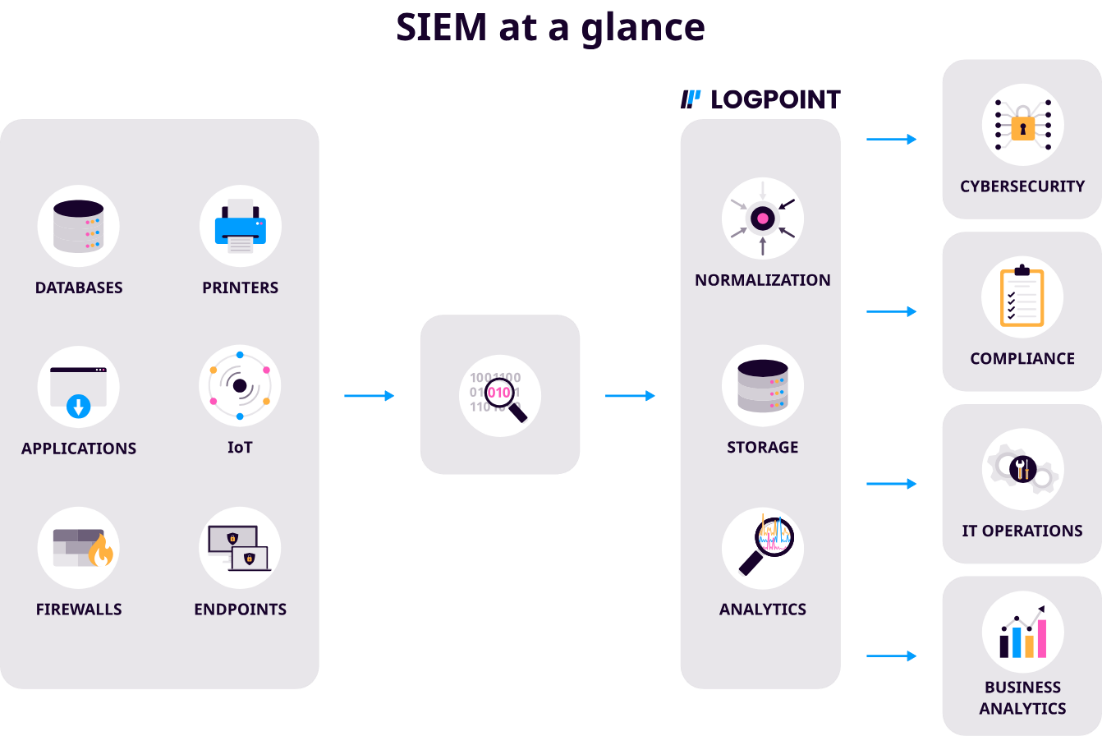
**ACTION PLAN [5] – SIEM | IDS | IPS**

**SIEM** A

* SIEM stands for ‘Security Information & Event Management,’ and is a solution that combines existing tools; namely SIM (Security Information Management) and SEM (Security Event Management).
* Modern SIEM solutions also include technologies such as SOAR to automate threat response and UEBA to detect threats based on anomalous behaviour.
* Together, they provide accelerated detection and response to security events or incidents within an IT environment.
* They provide a comprehensive and centralized view of the security posture of an IT infrastructure and provide cybersecurity professionals with insight into the activities within their IT environment.

Working of SIEM

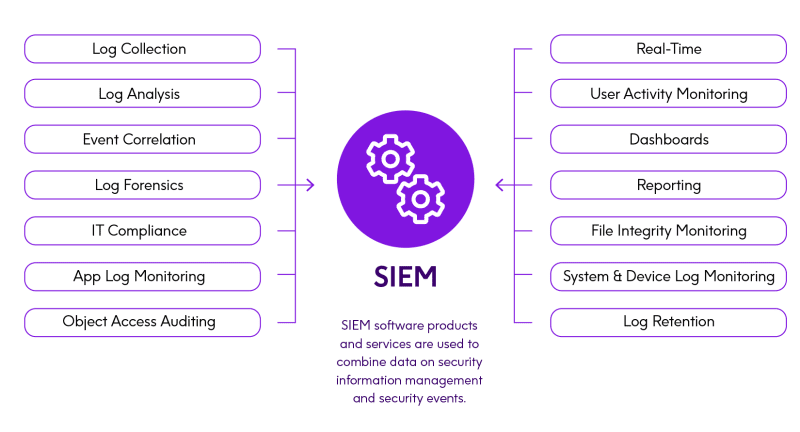
* SIEM software collects and aggregates log data generated across the enterprise’s IT infrastructure from cloud systems and applications to network and security devices such as firewalls and antiviruses.
* The software then identifies, categorizes, and analyses incidents and events.
* SIEM analytics generate and send real-time alerts, dashboards, and reports to multiple critical services related to business operations and management.
* Modern SIEM solutions also use unsupervised machine learning on the collected log data to enable anomaly detection

****

* Normalization: The raw data collected from all the sources is standardized and structured. This makes it easier to analyze because different sources often have their unique formats.
* Storage: Once normalized, the data is securely stored in a repository for analysis and reporting.
* Analytics: The normalized and stored data is analysed to detect patterns, anomalies, or threats.

After the data is processed, the SIEM system provides various benefits depending on the need:

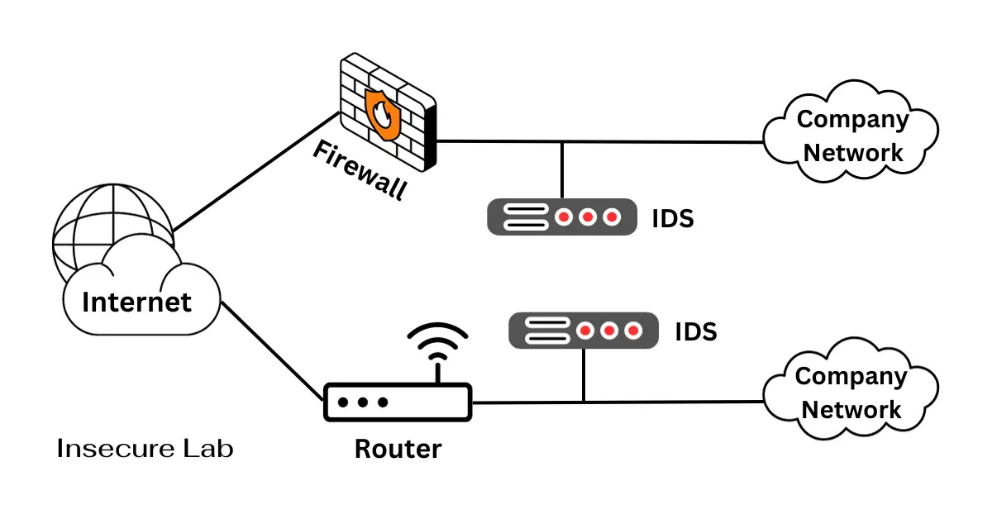
* Cybersecurity: Detects and responds to threats like malware, breaches, or insider attacks.
* Compliance: Ensures adherence to regulatory frameworks such as GDPR, HIPAA, or ISO standards.
* IT Operations: Optimizes IT systems' performance, monitors uptime, and ensures proper functioning.
* Business Analytics: Provides insights to drive business decisions, identify trends, and improve operations.



SIEM Use Cases:

* Threat detection and response
  + A SIEM can help a security team uncover and respond to even some of the most complex threats, such as insider threats, advanced persistent threats, and multidomain attacks.
* Compliance management
  + SOCs often use a SIEM solution to help them stay compliant with regional regulations like the HIPAA (US) and the GDPR (EU).
* Forensic Analysis

**IDS** S



* Intrusion detection system (IDS) is a software application or hardware device that monitors a network or system for malicious activities or policy violations.
* Any suspicious activity or breach detected is typically either reported to an administrator or collected centrally using a security information and event management (SIEM) system.

The primary goal of an IDS is to protect digital assets from several threats, including:

* Unauthorized Access - Preventing unauthorized users from gaining access to sensitive data or systems.
* Malware Detection - Identifying and mitigating the effects of malicious software, such as viruses, worms, and ransomware.
* Denial-of-Service (DoS) Attacks - Detecting and mitigating DoS attacks that overwhelm a system or network, rendering it unavailable.
* Anomalous Behaviour - Recognizing abnormal patterns or activities that may indicate an intrusion attempt.
* Data Exfiltration - Detecting and preventing the unauthorized transfer of data outside the organization.

Types of IDS:

* Network-Based Intrusion Detection Systems (NIDS) - deployed at the network perimeter, monitoring the traffic passing through the network. They analyze network packets, looking for suspicious patterns, known attack signatures, or anomalies that deviate from established baselines.
  + Signature-Based NIDS
    - These systems rely on a database of known attack signatures to identify malicious activities.
    - When incoming traffic matches a signature, the NIDS triggers an alert.
    - While effective against known threats, they may miss zero-day attacks.
  + Anomaly-Based NIDS
    - These systems establish a baseline of normal network behaviour and raise alerts when deviations occur.
    - While more adept at detecting novel threats, they may produce false positives if the baseline is not accurately set.
* Host-Based Intrusion Detection Systems (HIDS) - operate on individual hosts or endpoints, closely monitoring activities within the operating system and applications. They are especially useful for detecting insider threats and attacks that originate from within the organization.
  + System Call-Based HIDS
    - These systems monitor system calls and application interactions, looking for deviations from expected behaviour.
    - They can detect unauthorized access and software vulnerabilities exploitation.
  + Log-Based HIDS
    - Log-Based HIDS analyze system and application logs, searching for unusual patterns or events.
    - They are valuable for detecting unauthorized access and improper configuration changes.

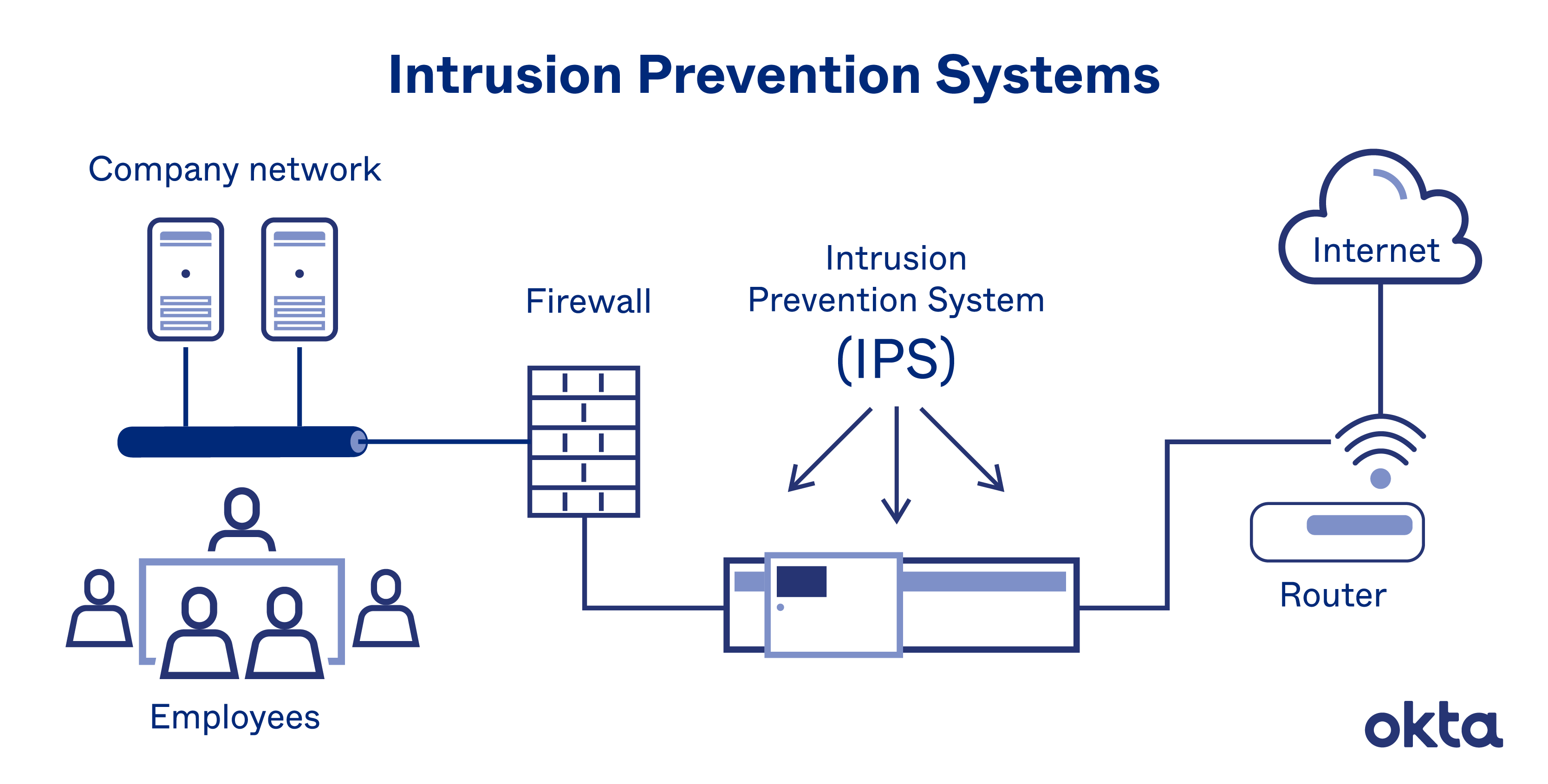
Working of the IDS

* Data Collection - The IDS collects data from various sources, such as network packets, system logs, and event records.
* Preprocessing - The collected data undergoes preprocessing to filter out irrelevant information and format it for analysis.
* Analysis - In this phase, the IDS applies detection algorithms to the pre-processed data. For signature-based systems, it compares network traffic or system activities against a database of known attack signatures. Anomaly-based systems compare data against established baselines or statistical models to identify deviations.
* Alert Generation - When the IDS detects suspicious or malicious activity, it generates alerts. These alerts can vary in severity, and they may trigger responses such as logging the event, notifying system administrators, or even initiating automated countermeasures.
* Response - Depending on the configuration, an IDS can trigger various responses, including blocking network traffic from suspicious sources, isolating compromised hosts, or initiating incident response procedures.

Challenges and Limitations:

* False Positives and Negatives
* Signature Dependency
* Complexity of Network Traffic
* Evasion Techniques
* Resource Consumption

**IPS** A



* An intrusion prevention system (IPS) is a form of network security that works to detect and prevent identified threats.
* Intrusion prevention systems continuously monitor your network, looking for possible malicious incidents and capturing information about them.
* The IPS reports these events to system administrators and takes preventative action, such as closing access points and configuring firewalls to prevent future attacks.
* IPS solutions can also be used to identify issues with corporate security policies, deterring employees and network guests from violating the rules these policies contain.

Working of IPS:

* An IPS sits inline, typically right behind your firewall. Every packet must move past it, and as it moves, each packet is inspected.
* When an anomaly is spotted, the IT administrator is notified. At the same time, the IPS deactivates the threat.
* An IPS is typically designed to spot attacks based on:
  + Signature-Based - The signature-based approach uses predefined signatures of well-known network threats. When an attack is initiated that matches one of these signatures or patterns, the system takes necessary action.
  + Anomaly-Based - The anomaly-based approach monitors for any abnormal or unexpected behaviour on the network. If an anomaly is detected, the system blocks access to the target host immediately.
  + Policy-Based - This approach requires administrators to configure security policies according to organizational security policies and the network infrastructure. When an activity occurs that violates a security policy, an alert is triggered and sent to the system administrators.
* When the IPS detects a problem, it responds by terminating the source of the traffic.
* Then, the system reconfigures the firewall to prevent a future attack, and it scours the network to remove any malignant code records.
* All work done is logged for our review.

**Differences and Similarities between SIEM, IPS, and IDS:**

