

Domain 4. Incident Response

Incident Response Phases

- Preparation
- Detection & Analysis
- Containment
- Eradication & Recovery
- Post Incident Activity

Communication plan

- Limiting communication to trusted parties
- Disclosing based on regulatory/legislative requirements
- Preventing inadvertent release of information
- Using a secure method of communication
- Reporting requirements

Reporting Requirements - Type of Breach

- Data exfiltration
- Insider data exfiltration
- Device theft/loss
- Accidental data breach
- Integrity/availability

Response coordination

- Legal
- Human resources
- Public relations
- Internal and external
- Law enforcement
- Senior leadership
- Regulatory bodies

Data Criticality and Prioritization

- Personally Identifiable Information (PII)
- Sensitive Personal Information (SPI)
- Personal Health Information (PHI)
- Financial Information
- Intellectual property (IP)
- Corporate Information
- high value asset (HVA)

Preparation Phase

- Training
- Testing
- Documentation of procedures

Documentation of Procedures

- Incident Response Plan
- Call List/Escalation List
- Incident Form

OODA loop

- Observe
- Orient
- Decide
- Act



Domain 4. Incident Response (cont)

Defensive Capabilities	<ul style="list-style-type: none"> - Detect - Destroy - Degrade - Disrupt - Deny - Deceive
Immediate impact	direct costs incurred because of an incident
Total impact	costs that arise following the incident, including damage to the company's reputation
Incident Security Level Classification characteristics (Detection & Analytics)	<ul style="list-style-type: none"> - Data integrity - System process criticality - Downtime - Economic - Data correlation - Reverse engineering - Recovery time - Detection time
Containment	<ul style="list-style-type: none"> - Isolation-Based Containment - Segmentation-based Containment
Containment principals	<ul style="list-style-type: none"> - Ensure the safety and security of all personnel. - Prevent ongoing intrusion or data breach. - Identify whether the intrusion is the primary attack or a secondary one (part of a more complex campaign). - Avoid alerting the attacker to the fact that the intrusion has been discovered. - Preserve forensic evidence of the intrusion.
Eradication	<ul style="list-style-type: none"> - Sanitization and Secure Disposal (cryptographic erase, zero-fill) - Reconstruction/Reimaging - Reconstitution of Resources
cryptographic erase	A method of sanitizing a self-encrypting drive by erasing the media encryption key
zero-fill	A method of sanitizing a drive by setting all bits to zero.
Secure disposal	physical destruction by mechanical shredding or incineration
Reimage	A method of restoring a system that has been sanitized using an image-based backup.
Reconstruction	A method of restoring a system that has been sanitized using scripted installation routines and templates.



Domain 4. Incident Response (cont)

Reconstitution	A method of restoring a system that cannot be sanitized using manual removal, reinstallation, and monitoring processes.
Recovery	<ul style="list-style-type: none"> - Patching - Restoration of Permissions - Verification of Logging/Communication to Security Monitoring - Vulnerability Mitigation and System Hardening
Post-Incident Activities	<ul style="list-style-type: none"> - Report Writing - Incident Summary Report - Evidence Retention

Domain 3. Security Operations and Monitoring

heuristic analysis	A method that uses feature comparisons and likenesses rather than specific signature matching to identify whether the target of observation is malicious.
Endpoint Data Collection and Analytics Tools	<ul style="list-style-type: none"> - Anti-virus (A-V) - Host-Based Intrusion Detection/Prevention (HIDS/HIPS) - Endpoint Protection Platform (EPP) - Endpoint Detection and Response (EDR) - User and Entity Behavior Analytics (UEBA)
Endpoint Protection Platform (EPP)	<ul style="list-style-type: none"> - a single agent performing multiple security tasks and features. - (malware/IDP), host firewall, web content filtering, (DLP) enforcement, and file/message encryption. - In an enterprise solution, there will also be a single management dashboard for configuring and monitoring hosts. - mostly signature-based detection and prevention
Endpoint Detection and Response (EDR)	<ul style="list-style-type: none"> - focused on logging of endpoint observables and indicators combined with behavioral- and anomaly-based analysis. - to provide real-time and historical visibility, containment, and facilitate remediation of the host to its original state.

Domain 3. Security Operations and Monitoring (cont)

User and Entity Behavior Analytics (UEBA)	<ul style="list-style-type: none"> - analysis process supporting identification of malicious behaviors from comparison to a baseline - tracks user account behavior across different devices and cloud services
Sandboxing	technique that isolates untrusted data in a closed virtual environment to conduct tests and analyze the data for threats and vulnerabilities.
Disassemblers and Decompilers	software that translate low-level machine language code into higher level code
Malware Exploit Techniques	<ul style="list-style-type: none"> - Malware Exploit Techniques - Maintain access - Strengthen access - Actions on objectives - Concealment
Living off the land	subvert existing architecture, such as Windows PowerShell, to perform the malicious activity.



