Introduction to SIEM

Course Incharge: **Yahya Batla**

Course Instructor: **Umar Bilal**

Understanding SIEM

- **SIEM** stands for Security Information and Event Management.

It's a comprehensive solution that provides real-time analysis of security alerts generated by applications and network hardware.

Key Functions:

Real-Time Monitoring: Continuous observation of network activity to detect suspicious behavior.

Event Log Management: Collecting and storing logs from various sources for analysis.

Incident Response: Facilitating rapid response to identified security incidents.

Compliance Reporting: Assisting in generating reports for compliance with various cybersecurity standards and regulations.

Why SIEM?

SIEM systems are crucial for modern businesses to quickly detect, analyze, and respond to potential security threats.

They help in maintaining regulatory compliance and enhancing the overall security posture of an organization.

Example SIEM Tools:

Splunk: Known for its powerful data processing capabilities.

IBM QRadar: Offers a comprehensive and scalable solution.

LogRhythm: Integrates log management and SIEM for enhanced security analytics.

SIEM Architecture

Components of a SIEM System:

Data Collection: Gathering data from various sources like network devices, servers, and security systems.

Aggregation: Compiling data from different sources to enable comprehensive analysis.

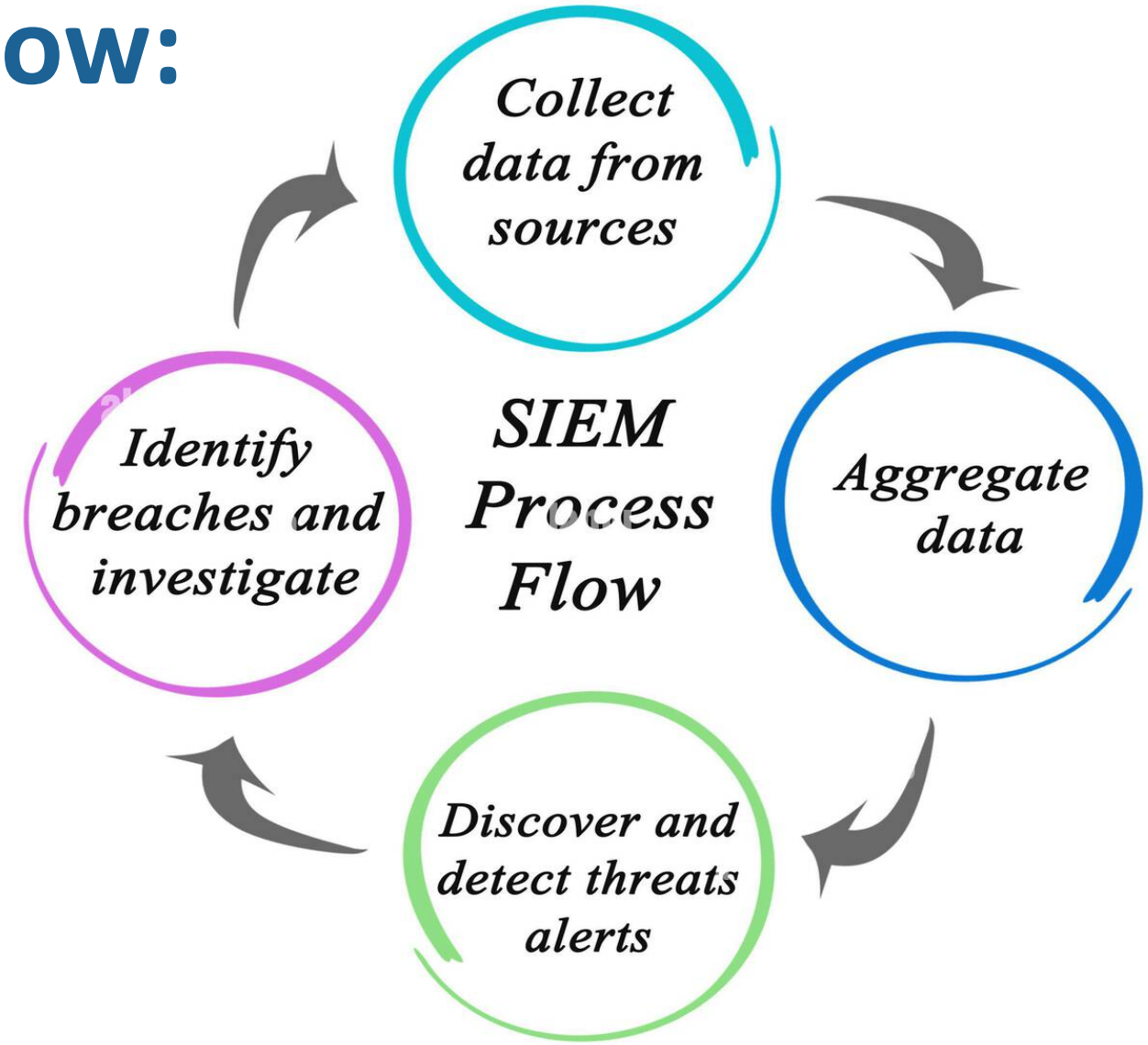
Correlation: Analyzing aggregated data to identify patterns indicative of potential security incidents.

Alerting: Generating notifications based on identified threats or anomalies.

Dashboards: Providing real-time views of an organization's security status.

Compliance Tools: Assisting in adhering to industry regulations and standards.

SIEM Process Flow:



How SIEM Contributes to Cybersecurity:

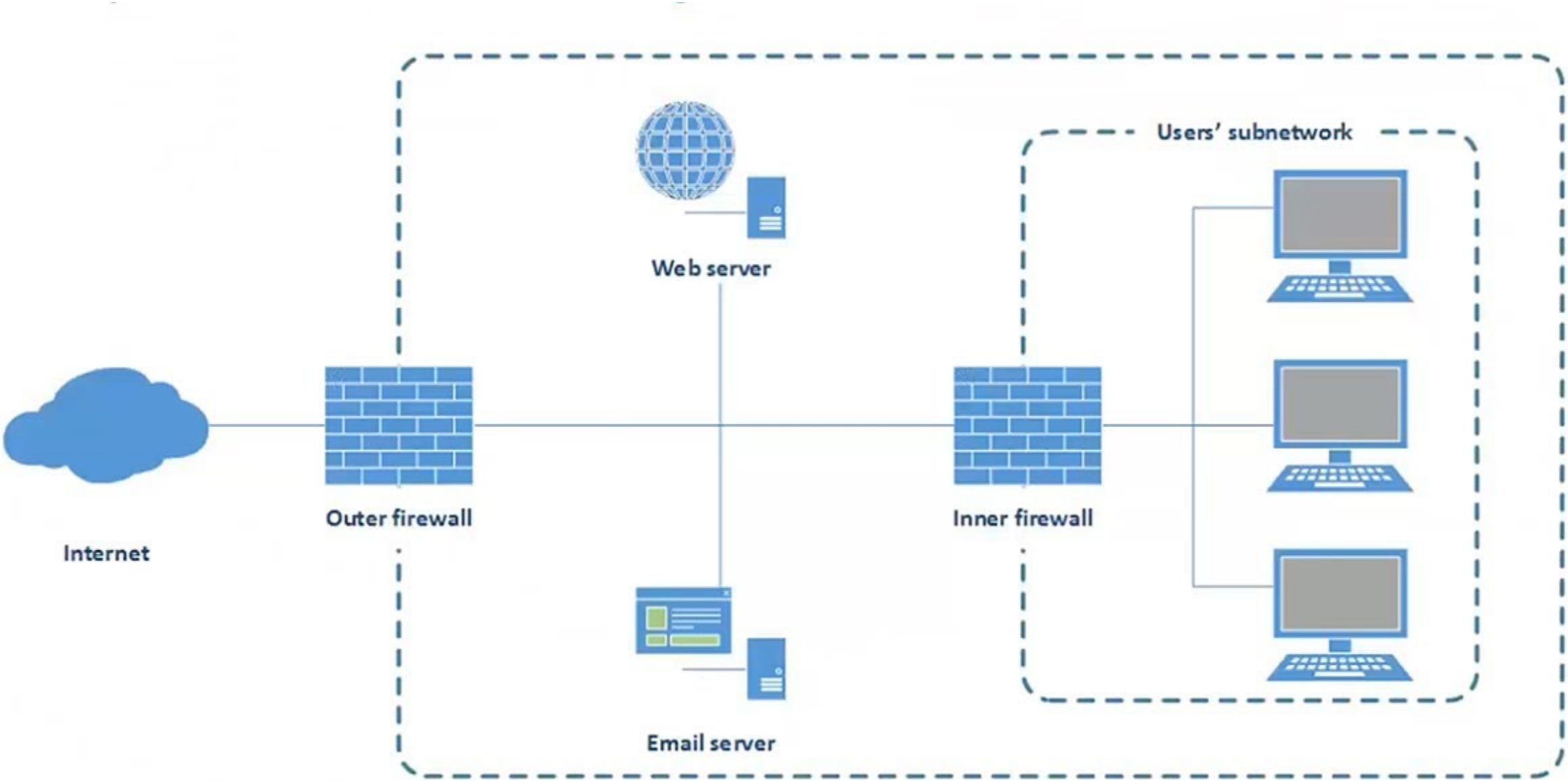
Proactive Threat Detection: Utilizing advanced analytics to identify threats before they cause harm.

Incident Response and Forensics: Enabling quicker response to security incidents and providing tools for post-incident analysis.

Compliance Management: Streamlining the process of meeting various regulatory requirements.

Firewalls

- A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- **Primary purpose:** To establish a barrier between your internal network and incoming traffic from external sources (such as the internet) to block malicious traffic like viruses and hackers.


Users' subnetwork
Web server
Internet
Outer firewall
Inner firewall
Email server

5 Types of Firewalls

1. Packet filtering firewalls

2. Circuit-level gateways

3. Stateful inspection firewalls

4. Application or proxy firewalls

5. Next-generation firewalls

Packet Filtering Firewalls

- Basic form of protection that controls access to network resources by monitoring outgoing and incoming packets.
- Not allowing packets to pass through the firewall unless they match the established rule set.
- Can be configured to block data from certain locations (IP addresses), applications, or ports.
- Pros: Simplicity, low impact on system resources.
- Cons: Limited filtering capabilities; cannot prevent all types of attacks.

Circuit-Level Gateways

- Monitor TCP handshaking between packets to determine whether a requested session is legitimate.
- It works by validating TCP handshake sessions. Once the handshake is confirmed to be legitimate, the firewall sets up a circuit between the user and the external host, allowing packets to flow freely between them.
- Information passed to remote computer through the firewall appears to have originated from the gateway.
- Often used in situations where the speed of connection is crucial but a basic level of security is still needed.
- Pros: Efficiency and speed.
- Cons: Do not inspect the packet itself, so cannot filter individual packet content.

Stateful Inspection Firewalls

- Also known as dynamic packet filtering.
- Keep track of active connections and make decisions based on the state of these connections.
- Inspect both the header and the payload of packets.
- Pros: Greater security than packet filtering or circuit-level gateways.
- Cons: Can impact system performance; more complex to configure.

Application or Proxy Firewalls

- Work at the application layer to filter incoming traffic between your network and the traffic source.
- Acts as an intermediary (proxy) for requests from users seeking resources from other servers.
- Inspects the entire packet, deep into the payload, making them more thorough.
- Pros: Can provide features like content caching and security on specific applications (e.g., HTTP, FTP).
- Cons: Can significantly impact performance due to the level of inspection and overhead.

Next-Generation Firewalls (NGFW)

- Blend features of the other types of firewalls with additional functionalities.
- Include deep packet inspection, intrusion prevention systems, and SSL/SSH inspection.
- Capable of more granular security controls, identifying applications, and enforcing security policies at the application layer.
- Pros: Comprehensive security features.
- Cons: Complexity and cost.

IDS & IPS

IDS and IPS Defined:

- Intrusion Detection Systems (IDS): Monitors network traffic for suspicious activity and issues alerts when such activity is detected.
- Intrusion Prevention Systems (IPS): Actively blocks and prevents intrusion attempts in addition to detecting them.

Types of IDS/IPS:

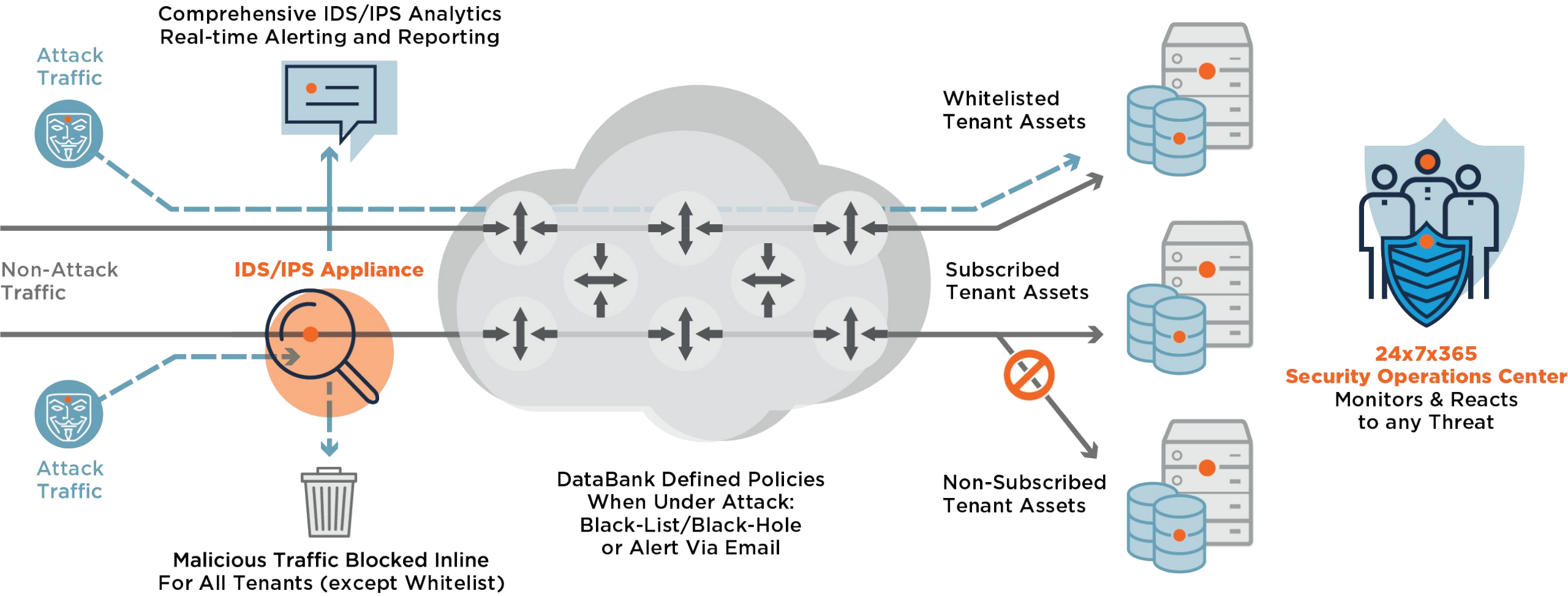
- Network-based: Monitors network traffic for all devices on the network.
- Host-based: Installed on individual devices to monitor and analyze internal traffic.

Key Functionalities:

Signature-based detection, Anomaly-based detection, Policy-based detection

Differences Between IDS and IPS:

IDS is passive and alerts upon detection, while IPS is active and prevents intrusion.


Comprehensive IDS/IPS Analytics
Real-time Alerting and Reporting
Attack Traffic
Non-Attack Traffic
IDS/IPS Appliance
Attack Traffic
Malicious Traffic Blocked Inline
For All Tenants (except Whitelist)
DataBank Defined Policies
When Under Attack:
Black-List/Black-Hole
or Alert Via Email
Whitelisted Tenant Assets
Subscribed Tenant Assets
Non-Subscribed Tenant Assets
24x7x365
Security Operations Center
Monitors & Reacts
to any Threat

Endpoint Detection and Response (EDR)

A security solution focused on detecting, investigating, and mitigating suspicious activities on hosts and endpoints.

- Core Capabilities:
  - Continuous Monitoring: Keeps track of all activities and changes on the endpoints.
  - Threat Detection: Uses behavioral analysis to identify malicious activities.
  - Automated Response: Executes automated responses to isolate and remediate threats.
- Examples of EDR Solutions:
  - CrowdStrike Falcon: Known for its cloud-native platform and AI-powered threat detection.
  - SentinelOne: Offers autonomous endpoint protection.
  - McAfee MVISION EDR: Provides advanced analytics and AI-guided investigations.

Managed Detection and Response (MDR)

A service that combines technology and human expertise to perform threat hunting, monitoring, and response.

- How MDR Services Work:

  - Outsourcing security operations to a dedicated team that continuously monitors and responds to threats.

- Benefits of Using MDR Services:

  - Access to expert security personnel
  - 24/7 monitoring and response capabilities
  - Enhanced threat detection and remediation

Extended Detection and Response (XDR)

An advanced security solution that provides comprehensive threat detection and response across various security layers (email, endpoint, server, cloud workloads, etc.).

- Differences Between XDR and Traditional Endpoint Security:
  - Broader visibility across multiple layers of security
  - Correlation of information from various sources for better threat detection
- Examples of XDR Solutions:
  - Palo Alto Networks Cortex XDR: Integrates network, endpoint, and cloud data.
  - Sophos XDR: Offers extensive visibility into network and endpoint threats.

Best Practices for Implementing Cybersecurity Solutions

- **Best Practices:**
  - Conduct thorough needs analysis and risk assessment.
  - Choose solutions that integrate well with existing infrastructure.
  - Prioritize scalability and flexibility to adapt to evolving threats.
  - Train staff and users on cybersecurity best practices and tool usage.
- **Integration Challenges and Solutions:**
  - Address potential compatibility issues with legacy systems.
  - Ensure proper configuration and regular updates of security tools.
  - Foster a culture of security awareness within the organization.

Pathways to Cybersecurity Expertise: Certifications

Importance of Certifications:

- Validate knowledge and skills in cybersecurity.
- Enhance career prospects and professional credibility.

Overview of Leading Cybersecurity Certifications:

- For beginners: CompTIA Security+
- For intermediate professionals: Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP)
- For advanced professionals: Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA)

International Certifications: CISSP

CISSP: A Gold Standard in Cybersecurity Certification

- **Certified Information Systems Security Professional (CISSP):**
  - Recognized globally as a leading cybersecurity certification.
  - Covers critical security concepts and practices.
- **Eligibility and Benefits:**
  - Requires a minimum of five years of cumulative, paid work experience in two or more of the eight domains.
  - Benefits include higher earning potential, enhanced career opportunities, and recognition as an industry expert.

- **CompTIA Security+:**
  - Target Audience: Individuals starting their cybersecurity career.
  - Key Areas: Network security, compliance and operational security, threats and vulnerabilities, data and host security, identity management, cryptography.
  - Benefits: Lays the foundation for cybersecurity knowledge, widely recognized by employers.
- **Certified Ethical Hacker (CEH):**
  - Target Audience: Mid-level cybersecurity professionals.
  - Key Areas: Ethical hacking methodologies, penetration testing tools and techniques, network and system security assessment.
  - Benefits: Specialized knowledge in ethical hacking, in-demand skillset for cybersecurity defense strategies.

- **Certified Information Security Manager (CISM):**
  - Focuses on management and governance of information security.
  - Ideal for IT professionals aspiring to move into management roles.
  - Benefits: Recognized globally, enhances leadership and management skills.
- **Certified Information Systems Auditor (CISA):**
  - Specializes in information systems auditing, control, and assurance.
  - Suitable for IT auditors and control professionals.
  - Benefits: Recognized as a standard of achievement for IT audit professionals.
- **Certified in Risk and Information Systems Control (CRISC):**
  - Focuses on IT risk management and control.
  - Ideal for IT professionals, project managers, and others involved in IT risk management.
  - Benefits: Enhances skills and knowledge in IT risk identification and management, boosts career opportunities.

THANK YOU