Alerting and Monitoring

Objective 4.4: Explain security alerting and monitoring concepts and tools

- **Alerting and Monitoring**
    - Alerting and Monitoring
        - Importance
            - Crucial for maintaining integrity, confidentiality, and availability of information systems
        - Components
            - Alerting (notifying personnel of potential security incidents)
            - Monitoring (continuous observation to detect anomalies or threats)
    - Study Topics
        - Types of Alerts
            - *True Positive*
                - Correctly identifies a legitimate issue
            - *False Positive*
                - Incorrectly indicates an issue when there isn't one
            - *True Negative*
                - Correctly recognizes the absence of an issue
            - *False Negative*
                - Fails to alert about a real issue
        - Alerting System Goals
            - Maximize true positives
            - Minimize false positives to avoid alert fatigue

- Monitoring Types
  - *Automated Monitoring*
    - Software tools for scanning and analyzing
  - *Manual Monitoring*
    - Human personnel actively reviewing and analyzing
- Monitoring Resources
  - Overview of monitoring systems, applications, and infrastructure
- Alerting and Monitoring Activities
  - *Log Aggregation*
    - Collecting and centralizing log data
  - *Alerting*
    - Notification of potential security incidents
  - *Scanning*
    - Continuous examination for anomalies
  - *Reporting*
    - Generating reports on system and network status
  - *Archiving*
    - Storing historical data
  - *Alert Response and Remediation/Validation*
    - Responding to alerts and validating remediation
- *Simple Network Management Protocol (SNMP)*
  - Widely used in network management systems
  - Monitors and manages network devices
  - SNMP traps for setting up and collecting data
- *Security Information and Event Management (SIEM)*
  - Integrated management technologies for holistic security views

        - Collects and aggregates log data
        - Agent-based and Agentless Monitoring
    - Data from Security Tools
        - Collection from various sources (Antivirus, DLP systems, NIDS, NIPS, firewalls, Vulnerability scanner)
        - Consolidation in a SIEM
    - *Security Content Automation and Protocol (SCAP)*
        - Enables automated vulnerability management, measurement, and policy compliance evaluation
    - *Network Traffic Flows*
        - A sequence of packets from source to destination
        - Identifiable by a unique set of identifiers
        - Crucial for understanding network usage patterns and detecting security threats
    - *Single Pane of Glass*
        - Consolidates data from different sources into a unified display
        - Provides administrators with a comprehensive view

- **Monitoring Resources**
    - *Monitoring Systems*
        - Involves observing a computer system's performance, including
            - CPU
            - Memory
            - Disk usage
            - Network performance

- *Baseline*
  - A reference point representing normal system behavior under typical operating conditions
  - Baseline metrics can include CPU usage, memory utilization, disk activity, and network traffic
  - Deviations from the baseline can indicate potential issues, prompting proactive troubleshooting and maintenance
- *Application Monitoring*
  - Focuses on managing and monitoring software application performance and availability
  - Tracks errors, bottlenecks, and issues that may affect an application's performance or user experience
  - Tools like New Relic and AppDynamics track response times and error rates
  - Slower response times may indicate code problems or resource deficiencies
- *Infrastructure Monitoring*
  - Observes physical and virtual infrastructure, including servers, networks, virtual machines, containers, and cloud services
  - Provides insights into network traffic, bandwidth usage, and device status
  - Tools like SolarWinds and PRTG Network Monitor help monitor network infrastructure
  - Overloaded network switches can signal the need for additional capacity or configuration issues

- **Alerting and Monitoring Activities**
    - Alerting and monitoring utilizes a wide range of activities
        - *Log Aggregation*
            - Collects and consolidates log data from various sources into a central location
            - Aids in troubleshooting, performance monitoring, security analysis, and compliance
            - Provides a holistic view of system events for identifying issues and correlations
            - Vital for maintaining system health and analyzing performance trends
            - Used for
                - Detecting security incidents
                - Investigating breaches
                - Gathering evidence
        - *Alerting*
            - Involves setting up notifications for specific events or conditions
            - Alerts can be triggered based on thresholds or anomalies
            - Critical for proactive issue resolution, incident detection, and regulatory compliance
            - Delivered through various channels, such as email, SMS, or push notifications
        - *Scanning*
            - Regularly examines systems, networks, or applications to identify vulnerabilities, misconfigurations, and issues

- Includes the following
    - *Vulnerability scanning*
        - Checks for vulnerabilities in systems, networks, or applications
        - Compares system's state against a database of known vulnerabilities
    - *Configuration scanning*
        - Checks for misconfigurations that could impact system performance or security
        - Deviations are flagged for administrative review
    - *Code scanning*
        - Checks the source code of an application for potential issues, such as security vulnerabilities or coding errors
- Utilizes tools like Nessus, OpenVAS, and Qualys
- Helps maintain system health, security, and optimal performance

- *Reporting*
    - Generates summaries or detailed reports based on collected and analyzed data
    - Provides insights into system performance, security incidents, compliance status, and more
    - Essential for compliance reporting and continuous improvement
- *Archiving*
    - Involves long-term storage of data, including
        - Log data
        - Performance data
        - Incident data

- Ensures data is retained for future reference, analysis, auditing, or compliance
- Important for legal and regulatory requirements
- Can be achieved using cloud storage solutions like Amazon S3 or Google Cloud Storage

■ *Alert Response and Remediation/Validation*

- Managing and resolving identified issues based on alerts or scans
- Begin by taking appropriate actions such as
  - Investigating
  - Escalating
  - Initiating
- Initial response may include investigation, escalation, or predefined procedures
- *Remediation*
  - involves taking steps to address vulnerabilities or issues, such as patching or reconfiguration
- *Validation*
  - verifies that remediation efforts were successful in addressing the identified problems

○ *Quarantining*

■ Isolates a system, network, or application suspected of being compromised
■ Prevents the spread of threats and limits potential impact
■ Commonly used when dealing with malware infections

○ *Alert Tuning*

■ Adjusts alert parameters to reduce errors, false positives, and improve alert relevance

        - Can involve changing alert thresholds, conditions, or delivery methods
        - Helps minimize excessive alerts and noise, making alerts more actionable

- **Simple Network Management Protocol (SNMP)**
    - *SNMP (Simple Network Management Protocol)*
        - An Internet protocol used for collecting information from managed devices on IP networks and modifying device behavior
        - Managed devices include the following
            - Routers
            - Switches
            - Firewalls
            - Printers
            - Servers
            - Client devices
    - *SNMP Manager*
        - A central system that collects and processes information from managed devices
        - Often set up as a server, especially in large enterprise environments
        - Sends and receives SNMP messages to and from agents
    - *SNMP Agents*
        - Networked devices that send information about themselves to the manager
        - Run background services to collect data and send it to the manager
        - Transmit data at regular intervals or when requested by the manager
    - SNMP Message Types
        - *SET*
            - Manager-to-agent request to change variable values

- *GET*
  - Manager-to-agent request to retrieve variable values
- *TRAP*
  - Asynchronous notifications from agents to the manager to notify significant events
  - Notify the manager of events such as uptime, configuration changes, and network downtime
  - May be granular or verbose
    - *Granular*
      - Sent TRAP messages get a unique object identifier OID) to distinguish each message as a unique message being received
      - *OID (Object Identifier)*
        - Unique object identifier used to identify variables for reading or setting via SNMP
        - Allows the manager to distinguish individual SNMP trap messages
      - *MIB (Management Information Base)*
        - A hierarchical namespace containing OIDs and their descriptions
        - Describes the structure of device subsystem management data
        - Stores consolidated information received through SNMP traps
    - *Verbose*
      - SNMP traps may be configured to contain all of the

information about a given alert or event as a payload

- Data in SNMP TRAPS are stored in a simple key-value pair configuration known as a “variable binding”

- SNMP Versions 1, 2, and 3
  - SNMP versions 1 and 2 use plain-text community strings for access, making them less secure
  - SNMP version 3 offers enhanced security features
    - Security Enhancements in SNMP Version 3
      - *Integrity*
        - Hashing messages before transmission to prevent data alteration
      - *Authentication*
        - Validating the source of messages
      - *Confidentiality*
        - Adding encryption using DES, 3DES, or AES
      - Dividing SNMP components into entities with different access privileges for improved security

- **Security Information and Event Management (SIEM)**
  - *SIEM (Security Information and Event Management)*
    - A solution for real-time or near-real-time analysis of security alerts generated by network hardware and applications
    - SIEM helps correlate various events and incidents from system logs
  - Importance of Log Reviews
    - Critical for security assurance
    - Logs should be reviewed regularly and routinely, not just after an incident or as

part of an instant response

- SIEM Functionality
  - Correlates and analyzes log data
  - Consolidates data from various systems into a centralized database or repository
  - Detects patterns indicating security threats
  - Generates alerts for security teams to investigate
- Agent-Based vs. Agentless SIEM
  - *Agent-Based*
    - Software agents are installed on each system to collect and send log data
    - Provides real-time data and detailed information
  - *Agentless*
    - Log data is collected directly from systems using standard protocols
    - Reduces maintenance but may not collect real-time or detailed data
- SIEM Implementation Considerations
  - Log all relevant events and filter out irrelevant data
  - Establish and document the scope of events
  - Develop use cases to define threats
  - Plan incident response actions for different events
  - Establish a ticketing process to track flagged events
  - Schedule regular threat hunting to detect unnoticed events
  - Provide auditors and analysts with an evidence trail
- Common SIEM Solutions
  - *Splunk*
    - Big data information gathering and analysis tool
    - Offers connectors for various data systems
    - Provides search processing language for data analysis

        - Comes with pre-configured templates and dashboards
    - *ELK (Elastic Stack)*
        - A collection of free and open-source SIEM tools, including the following
            - Elasticsearch
            - Logstash
            - Kibana
            - Beats
        - Components work together for log collection, storage, analysis, and visualization
    - *ArcSight*
        - SIEM log management and analytics software
        - Suitable for compliance reporting for regulations like HIPAA, SOX, and PCI DSS
    - *QRadar*
        - A SIEM log management, analytics, and compliance reporting platform created by IBM
        - Offers a dashboard for data visualization and analysis

- **Data from Security Tools**
    - *Antivirus Software*
        - Protects systems against malware, including the following
            - Viruses
            - Worms
            - Trojans
            - Ransomware
            - Spyware

- Generates data like malware detection logs, system scans, and updates
- Data sent to SIEM for aggregation and correlation
- Helps identify security threats and system health

- *Data Loss Prevention (DLP) Systems*
  - Monitor and control data endpoints, network traffic, and cloud-stored data to prevent data breaches
  - Generate data on potential data leak incidents, policy violations, and suspicious user activities
  - Flags attempts to send sensitive data outside the organization
  - Data sent to SIEM for timely corrective actions
- Network Intrusion Detection Systems and Network Intrusion Prevention Systems
  - *Network Intrusion Detection Systems (NIDS)*
    - Passively identify potential threats and generate alerts
  - *Network Intrusion Prevention Systems (NIPS)*
    - Actively block or prevent threats from accessing the network
  - Data includes the following
    - Detected threats
    - Blocked traffic
    - Network anomalies
  - Sent to SIEM for identifying malicious activity, security vulnerabilities, and effectiveness of intrusion prevention measures
- *Firewalls*
  - Act as a barrier between trusted internal networks and untrusted external networks
  - Filter incoming and outgoing traffic based on security rules (ACLs)
  - Generate logs with data on allowed and blocked traffic, rule changes, and

potential threats

- Sent to SIEM for monitoring network perimeter security and identifying intrusion attempts

- *Vulnerability Scanners*
  - Identify security weaknesses, including missing patches, incorrect configurations, and known vulnerabilities
  - Generate data on identified vulnerabilities, severity, and remediation recommendations
  - Data integrated into SIEM to prioritize vulnerability remediation
    - Used to track remediation progress and verify the effectiveness of steps taken

- **Security Content Automation and Protocol (SCAP)**
  - *Security Content Automation Protocol (SCAP)*
    - Suite of open standards that enhances the automation of vulnerability management, measurement, and policy compliance evaluation of systems deployed in an organization
    - Developed by the National Institute of Standards and Technology (NIST)
    - Enhances the automation of security tasks, including the following
      - Vulnerability scanning
      - Configuration checking
      - Software inventory
  - Components of SCAP
    - SCAP comprises a suite of open standards used to automate security tasks
    - Supports standardized vulnerability scanning, results reporting, and scoring
    - Promotes vulnerability prioritization and compliance with internal and external

requirements

- Ensures that different security tools communicate using the same SCAP formatted data

- SCAP Languages
  - *OVAL (Open Vulnerability and Assessment Language)*
    - XML schema for describing system security states and querying vulnerability reports
  - *XCCDF (Extensible Configuration Checklist Description Format)*
    - XML schema for developing and auditing best-practice configuration checklists and rules
    - Allows improved automation
  - *ARF (Asset Reporting Format)*
    - XML schema for expressing information about assets and their relationships
    - Vendor and technology neutral
    - Flexible
    - Suited for a wide variety of reporting applications

- Enumeration Methods in SCAP
  - *CCE (Common Configuration Enumeration)*
    - Scheme for provisioning secure configuration checks across multiple sources
    - Provides unique identifiers for different system configuration issues
  - *CPE (Common Platform Enumeration)*
    - Identifies hardware devices, operating systems, and applications
    - Standard format:

        - cpe:/part:vendor:product:version:update:edition:language
    - *CVE (Common Vulnerabilities and Exposures)*
        - Describes publicly known vulnerabilities with unique identifiers
        - Standard format
            - CVE-Year first documented-Number
            - CVE-2017-0144
- *Common Vulnerability Scoring System (CVSS)*
    - Used to provide a numerical score reflecting the severity of a vulnerability (0 to 10)
    - Scores are used to categorize vulnerabilities as none, low, medium, high, or critical
    - Scores assist in prioritizing remediation efforts but do not account for existing mitigations
- SCAP Benchmarks
    - *Benchmarks*
        - Sets of security configuration rules for specific products to establish security baselines
        - Provide a detailed checklist that can be used to secure systems to a specific baseline
    - Expressed in the XCCDF format and used for compliance testing
    - Many SCAP Benchmarks available for different systems and applications, ensuring proper system configuration and vulnerability identification
    - Examples of SCAP Benchmarks
        - *Red Hat Enterprise Linux Benchmark*
            - Provides security configuration rules for Red Hat Enterprise Linux
        - *CIS Microsoft Windows 10 Enterprise Benchmark*

        - Includes security configuration rules for Microsoft Windows 10 Enterprise
    - Three languages used in SCAP
        - OVAL
        - XCCDF
        - ARF

- **Network and Flow Analysis**
    - *Full Packet Capture (FPC)*
        - Captures entire packets, including headers and payloads
    - *Flow Analysis*
        - Focuses on recording metadata and statistics about network traffic, saving storage space
        - Doesn't include the actual content, just the metadata
        - Rapidly generates visualizations to map network connections, traffic types and session volumes
    - *Flow Collector*
        - Records metadata and statistics about network traffic
        - Collects information about the following
            - Type of traffic
            - Protocol used
            - Data volume
        - Allows for efficient data storage and reduces processing overhead
    - Metadata vs. Contents
        - Flow analysis provides metadata about data, not the actual content
        - Metadata includes details about traffic types and volumes

        - No information about the content of conversations or messages sent
    - Data Storage and Querying
        - Flow analysis information is stored in a database
        - Data can be queried and used to generate reports and graphs
        - Flow analysis identifies trends, patterns, and anomalies in network traffic
    - *NetFlow*
        - Cisco-developed protocol for reporting network flow information
        - Also known as IPFIX (IP Flow Information Export)
        - Defines traffic flows based on shared characteristics (e.g., source and destination IP)
        - Data collected by NetFlow
            - Network protocol interface
            - IP version and type
            - Source and destination
            - IP addresses
            - Source and destination ports
            - Type of service used
        - Use of NetFlow Data
            - NetFlow data is analyzed visually using various tools
            - Tools like SolarWinds display NetFlow data, highlighting flows
            - Data can be used to identify traffic patterns and anomalies
    - *Zeek*
        - Hybrid tool for network monitoring
        - Monitors traffic like NetFlow but logs full packet captures based on interest
        - Filters or signatures trigger full packet capture to analyze specific data
        - Normalizes data for easy import into other tools for visualization and analysis

- *MRTG (Multi Router Traffic Grapher)*
  - Creates graphs displaying network traffic flows through routers and switches
  - Uses SNMP (Simple Network Management Protocol) to gather data
  - Helps identify traffic patterns and anomalies by visualizing data transfer volumes
- Analyzing Traffic Spikes
  - Traffic spikes can indicate anomalies
  - Investigate the cause of traffic spikes
  - Spike analysis may reveal issues like malware infection or unauthorized data transfer
- *Incident Investigation*
  - Suspicious spikes may require setting up network sniffers
  - Analyze packet capture data and flow analysis to identify indicators of compromise
  - Investigate further to understand the nature of anomalies

- **Single Pane of Glass**
  - *Single Pane of Glass (SPOG)*
    - Central point of access for security teams
    - Provides access to information, tools, and systems for monitoring, managing, and securing an organization's IT environment
    - Offers a unified view of the security posture and facilitates informed decision-making
      - Can quickly and easily access critical information, aiding informed decision-making
  - Benefits of SPOG
    - Simplifies security operations management, offering a unified view in detecting

and responding to threats

- Security teams can monitor the environment for suspicious signs like unusual traffic or failed logins
- Security teams can track the progress of incident response, ensuring that all required steps are taken to resolve an incident
- A SPOG can improve the efficiency of a security operation center by automating repetitive tasks
- Improves collaboration and communication within security teams
- Aids compliance with regulatory and compliance requirements by generating necessary documentation

- Implementation of SPOG
  - Can be implemented as software or hardware
  - Steps for implementing
    - *Defining Requirements*
      - Identify the information, tools, and systems required for effective security management
      - Specify data types (logs, alerts, reports) and integrate necessary tools (intrusion detection, incident response)
    - *Identifying and Integrating Data Sources*
      - Identify data sources (log servers, intrusion detection systems) that need integration
      - Use APIs, webhooks, plugins, or connectors to collect and analyze data from various sources
      - Consider data formats, locations, and integration methods
    - *Customizing the Interface*
      - Design a user-friendly interface

    - Configure panels and views for displaying data and information
    - Create an organized layout for navigation
- *Developing Standard Operating Procedures (SOPs) and Documentation*
    - Document procedures for using the SPOG
    - Ensure security teams understand how to use the solution
    - Promote consistency and repeatability in security operations management
- *Continuous Monitoring and Maintenance*
    - Regularly review collected data and make necessary adjustments
    - Ensure the SPOG is properly configured and secured
    - Protect against unauthorized access