Task 14: Cybersecurity Processes

1. Monitoring and Detection

Purpose

Monitoring and detection represent the foundation of a proactive security strategy. These functions are designed to ensure continuous oversight of network, host, and application activity to detect unauthorized behavior, potential compromises, and deviations from defined baselines. Effective monitoring enables organizations to transition from reactive to proactive security operations.

Key Components

- **SIEM (Security Information and Event Management)**: Aggregates logs and events from across the infrastructure, applies normalization and correlation rules, and generates alerts. It centralizes visibility and often integrates with detection logic.

- **IDS/IPS (Intrusion Detection/Prevention Systems)**: Detects and potentially blocks malicious traffic. Signature-based IDS rely on known patterns, whereas anomaly-based IDS model expected behavior and alert on deviations.

- **Endpoint Detection and Response (EDR)**: Focuses on visibility at the endpoint level. EDR agents monitor for suspicious process behavior, unauthorized memory access, or abnormal API usage, and allow retrospective investigation.

- **Security Orchestration, Automation, and Response (SOAR)**: Enhances detection by automating enrichment, correlation, and response actions to reduce analyst workload and improve MTTD/MTTR.

Task 14: Cybersecurity Processes

Detection Approaches

- **Signature-based detection**: Relies on known patterns, such as byte sequences in malware files or suspicious domain names. Very accurate but easily evaded by novel or obfuscated threats.

- **Anomaly-based detection**: Uses statistical or machine learning models to define a baseline of "normal" activity and flags deviations. Useful for detecting zero-days or insider threats.

- **Heuristic and behavioral detection**: Applies logic rules to identify potentially malicious activity based on behavior, not specific signatures. Examples include detecting privilege escalation or lateral movement patterns.

Metrics

- **Detection latency**: Time taken from occurrence to alert generation.

- **False positive/negative rate**: Reflects the quality and tuning of detection rules.

- **Mean time to detect (MTTD)**: Average duration between incident onset and detection.

Challenges

- High alert volume leading to analyst fatigue.

- Incomplete telemetry due to poor log coverage or dropped packets.

- Difficulty distinguishing between benign anomalies and real threat

---

Task 14: Cybersecurity Processes

2. Threat Intelligence

Purpose

Threat intelligence provides context around adversaries, their methods, and the evolving threat landscape. It enhances the capability of detection systems by supplying information on emerging tools, vulnerabilities, and infrastructure used in attacks.

Sources of Intelligence

- **OSINT (Open Source Intelligence)**: Freely available data including malware repositories, security blogs, public threat feeds, and community reports.

- **Commercial Intelligence Platforms**: Offer curated, validated, and often automated feeds of indicators, TTPs, and adversary profiling.

- **Information Sharing Groups (e.g., ISACs, CERTs)**: Collaborative entities that allow organizations in similar sectors to share threat data.

Types of Threat Intelligence

- **Strategic Intelligence**: Non-technical, high-level insights intended for executive decision-makers. Includes trends, risks, and geopolitical threats.

- **Tactical Intelligence**: Describes the tools, techniques, and procedures (TTPs) used by adversaries. Often mapped to MITRE ATT&CK.

- **Operational Intelligence**: Real-time or near-real-time data about specific threats targeting the organization.

Task 14: Cybersecurity Processes

- **Technical Intelligence**: Includes raw indicators such as IP addresses, hashes, URLs, domain names, and malware signatures.

Integration into Operations

- Enrich SIEM and EDR alerts with contextual threat data.
- Apply threat intelligence to block known malicious IPs or domains at the firewall or proxy.
- Launch targeted threat hunts based on TTP profiles or campaign indicators.
- Update detection logic based on observed actor behavior.

Limitations

- Overreliance on IOC-based detection can lead to false positives.
- Difficulty in assessing credibility and timeliness of threat feeds.
- Integration complexity and redundancy across multiple sources.

---

3. Log Analysis

Purpose

Log analysis is critical for understanding system behavior, verifying compliance, detecting anomalies, and reconstructing security incidents. Comprehensive and contextual log analysis enables forensic investigation, proactive hunting, and incident triage.

Task 14: Cybersecurity Processes

Logging Pipeline

1. **Ingestion**: Centralize logs from diverse sources including servers, firewalls, cloud providers, and user applications. Tools like Fluentd, Logstash, or native collectors are used.

2. **Parsing and Normalization**: Convert logs into structured formats to allow for field-based searches and correlation.

3. **Storage and Retention**: Store logs in systems like Elasticsearch, Hadoop, or Splunk indexers. Retention policies depend on regulatory requirements.

4. **Query and Correlation**: Use tools to perform rule-based correlation (e.g., brute force followed by login success) or temporal correlation.

5. **Alerting and Visualization**: Build dashboards to visualize trends (e.g., failed login attempts, process starts), and trigger alerts based on thresholds or pattern matches.

Key Log Types

- **Authentication logs**: Login attempts, credential use, MFA status.

- **Process execution logs**: Which binaries were executed, by whom, and how.

- **Network logs**: Connections initiated, DNS queries, proxy logs.

- **Cloud audit logs**: API activity, IAM changes, key rotations.

Task 14: Cybersecurity Processes

Challenges

- High volume: Modern environments produce terabytes of log data daily.
- Log quality: Inconsistent or missing fields, poor timestamping.
- Alert fatigue: Difficulty in defining precise thresholds for detection.

---

4. Network Traffic Analysis

Purpose

Network traffic analysis (NTA) provides deep visibility into communication patterns, allowing defenders to detect malicious behavior such as lateral movement, exfiltration, or command-and-control (C2) activity. Unlike endpoint tools, NTA operates on passive observation.

Data Sources

- **Flow Records (e.g., NetFlow, IPFIX)**: Provide metadata about connections such as IP pairs, ports, byte counts, and timing.
- **Full Packet Capture (PCAP)**: Raw packet-level data enabling payload inspection and protocol analysis.
- **DNS and HTTP Logs**: Reveal application-layer behavior and indicators.

Task 14: Cybersecurity Processes

Key Techniques

- **Protocol Dissection**: Analyze DNS, HTTP, SSL, SMB, and other protocols to detect misuse.
- **Traffic Pattern Analysis**: Identify beaconing, periodicity, or high-volume exfiltration.
- **Encrypted Traffic Analysis**: Analyze SSL/TLS metadata (e.g., JA3 fingerprints) without decryption.
- **Baselining and Deviation Detection**: Detect deviations from normal traffic volumes or communication paths.

Use Cases

- Detecting malware callbacks and C2 infrastructure.
- Identifying unauthorized data transfers or use of remote management tools.
- Validating firewall and segmentation policies by mapping actual flows.

Limitations

- Storage requirements for full PCAPs are high.
- Encrypted traffic limits payload visibility.
- Flow data may lack sufficient detail without enrichment.

Task 14: Cybersecurity Processes

5. Incident Analysis

Purpose

Incident analysis investigates security alerts and confirmed incidents to determine their origin, scope, and impact. It serves as the backbone of incident response and provides data for long-term security improvements.

Analysis Lifecycle

1. **Triage**: Determine whether an alert is a true positive. Prioritize based on criticality.

2. **Scoping**: Identify all systems, accounts, and assets involved.

3. **Root Cause Analysis**: Trace how the attacker entered (e.g., phishing, RDP, vulnerability exploitation).

4. **Impact Assessment**: Understand what was accessed, modified, or exfiltrated.

5. **Remediation**: Remove persistence mechanisms, revoke access, apply patches.

6. **Recovery**: Restore systems, services, and normal operations.

7. **Post-Incident Review**: Document lessons learned, update detection logic, and improve processes.

Task 14: Cybersecurity Processes

Data Sources and Tools

- **SIEM**: Correlates events and timelines.
- **EDR/Forensics**: Provides disk/memory artifacts and execution traces.
- **Network Logs**: Identify lateral movement, data transfer paths.
- **Threat Intel**: Correlate attack patterns to known adversary groups.

Deliverables

- Timeline of events
- List of affected systems
- IoCs (Indicators of Compromise)
- Remediation steps taken
- Executive and technical reports

Challenges

- Attribution is often imprecise.
- Evidence may be incomplete or overwritten.
- Incident impact may span hybrid and cloud environments.

Task 14: Cybersecurity Processes

6. Sources

- Google Cybersecurity Certificate Material
