Cybersecurity Incident Response Cheat Sheet

A comprehensive cheat sheet covering the key stages, processes, and best practices for effective cybersecurity incident response. Aimed at security professionals and IT teams.

Incident Response Lifecycle

Preparation

Description: Establishing policies, procedures, and resources to effectively manage incidents.

Key Activities:

- Develop and maintain an incident response plan (IRP).
- Define roles and responsibilities for the incident response team (IRT).
- Identify critical assets and data.
- Implement security awareness training for employees.
- Establish communication channels.

Tools & Technologies:

- Security Information and Event Management (SIEM) systems.
- Threat intelligence platforms.
- Vulnerability scanners.

Identification

Description: Detecting and confirming potential security incidents.

Key Activities:

- Monitor security alerts and logs.
- Analyze network traffic for suspicious activity.
- Investigate user reports of potential incidents.
- Utilize threat intelligence to identify potential threats.

Tools & Technologies:

- Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS).
- Endpoint Detection and Response (EDR) solutions.
- Log management tools.

Containment

Description: Limiting the scope and impact of an incident.

Key Activities:

- Isolate affected systems and network segments.
- Disable compromised accounts.
- Block malicious traffic.
- Implement temporary security controls.

Tools & Technologies:

- Network segmentation tools.
- Firewall rules.
- Endpoint isolation capabilities.

Eradication & Recovery

Eradication

Description: Removing the root cause of the incident to prevent recurrence.

Key Activities:

- Identify and patch vulnerabilities.
- Remove malware and malicious code.
- Rebuild compromised systems.
- Update security configurations.

Tools & Technologies:

- Patch management systems.
- Anti-malware software.
- System imaging and deployment tools.

Recovery

Description: Restoring affected systems and data to normal operations.

Key Activities:

- Restore data from backups.
- Re-enable systems and services.
- Monitor systems for anomalies.
- Verify system integrity.

Tools & Technologies:

- Backup and recovery solutions.
- System monitoring tools.
- Data integrity verification tools.

Lessons Learned

Description: Documenting the incident and identifying areas for improvement.

Key Activities:

- Conduct a post-incident review.
- Identify weaknesses in security controls.
- Update incident response plan.
- Implement corrective actions.

Tools & Technologies:

- Documentation and knowledge management systems.
- Project management tools.
- Risk assessment tools.

Incident Response Team (IRT)

IRT Roles & Responsibilities

Team Lead	Overall coordination, communication, and decision-making.
Security Analyst	Incident detection, analysis, and containment.
Forensic Investigator	Data collection, analysis, and evidence preservation.
Communications Lead	Internal and external communications.
Legal Counsel	Legal guidance and compliance.
IT Support	System restoration and technical assistance.

Communication Plan

Internal Communication:

- Establish clear channels for reporting incidents.
- Regularly update stakeholders on incident status.
- Use secure communication methods.

External Communication:

- Coordinate with law enforcement and regulatory agencies.
- Manage media inquiries.
- Communicate with customers and partners.

Tools and Technologies

Essential Tools

SIEM (Security Information and Event Management): Centralized log collection and analysis for threat detection.
EDR (Endpoint Detection and Response): Real-time monitoring and response capabilities on endpoints.
IDS/IPS (Intrusion Detection/Prevention Systems): Network-based threat detection and prevention.
Firewalls: Network security devices that control traffic based on defined rules.
Vulnerability Scanners: Identify security weaknesses in systems and applications.
Packet Analyzers: Capture and analyze network traffic for forensic investigation.

Advanced Technologies

Threat Intelligence Platforms (TIP): Aggregate and analyze threat data from various sources.
SOAR (Security Orchestration, Automation, and Response): Automate incident response workflows.
UEBA (User and Entity Behavior Analytics): Detect anomalous user and system behavior.
Deception Technology: Use decoys and traps to detect and deceive attackers.