication

IV.4.1 Remove malware

IV.4.1.a Remove infection (automated)

Reboot and update infected devices to remove malware infection.

IV.4.1.b Remove infection (manual)

Manually delete malicious files, processes, and registry entries if needed.

IV.4.2 Address root cause

IV.4.2.a Root cause analysis

Investigate how the threat bypassed defenses.

IV.4.1.b Remove persistence mechanisms

Remove persistence mechanisms, such as scheduled tasks or malicious user accounts.

IV.5 Recovery

IV.5.1 Restore operations

IV.5.1.a Restore from backup

Rebuild affected systems from known-good backups.

IV.5.1.b Validate backup integrity

Validate system integrity and ensure no residual threats exist.

IV.5.2 Monitor post-incident

IV.5.2.a Watch for re-infection

Closely watch affected systems for signs of re-infection.

IV.5.2.b Reduce visibility gaps

Use enhanced logging and detection rules for similar attack vectors.

IV.6 Post-Incident Analysis

IV.6.1 Conduct review

IV.6.1.a Create timeline

Create a detailed timeline of the incident.

IV.6.1.b Evaluate processes

Evaluate the effectiveness of detection, containment, eradication, and recovery efforts.

IV.6.2 Document findings

IV.6.2.a Incident report

Write a comprehensive incident report.

IV.6.2.b Lessons learned

Summarize lessons learned and proposed improvements.

IV.6.3 Implement changes

IV.6.3.a Update IR processes

Update the IRP and related playbooks.

IV.6.3.b Implement mitigations

Strengthen defenses based on vulnerabilities identified during the attack.

💬 V. Communication Plan

V Communication Plan

V.1 Internal Communication

V.1.a

Notify leadership and affected departments immediately upon incident confirmation.

V.1.b

Provide regular, structured updates throughout the incident response process to ensure situational awareness and coordinated action among teams.

V.2 External Communication

V.2.a

Inform customers, partners, or third parties **only if required** by contractual, legal, or regulatory obligations.

V.2.b

Evaluate the potential regulatory, legal, and financial impacts before disclosing incident details. If disclosure could result in significant penalties or reputational damage, carefully assess whether the incident meets the criteria for **mandatory reporting** under applicable regulations (such as GDPR, HIPAA, or state breach notification laws) and limit external communication accordingly.

V.2.c

In situations where public disclosure could negatively impact the company’s reputation or ongoing investigations, refrain from issuing public statements until authorized by executive leadership and the Legal or Communications teams.

🎯 VI Key Performance Indicators (KPIs)

VI Key Performance Indicators (KPIs)

VI.1 Time to Detect (TTD)

The following KPIs are used to measure the **effectiveness and efficiency** of Capybara Unlimited's Incident Response process. These metrics provide clear, quantifiable insights for both technical teams and executive stakeholders.

VI.2 Time to Contain (TTC)

Measures how quickly the Incident Response Team isolates or neutralizes affected systems after detection. A low TTC reflects efficient containment procedures and rapid decision-making to prevent further impact.

VI.3 Time to Recover Baseline Security Posture (TTRBSP)

Measures the time required to fully restore systems, applications, and controls to their pre-incident baseline security state.
This metric demonstrates how efficiently the organization can recover normal operations while maintaining security integrity.

VI.4 Incident Closure Rate

Represents the percentage of reported incidents that are fully resolved within the organization's defined response timeframes.
A higher closure rate indicates effective coordination, proper resource allocation, and adherence to established IR processes.

VI.5 Post-Incident Improvement Rate

Measures the percentage of documented lessons learned that lead to implemented security enhancements, updated policies, or improved response procedures.
This KPI reflects the organization’s commitment to continuous improvement and proactive risk reduction.

🧨 VII. Common Mistakes & Mitigations

VII Common Mistakes & Mitigations

VII.1 Overlooking early indicators

VII.1.a Mistake

Dismissing minor anomalies or alerts as false positives.

VII.1.b Mitigation

Implement automated alert prioritization and correlation within SIEM systems to ensure early indicators are analyzed and escalated appropriately. it directly addresses the mistake by improving detection accuracy and response awareness.

VII.2 Inadequate documentation

VII.2.a Mistake

Failing to record actions, timestamps, and decisions taken during the incident response process.

VII.2.b Mitigation

Assign a dedicated incident scribe or recorder to document all activities, communications, and decisions in real time. Assigning a scribe ensures proper accountability and supports post-incident analysis.

VII.3 Premature recovery

VII.3.a Mistake

Reconnecting or restoring systems before confirming complete eradication of the threat.

VII.3.b Mitigation

Conduct comprehensive validation and system integrity checks before resuming normal operations or reconnecting affected systems to the network. Validation before recovery is standard NIST practice.

VII.4 Neglecting post-incident reviews

VII.3.a Mistake

Skipping post-incident or “lessons learned” reviews due to time constraints or resource limitations.

VII.3.b Mitigation

Make post-incident reviews mandatory for incident closure and incorporate findings into updated procedures and training programs. Mandatory reviews ensure continuous improvement and organizational learning.

🛠️ VIII. Tools & Techniques

VIII Tools & Techniques

VIII.1 Detection

SIEM (Splunk, QRadar), IDS/IPS (Snort, Suricata), EDR (CrowdStrike, SentinelOne).

VIII.2 Containment

NAC (Cisco ISE), firewalls (Palo Alto, Fortinet).

VIII.3 Eradication

Antivirus/Antimalware (Sophos, Malwarebytes, Windows Defender).

VIII.4 Recovery

Backup solutions (Veeam, Acronis).

VIII.5 Analysis

Forensic tools (FTK, EnCase, Wireshark).

🧰 IX. Review & Maintenance

IX Review and Maintenance

IX.1 Annual updates

Review and revise the IRP proactive **annual or event-driven review** for compliance or regulatory purposes.

IX.2 Ongoing Training

Conduct **quarterly training sessions and simulations** to ensure that all team members remain familiar with response procedures, communication protocols, and new tools.
Training should include both technical staff and executive stakeholders to promote coordinated and efficient responses.

IX.3 First-Party Audits

Perform **internal audits** of the Incident Response Program to verify the effectiveness of detection, containment, and recovery processes.
Engage **internal security and compliance experts** to minimize the risk of exposing sensitive IR strategies, while ensuring objectivity and adherence to audit standards.

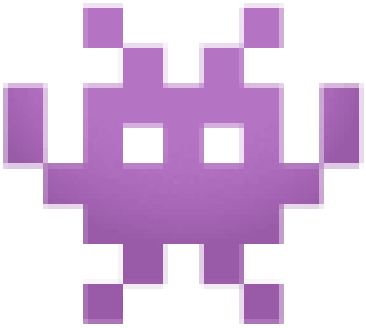
Appendix

APPENDIX

Playbooks

IR PLAYBOOKS

Malware Infection



Malware Infection Playbook

1. Identify and contain the malware

Quickly detect, isolate, and limit the spread of malware to minimize damage while performing a **thorough but cautious analysis** in a controlled environment..

1.1 Identify and observe infected systems

Infected systems should not remain online on the production network. Instead, isolate them immediately to prevent lateral movement or additional compromise, while keeping them powered on (if needed) to preserve volatile evidence.

1.2 Conduct preliminary analysis

Gather initial indicators of compromise (IOCs) such as suspicious files, processes, registry changes, or outbound connections to inform containment and eradication strategies.

2. Perform static analysis of the malware sample

Analyze the malware file without executing it to understand its characteristics.

2.1 Inspect file structure and metadata

Examine the malware file's properties, including size, hash values, and embedded metadata.

2.2 Extract embedded strings and suspicious code

Use tools like Strings, VirusTotal, or PEStudio to identify readable text, URLs, or code fragments that provide insight into the malware's intent and behavior.

3. Perform dynamic analysis in a controlled environment

Never run malware on a production system — it must be executed in a sandbox or isolated virtual lab.

This is critical to prevent unintentional spread or damage

3.1 Execute malware on a clean system

Run the malware in a controlled virtual lab or sandbox, not in production, to safely observe its behavior and capture forensic data.

3.2 Record system modifications and activities

Document all system changes, including registry edits, file creation/deletion, process launches, and network connections made during execution.

4. Conduct network traffic analysis

Analyze communication attempts made by the malware to uncover external connections.

4.1 Capture network traffic

Use packet-capturing tools to monitor network activity generated by the malware.

4.2 Identify external entities

Look for connections to command-and-control (C2) servers or data exfiltration endpoints.

5. Investigate behavioral patterns and persistence mechanisms

Determine how the malware survives and operates over time.

5.1 Identify persistence techniques

Investigate changes such as registry modifications, scheduled tasks, or startup files.

5.2 Examine behavioral indicators

Look for recurring patterns, such as periodic network requests or file executions.

6. Eradicate the malware and recover systems

Remove the malware and restore affected systems to their original state.

6.1 Deploy cleanup tools

Use antivirus or specialized malware removal tools to eradicate infections.

6.2 Restore from clean backups

Reinstall or rebuild affected systems and data using backups confirmed to be malware-free.

6.3 Apply mitigations to prevent reinfection

Address any vulnerabilities that permitted the original infection to occur by applying the appropriate mitigation.

7. Post-incident reporting and prevention

Document lessons learned and strengthen defenses against future incidents.

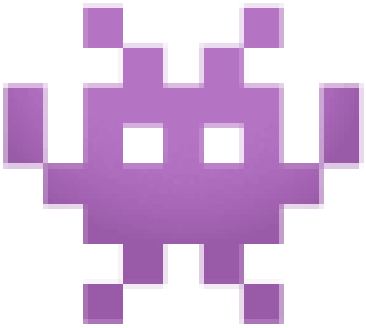
7.1 Generate incident report

Detailed findings, response steps, and impact assessment in a comprehensive report.

7.2 Implement prevention measures

Update security policies, patch vulnerabilities, and educate staff to avoid recurrence.

🪝 Phishing



Phishing Playbook

1. Identify and verify the phishing email

Confirm that the suspicious email is a phishing attempt, not a legitimate message.

1.1 Analyze email headers and content

Inspect email headers for inconsistencies like mismatched sender domains or unusual reply-to addresses. Review the content for generic greetings, poor grammar, or urgent requests for sensitive information.

1.2 Compare against known phishing indicators

Cross-check email elements against known phishing indicators, such as fake links (hover over to inspect URLs), suspicious attachments, or spoofed branding.

2. Contain the threat

Prevent further exposure or escalation.

2.1 Isolate the email

Instruct recipients not to click links, open attachments, or reply. Move the email to a quarantined folder or report it using the “Report Phish” feature if available.
(If multiple users received the same campaign, security should purge the message organization-wide and block the sender/domain.)

2.2 Notify IT/security team

Report the phishing email to the organization's security team immediately, following internal reporting procedures.

3. Investigate the impact

Determine the extent of the threat and affected users.

3.1 Verify user interaction

Do not assume no one interacted with the email. Proactively check mail logs, proxy logs, and EDR telemetry to confirm whether users opened the message, clicked links, or downloaded attachments. Communicate directly with recipients to verify potential interaction.

3.2 Check affected systems

Use Endpoint Detection and Response (EDR) tools to monitor devices for suspicious activity or malware from phishing payloads. Review identity logs (e.g., sign-in anomalies, mailbox rule changes) for potential account compromise.

4. Eradicate the threat

Remove malicious elements and secure compromised accounts or systems.

4.1 Preserve phishing emails

Do not leave phishing emails in user inboxes. The security team should preserve samples safely in a secured evidence repository for analysis, then remove or quarantine all copies from user mailboxes.

4.2 Secure compromised accounts

If credentials were entered, reset passwords immediately, revoke active sessions, check for malicious inbox rules or forwarding, and enable or enforce multi-factor authentication (MFA). Continue monitoring account activity for unauthorized access.

5. Educate and prevent future incidents

Strengthen user awareness and defenses.

5.1 Notify all employees

Notify employees with clear, factual information about the phishing campaign (e.g., subject line, sender name, and how to report similar messages). Avoid disclosing unnecessary technical details that may cause confusion or panic.

5.2 Provide training

Conduct phishing awareness sessions and simulated phishing exercises to reinforce detection skills.

6. Monitor and report

Ensure no residual threats remain and document the incident.

6.1 Monitor for reoccurrence

Continue monitoring mail gateways, user accounts, and endpoints for signs of repeated phishing attempts or related campaigns. Update blocklists and detection rules as needed.

6.2 Document the incident

Log all details about the phishing attack, including timeline, impact, user responses, and actions taken. Summarize lessons learned to enhance training and refine future response efforts.

Denial-of-Service

Denial-of-Service Playbook

1. Identify and characterize the attack traffic

Confirm the nature of the traffic to ensure it's consistent with a DoS attack rather than a legitimate traffic spike.

1.1 Automate detection of unusual number of packets

Use network monitoring and intrusion detection tools (e.g., NetFlow, Zeek, IDS/IPS, or SIEM) to identify abnormal traffic patterns such as excessive requests from specific IPs, unusually large packets, or repeated connections targeting the same service or port.

1.2 Classify the type of DoS

Characterize the traffic to determine if it aligns with known DoS attack patterns (*e.g.,* SYN flood, ICMP flood, Application Layer Attacks).

2. Measure traffic volume and bandwidth consumption

Accurately assess traffic volume to prioritize resources and decide on appropriate mitigation strategies.

2.1 Assess scope of DoS

Monitor network metrics to assess the scope, including packet size, rate of incoming requests, and bandwidth impact.

2.2 Evaluate impact of DoS

Use these metrics to understand the impact on network resources and how severely the attack affects performance.

3. Locate the source of attack traffic

Identify malicious origins to inform defensive filtering or external coordination with ISPs.

3.1 Identify patterns in DoS traffic source

Use IP flow data and threat intelligence tools to detect patterns such as repetitive IP addresses, specific geolocations, or Autonomous System Numbers (ASNs).

3.2 Analyze identified patterns

Document consistent IP ranges or behavioral indicators that may suggest botnet activity or amplification attacks (e.g., via DNS or NTP).

4. Identify affected services and network components

Pinpoint affected systems to prioritize protective measures and service continuity efforts.

4.1 Identify affected internal systems

Use logs and network monitoring to determine which servers, services, or endpoints are being targeted by the attack (*e.g.,* web servers, DNS).

5. Implement and monitor mitigation measures

Ensure mitigation is effectively reducing malicious traffic while maintaining service availability for legitimate users.

5.1 Implement firewall rules

Apply adaptive network defenses such as:

- Blocking malicious IPs, ports, or protocols at firewalls or routers.
- Enabling **rate-limiting, geo-blocking, or connection throttling**.

- Engaging upstream mitigation (e.g., ISP scrubbing centers, cloud-based DDoS protection like Cloudflare or AWS Shield).

.

5.2 Monitor effectiveness of firewall mitigations

Continuously monitor firewall, IDS, and network logs to verify that mitigation measures are reducing malicious traffic without hindering legitimate operations. Adjust rules as needed to optimize performance.