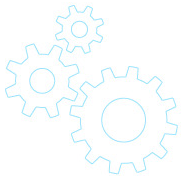


Monitoring Overview



- Continuous monitoring
- Baselines allow for easy detection of anomalies
- Threats are changing constantly
 - New malware variants
 - Hardware and software vulnerabilities
 - Climate change



Incident Management

Assets worth protecting



Threat identification



Threat detection



Threat response

Monitoring Overview

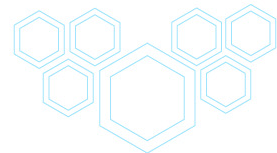


Logging

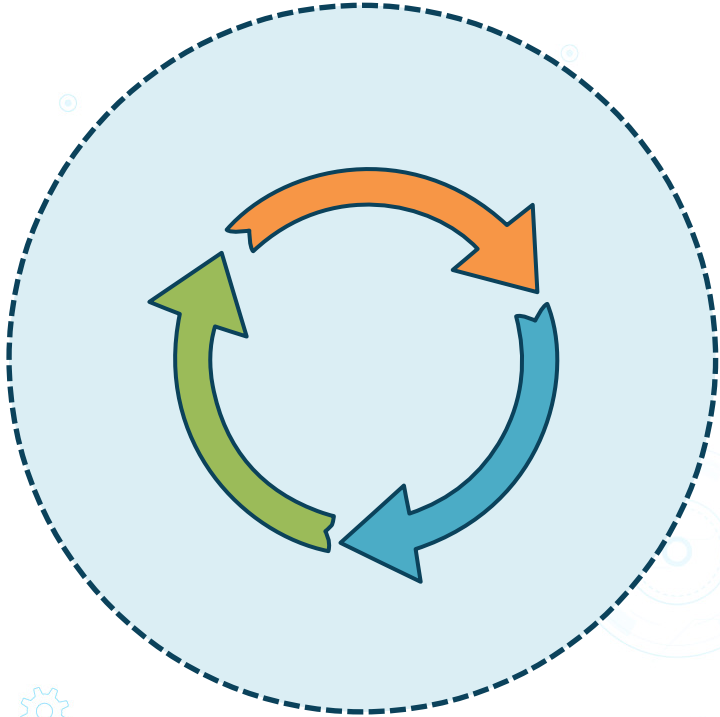
Alert notifications

Network and host scans

IT file and system auditing

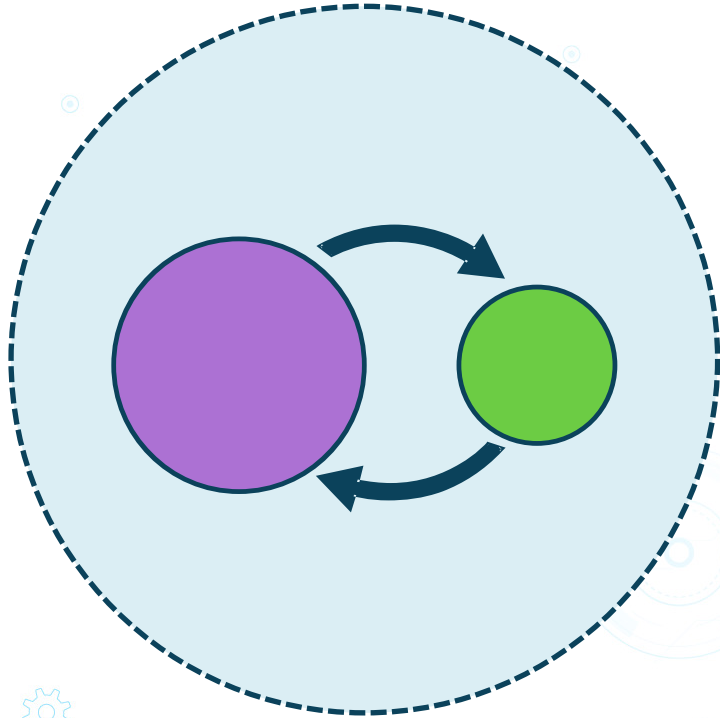


Business Processes



- Driven by organizational objectives
- Interact with assets and personnel
- Defines *how* the organization implements business strategy

Business Processes



- Techniques and tools used to get things done
- Serve the business while ensuring compliance
- Ability to adapt to change
- Periodic review to ensure effectiveness

COBIT 5 Process Reference Model (PRM)

Processes for governance of enterprise IT

Cost management	Resource optimization	HR management
Supplier management	Risk management	Security management
Project management	Change management	Asset management
Problem management	Business continuity	Process controls

Audit Sampling

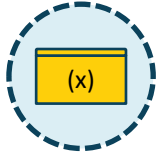


- Assures that audit assertions are backed up by evidence
 - Confidence coefficient normally means a larger sample size
- May be impractical to examine all details
- Identify expected sample outliers
- Identify tolerable error

Audit Sampling Types



Attribute sampling: presence or absence of characteristic



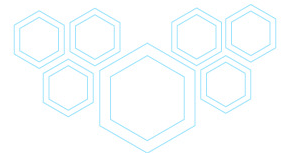
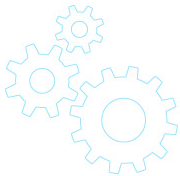
Variable sampling: total or average value



Discovery sampling: highlight deviations in a population



Statistical sampling: mathematical calculations on data subset



Packet Capturing

Network traffic monitoring



The diagram illustrates the packet capturing process. A central light blue circle with a dashed border contains a magnifying glass over a box of binary code. This circle is connected by lines to two tan-colored boxes on either side. The background features faint blue circuit-like patterns, a cloud, a gear, and a hexagonal cluster.

```
graph LR; A[Network traffic monitoring] --- B(( )); B --- C[Hardware or software]
```

01
0101
011110
00101110

Hardware or software


Packet Capturing - Placement



01
0101
0110110
00101110

- NIC promiscuous mode
- Wireless network "isolation" mode
- Network switch monitoring port
 - All switch port traffic is copied here
- Capture traffic on router
- Malicious user ARP poisoning or war flying

Packet Capturing



01
0101
01101110
00101110

Capture/display filters

Amount of traffic needed for valid sample

Baseline comparison

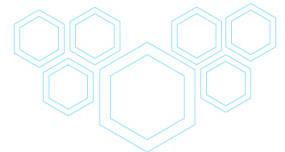
Security Information and Event Management (SIEM)



Real-time security alerts

Security events from multiple sources

Event analysis and correlation



SIEM Data Sources



Web applications



Network infrastructure equipment



Databases



Shared folders




Authentication servers

SIEM Configuration



- Each computing environment is different and the SIEM centralized solution will need to be tweaked
- Reduce false positives
- Baselines of "normalcy"
- Compliance with specific laws and regulations
 - Encryption strength
- Alert thresholds
 - After three incorrect login attempts

Intrusion Detection System (IDS)



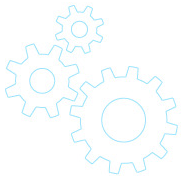
01
0101
0110110
00101110

- Host IDS (HIDS)
- Network IDS (NIDS)
- Hardware or software
- Detect anomalies
 - Log entries
 - Alarm is raised

Intrusion Prevention System (IPS)



- Host IPS (HIPS)
- Network IPS (NIPS)
- Hardware or software
- Detect anomalies and prevent further damage
 - Log entries
 - Alarm is raised
 - Block or reroute traffic
 - Run custom script



Intrusion Detection and Prevention Systems



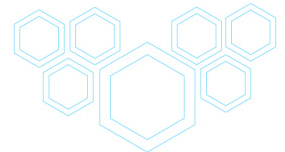
Consider placement

Establish host and network baselines

Consider encrypted network transmissions

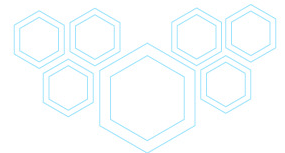
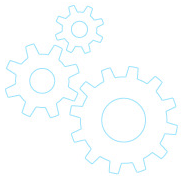
Monitor inbound and outbound traffic

Must be tweaked for the environment



In this exercise, you will

- Describe the purpose of IS audit sampling
- Describe the purpose of SIEM
- List characteristics of an Intrusion Prevention System (IPS)
- Capture and filter HTTP network traffic using Wireshark



IS Audit Sampling

- Assures that audit assertions are backed up by evidence
 - Confidence coefficient normally means a larger sample size
- May be impractical to examine all details
- Identify expected sample outliers
- Identify tolerable error

SIEM

The slide features a central beige box with a dashed dark blue border containing a bulleted list. The title 'SIEM' is at the top center. The background is light blue with various icons: a cloud at the top, a target-like circular graphic on the right, a smartphone and tablet on the right, a gear cluster at the bottom left, and a hexagon cluster at the bottom right. Thin blue lines connect some of these elements.

- Real-time security alerts
- Centralized
- Security events from multiple sources
- Event analysis and correlation

Intrusion Prevention System (IPS)

- Detect anomalies and prevent further damage
 - Log entries
 - Alarm is raised
 - Block or reroute traffic
 - Run custom script