Module 05

Network Security Controls - Technical Controls

Module Objectives

- Understanding Network Segmentation and
- Understanding the Different Types of Firew
- Understanding the Different Types of IDS/IP
- Overview of Different Types of Honeypots
- Understanding the Different Types of Proxy
- Understanding the Fundamentals of Virtual in Network Security
- Overview of Security Incident and Event Ma
- Overview of Various Antivirus/Anti-malware

Module Flow

1. Understand Different Types of Network Segmentation
2. Understand Different Types of Firewalls and their Role
3. Understand Different Types of IDS/IPS and their Role
4. Understand Different Types of Honeypots
5. Understand Different Types of Proxy Servers and their Benefits
6. Discuss Fundamentals of VPN and its importance in Network Security
7. **Discuss Security Incident and Event Management (SIEM)**
8. Discuss User Behavior Analytics (UBA)
9. Understand Various Antivirus/Anti-malware Software

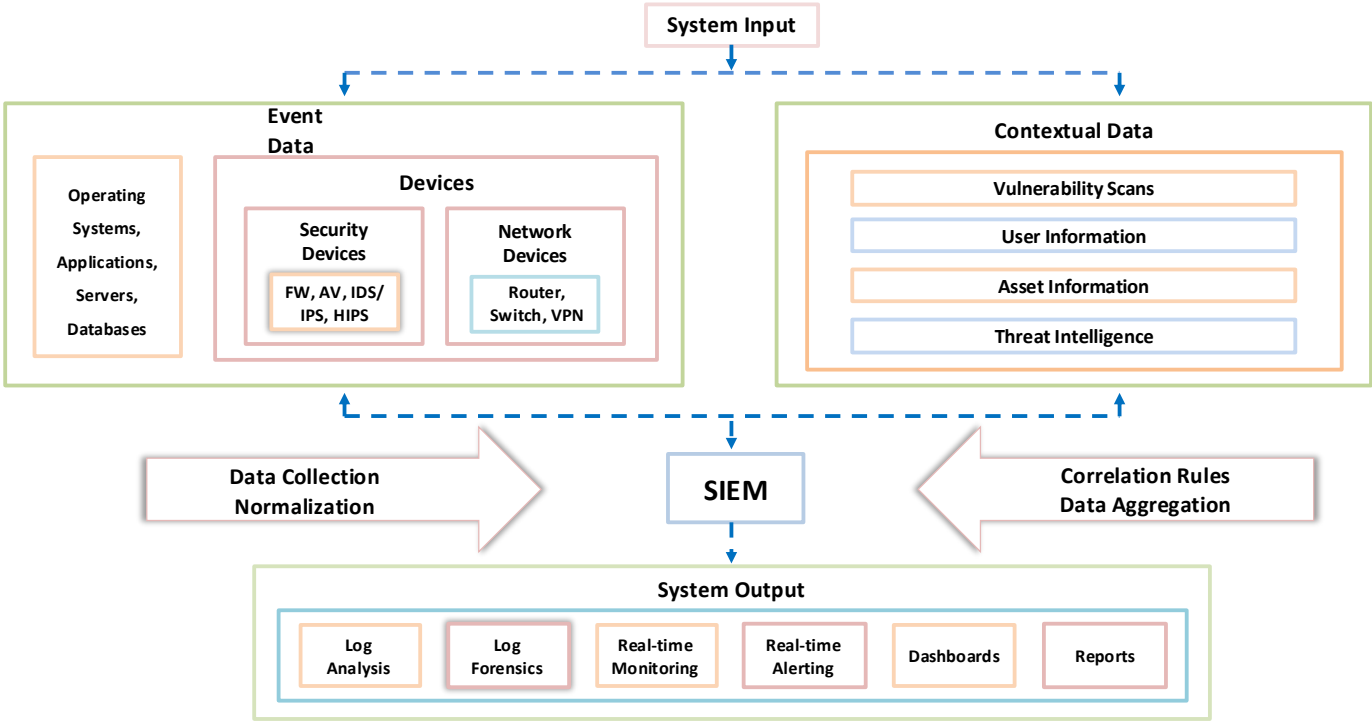
Security Incident and Event Management (SIEM)

1. ❑ SIEM performs **real-time SOC** (Security Operations Center) functions like identifying, monitoring, recording, auditing, and analyzing security incidents

2. ❑ It provides security by **tracking suspicious end-user behavior** activities within a real-time IT environment

3. ❑ It provides security management services combining **Security Information Management** (SIM), and **Security Event Management** (SEM)
   - ✓ SIM supports permanent storage, analysis and reporting of log data
   - ✓ SEM deals with real-time monitoring, correlation of events, notifications, and console views

SIEM Architecture



SIEM Functions

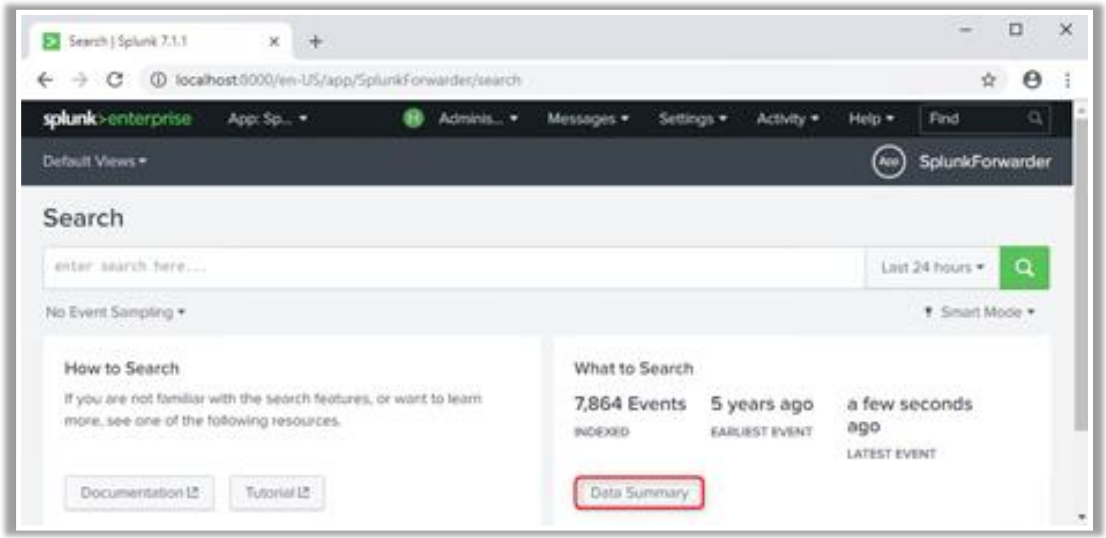
1. Log Collection and Log Analysis
2. Event Correlation
3. Log Forensics
4. IT Compliance and Reporting
5. Application Log Monitoring
6. Object Access Auditing

7. Data Aggregation
8. Real-time Alerting
9. User Activity Monitoring and Dashboards
10. File Integrity Monitoring
11. System and Device Log Monitoring
12. Log Retention

SIEM Solutions

Splunk ES

An analytics driven SIEM solution that provides you with what you need to detect and **respond to internal** and **external attacks** quickly



https://www.splunk.com

- **ArcSight ESM**
  https://www.microfocus.com
- **IBM Qradar SIEM**
  https://www.ibm.com
- **AlienVault OSSIM**
  https://cybersecurity.att.com
- **FortiSIEM**
  https://www.fortinet.com
- **SolarWinds Security Event Manager (SEM)**
  https://www.solarwinds.com

Module Flow

1. Understand Different Types of Network Segmentation
2. Understand Different Types of Firewalls and their Role
3. Understand Different Types of IDS/IPS and their Role
4. Understand Different Types of Honeypots
5. Understand Different Types of Proxy Servers and their Benefits
6. Discuss Fundamentals of VPN and its importance in Network Security
7. Discuss Security Incident and Event Management (SIEM)
8. **Discuss User Behavior Analytics (UBA)**
9. Understand Various Antivirus/Anti-malware Software

User Behavior Analytics (UBA)

01 UBA is the process of **tracking user behavior** to detect malicious attacks, potential threats, and financial fraud

02 It provides **advanced threat detection** in an organization to monitor specific behavioral characteristics of employees

03 UBA technologies are designed to **identify variations** in **traffic patterns** caused by user behaviors which can be either disgruntled employees or malicious attackers

Why User Behavior Analytics is Effective?

1. Detects malicious insiders and outsiders at an early stage
2. Identifies possible risk events in the IT infrastructure
3. Analyzes different patterns of human behavior and large volumes of user's data
4. Monitors geo-location for each login attempt
5. Detects malicious behavior and reduces risk
6. Monitors privileged accounts and provides real time alerts for suspicious behavior
7. Provides insights to security teams
8. Produces results soon after deployment

UBA/UEBA Tools

- User Behavior Analytics (UBA)/User and Entity Behavior (UEBA) Tools collect user activity details from multiple sources and **use artificial intelligence and machine learning (AI/ML)** algorithms to perform user behavior analysis to prevent and detect various threats before the fraud is perpetrated

Exabeam Advanced Analytics
https://www.exabeam.com

LogRhythm UEBA
https://logrhythm.com

Dtex Systems
https://dtexsystems.com

Gurucul Risk Analytics (GRA)
https://gurucul.com

Securonix UEBA
https://www.securonix.com

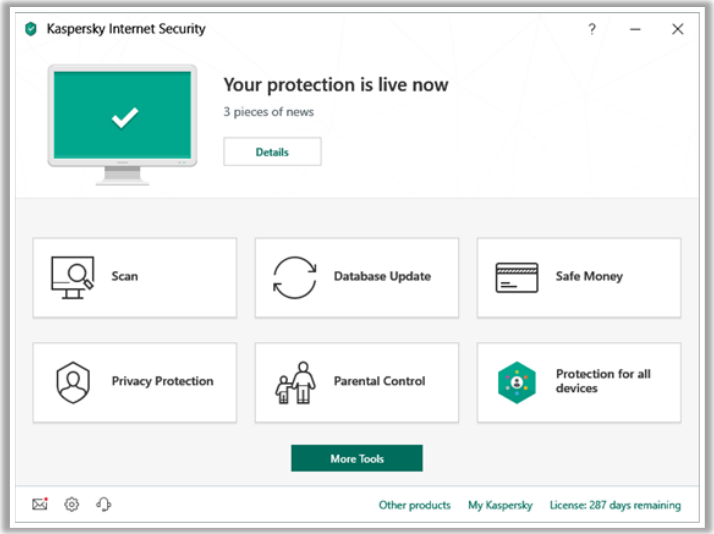
Module Flow

1. Understand Different Types of Network Segmentation
2. Understand Different Types of Firewalls and their Role
3. Understand Different Types of IDS/IPS and their Role
4. Understand Different Types of Honeypots
5. Understand Different Types of Proxy Servers and their Benefits
6. Discuss Fundamentals of VPN and its importance in Network Security
7. Discuss Security Incident and Event Management (SIEM)
8. Discuss User Behavior Analytics (UBA)
9. Understand Various Antivirus/Anti-malware Software

Anti-Trojan Software

Kaspersky Internet Security

Kaspersky Internet Security provides protection against Trojans, viruses, spyware, ransomware, phishing, and dangerous websites



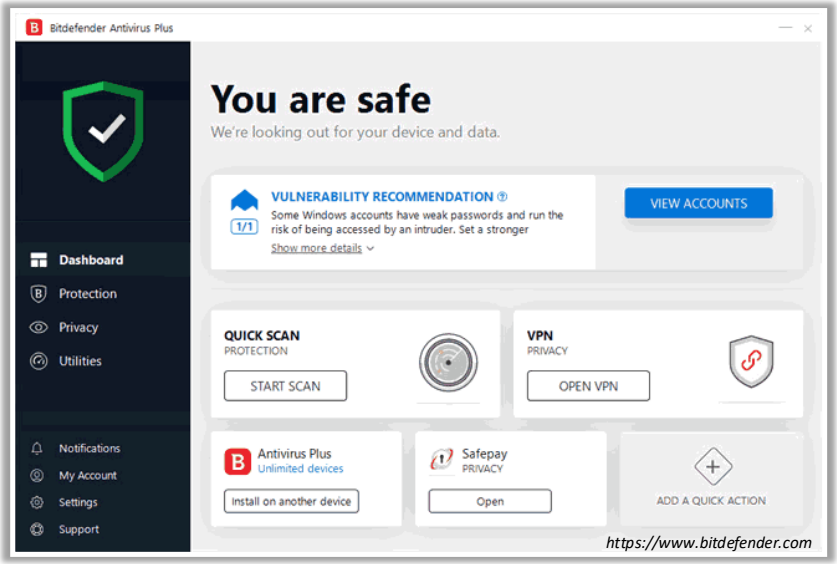
https://www.kaspersky.com

- **McAfee® LiveSafe™**
  https://www.mcafee.com
- **Bitdefender Total Security**
  https://bitdefender.com
- **HitmanPro**
  https://www.hitmanpro.com
- **Malwarebytes**
  https://www.malwarebytes.org
- **Zemana Antimalware**
  https://www.zemana.com

Antivirus Software

Bitdefender Antivirus Plus

Bitdefender Antivirus Plus works against all threats – from viruses, worms and Trojans, to ransomware, zero-day exploits, rootkits and spyware



- **ClamWin**
  http://www.clamwin.com
- **Kaspersky Anti-Virus**
  https://www.kaspersky.com
- **McAfee Total Protection**
  https://www.mcafee.com
- **Avast Premier Antivirus**
  https://www.avast.com
- **ESET Internet Security**
  https://www.eset.com

Module Summary

- This module has discussed network segmentation and its types
- This module introduced you to the different types of firewalls and their roles
- It has also discussed the different types of IDS/IPS and their roles
- This module also explained in detail on the different types of honeypots
- It has also explained the different types of proxy servers and their benefits
- This module briefly explained the fundamentals of VPN and its importance in the network security
- It has also discussed the SIEM and SIEM solutions
- Finally, this module ended with an overview on various antivirus/anti-malware software
- In the next module, we will discuss on virtualization and cloud computing concepts in detail