Cheat Sheet for comprehensive CompTIA CySA+

Incident Response Process

1. Preparation

- **Tools & Resources**:

- SIEM (Security Information and Event Management)
- IDS/IPS (Intrusion Detection/Prevention Systems)
- Forensic Tools (e.g., EnCase, FTK)
- Incident Response Plan

- **Training**:

- Regular drills and simulations
- Certifications (e.g., CISSP, GCFA)

2. Identification

- **Indicators of Compromise (IOCs)**:

- Malware signatures
- Unusual network traffic
- Unauthorized access attempts

- **Detection Tools**:

- Endpoint Detection and Response (EDR)
- Log analysis tools
- Threat intelligence platforms

3. Containment

- **Short-term Containment**:

- Isolate affected systems
- Block malicious IPs/domains

- **Long-term Containment**:

- Implement stricter access controls
- Patch vulnerabilities

4. Eradication

- **Remove Malicious Code**:

- Use antivirus/antimalware tools

- Manual removal if necessary

- **Clean Affected Systems**:

- Rebuild from known-good backups
- Wipe and reinstall if no backup available

5. Recovery

- **Restore Systems**:

- From verified backups
- Ensure all patches and updates are applied

- **Test Systems**:

- Run integrity checks
- Perform vulnerability scans

6. Lessons Learned

- **Document Findings**:

- Incident timeline
- Root cause analysis

- **Update Policies**:

- Incident response plan
- Security policies and procedures

Threat Management

Threat Intelligence

- **Types**:
  - **Strategic**: High-level, long-term trends
  - **Tactical**: Specific attack methods and tools
  - **Operational**: Immediate threats and IOCs
  - **Technical**: Detailed technical data (e.g., malware signatures)

- **Sources**:

- Open-source intelligence (OSINT)
- Commercial threat intelligence feeds
- Government and industry reports

Threat Hunting

- **Process**:

- Define objectives
- Collect data
- Analyze data
- Act on findings

- **Tools**:

- SIEM
- EDR
- Network traffic analysis tools

Vulnerability Management

Vulnerability Assessment

- **Tools**:

- Nessus
- OpenVAS
- Qualys

- **Process**:

- Scan for vulnerabilities
- Prioritize findings
- Remediate high-priority issues

Patch Management

- **Automated Tools**:

- WSUS (Windows Server Update Services)
- SCCM (System Center Configuration Manager)

- **Best Practices**:

- Regularly update systems
- Test patches in a lab environment before deployment

Security Architecture and Tool Sets

SIEM

- **Functions**:

- Log aggregation
- Correlation of events

- Real-time alerting

- **Popular Tools**:

- Splunk
- IBM QRadar
- ArcSight

IDS/IPS

- **Types**:

  - **Network-based**: Monitors network traffic

  - **Host-based**: Monitors individual systems

- **Popular Tools**:

- Snort
- Suricata
- Cisco Firepower

Endpoint Detection and Response (EDR)

- **Functions**:

- Continuous monitoring
- Automated response
- Forensic analysis

- **Popular Tools**:

- CrowdStrike Falcon
- Carbon Black
- Microsoft Defender for Endpoint

Security Policies and Procedures

Security Policies

- **Types**:

- Acceptable Use Policy (AUP)
- Password Policy
- Incident Response Policy

- **Best Practices**:

- Regularly review and update
- Ensure compliance with regulations

Security Awareness Training

- **Content**:

- Phishing awareness
- Social engineering prevention
- Proper use of security tools

- **Frequency**:

- Annual training
- Periodic refreshers

Data Privacy and Protection

Data Classification

- **Levels**:

- Public
- Internal
- Confidential
- Restricted

- **Labels**:

- Color-coded labels
- Digital watermarks

Data Encryption

- **Types**:

- Symmetric encryption (e.g., AES)
- Asymmetric encryption (e.g., RSA)

- **Best Practices**:

- Encrypt sensitive data at rest and in transit
- Use strong encryption algorithms

Compliance and Regulations

Common Regulations

- **GDPR**: General Data Protection Regulation

- **HIPAA**: Health Insurance Portability and Accountability Act

- **PCI DSS**: Payment Card Industry Data Security Standard

Compliance Audits

- **Process**:

- Prepare documentation
- Conduct internal audits
- Address findings

- **Tools**:

- Compliance management software
- Automated audit tools

Security Operations Center (SOC)

Functions

- **Monitoring**:

- 24/7 surveillance of security events
- Real-time alerting

- **Incident Response**:

- Rapid identification and containment
- Coordination with other teams

- **Reporting**:

- Daily, weekly, and monthly reports
- Trend analysis and forecasting

Tools and Technologies

- **SIEM**: Centralized log management

- **SOAR**: Security Orchestration, Automation, and Response

- **Ticketing Systems**: Jira, ServiceNow

Threat Modeling

Process

- **Identify Assets**:

- Critical systems and data
- Business processes

- **Identify Threats**:

- Potential attack vectors
- Threat actors

- **Assess Vulnerabilities**:

- Weaknesses in systems and processes
- Likelihood and impact

- **Mitigation Strategies**:

- Implement controls
- Prioritize remediation

Network Security

Firewalls

- **Types**:

- Packet-filtering
- Stateful inspection
- Next-generation firewalls (NGFW)

- **Best Practices**:

- Regularly update rules
- Monitor logs for suspicious activity

VPNs

- **Types**:

- Remote Access VPN
- Site-to-Site VPN

- **Best Practices**:

- Use strong encryption
- Regularly update VPN software

Network Segmentation

- **Benefits**:

- Limits lateral movement
- Enhances security monitoring

- **Implementation**:

- Use VLANs

- Implement firewalls between segments

Cloud Security

Cloud Service Models

- **IaaS**: Infrastructure as a Service

- **PaaS**: Platform as a Service

- **SaaS**: Software as a Service

Security Best Practices

- **Data Encryption**:

- At rest and in transit
- Use strong encryption algorithms

- **Access Controls**:

- Implement IAM (Identity and Access Management)
- Use multi-factor authentication (MFA)

- **Compliance**:

- Ensure cloud provider meets regulatory requirements
- Regularly audit cloud environments

Mobile Device Security

Security Controls

- **Encryption**:

- Encrypt data on devices
- Use strong encryption algorithms

- **MDM (Mobile Device Management)**:

- Remote wipe capabilities
- Application management

- **Authentication**:

- Use strong passwords
- Implement MFA

Physical Security

Controls

- **Access Controls**:

- Badge access systems
- Biometric authentication

- **Surveillance**:

- CCTV cameras
- Motion detectors

- **Environmental Controls**:

- Fire suppression systems
- Uninterruptible power supplies (UPS)

Security Automation

Benefits

- **Efficiency**:

- Automates repetitive tasks
- Reduces human error

- **Scalability**:

- Handles large volumes of data
- Adapts to growing environments

Tools

- **SOAR (Security Orchestration, Automation, and Response)**:

- Automates incident response
- Integrates with other security tools

- **RPA (Robotic Process Automation)**:

- Automates routine administrative tasks
- Enhances operational efficiency

Forensics and Investigations

Digital Forensics

- **Process**:

- Collection

- Preservation
- Analysis
- Reporting

- **Tools**:

- EnCase
- FTK (Forensic Toolkit)
- Autopsy

Incident Investigation

- **Steps**:

- Identify the incident
- Gather evidence
- Analyze data
- Report findings

- **Best Practices**:

- Follow legal and ethical guidelines
- Document all actions and findings

Threat Actors and Motives

Types of Threat Actors

- **Script Kiddies**: Unskilled attackers using existing tools

- **Hacktivists**: Motivated by political or social causes

- **Cybercriminals**: Motivated by financial gain

- **Insiders**: Employees or contractors with access to systems

- **Nation-States**: State-sponsored attackers

Motives

- **Financial Gain**: Theft, ransom, fraud

- **Espionage**: Stealing sensitive information

- **Disruption**: Denial of service, sabotage

- **Hacktivism**: Promoting a cause or ideology

Security Metrics and Reporting

Key Metrics

- **MTTD (Mean Time to Detect)**: Average time to detect an incident
- **MTTR (Mean Time to Respond)**: Average time to respond to an incident
- **MTTF (Mean Time to Failure)**: Average time a system operates before failure

Reporting

- **Types**:

- Incident reports
- Compliance reports
- Security posture reports

- **Best Practices**:

- Regularly update reports
- Use visual aids (graphs, charts)

Continuous Monitoring and Improvement

Continuous Monitoring

- **Tools**:

- SIEM
- EDR
- Network monitoring tools

- **Best Practices**:

- 24/7 monitoring
- Regularly review and update monitoring policies

Continuous Improvement

- **Process**:

- Regularly review security posture
- Implement lessons learned from incidents
- Update policies and procedures

- **Best Practices**:

- Conduct regular security assessments
- Engage in continuous training and education

Conclusion

- **Summary**:

- Comprehensive understanding of incident response, threat management, and security tools
- Continuous monitoring and improvement are key to maintaining a robust security posture

- **Final Tips**:

- Stay updated with the latest security trends and technologies
- Regularly review and update security policies and procedures
- Engage in continuous learning and professional development

By Ahmed Baheeg Khorshid

ver 1.0