Intrusion Detection

Intruder

- Apprentice
- Journeyman
- Master

Intruder Behavior - 1

- **Target Acquisition and Information Gathering:** Where the attacker identifies and characterizes the target systems using publicly available information, both technical and non-technical, and the use network exploration tools to map target resources.
  - Explore corporate website for information on corporate structure, personnel, key systems, as well as details of specific web server and OS used.
  - Gather information on target network using DNS lookup tools such as dig, host, and others; and query WHOIS database.
  - Map network for accessible services using tools such as NMAP.
  - Send query email to customer service contact, review response for information on mail client, server, and OS used, and also details of person responding.
  - Identify potentially vulnerable services, eg vulnerable web CMS.

Intruder Behavior - 2

- **Initial Access:** The initial access to a target system, typically by exploiting a remote network vulnerability, by guessing weak authentication credentials used in a remote service, or via the installation of malware on the system using some form of social engineering or drive-by-download attack.
  - Brute force (guess) a user's web content management system (CMS) password.
  - Exploit vulnerability in web CMS plugin to gain system access.
  - Send spear-phishing email with link to web browser exploit to key people.

Intruder Behavior - 3

- **Privilege Escalation:** Actions taken on the system, typically via a local access vulnerability, to increase the privileges available to the attacker to enable their desired goals on the target system.
  - Scan system for applications with local exploit.
  - Exploit any vulnerable application to gain elevated privileges.
  - Install sniffers to capture administrator passwords.
  - Use captured administrator password to access privileged information.

Intruder Behavior - 4

- **Information Gathering or System Exploit:** Actions by the attacker to access or modify information or resources on the system, or to navigate to another target system.
  - Scan files for desired information.
  - Transfer large numbers of documents to external repository.
  - Use guessed or captured passwords to access other servers on network.

Intruder Behavior - 5

- **Maintaining Access:** Actions such as the installation of backdoors or other malicious software, or through the addition of covert authentication credentials or other configuration changes to the system, to enable continued access by the attacker after the initial attack.
  - Install remote administration tool or rootkit with backdoor for later access.
  - Use administrator password to later access network.
  - Modify or disable anti-virus or IDS programs running on system.

Intruder Behavior - 6

- **Covering Tracks:** Where the attacker disables or edits audit logs to remove evidence of attack activity, and uses rootkits and other measures to hide covertly installed files or code.
  - Use rootkit to hide files installed on system.
  - Edit logfiles to remove entries generated during the intrusion.

Intrusion Detection

- **Intrusion Detection:** A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.
- An IDS comprises three logical components:
  - **Sensors**: Sensors are responsible for collecting data.
  - **Analyzers**: Analyzers receive input from one or more sensors or from other analyzers. The analyzer is responsible for determining if an intrusion has occurred.
  - **User interface:** The user interface to an IDS enables a user to view output from the system or control the behavior of the system

Intrusion Detection

- IDSs are often classified based on the source and type of data analyzed
  - **Host-based IDS (HIDS)**: Monitors the characteristics of a single host and the events occurring within that host, such as process identifiers and the system calls they make, for evidence of suspicious activity.
  - **Network-based IDS (NIDS)**: Monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.
  - **Distributed or hybrid IDS**: Combines information from a number of sensors, often both host and network-based, in a central analyzer that is able to better identify and respond to intrusion activity.

Analysis Approaches

- **Anomaly detection:** Involves the collection of data relating to the behavior of legitimate users over a period of time. Then current observed behavior is analyzed to determine with a high level of confidence whether this behavior is that of a legitimate user or alternatively that of an intruder.
- **Signature or Heuristic detection:** Uses a set of known malicious data patterns (signatures) or attack rules (heuristics) that are compared with current behavior to decide if is that of an intruder. It is also known as misuse detection. This approach can only identify known attacks for which it has patterns or rules.

Anomaly detection

- Statistical
- Knowledge based
- Machine-learning
  - Bayesian networks
  - Markov models
  - Neural networks
  - Fuzzy logic
  - Genetic algorithms
  - Clustering and outlier detection

Signature or Heuristic detection

- **Signature approaches** match a large collection of known patterns of malicious data against data stored on a system or in transit over a network
- **Rule-based heuristic identification** involves the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses

HIDS

- The HIDS monitors activity on the system in a variety of ways to detect suspicious behavior
- Data Sources and Sensors
  - System call traces
  - Audit (log file) records
  - File integrity checksums
  - Registry access

Types of HIDS

- **Anomaly HIDS**
- **Signature or Heuristic HIDS**
- **Distributed HIDS**

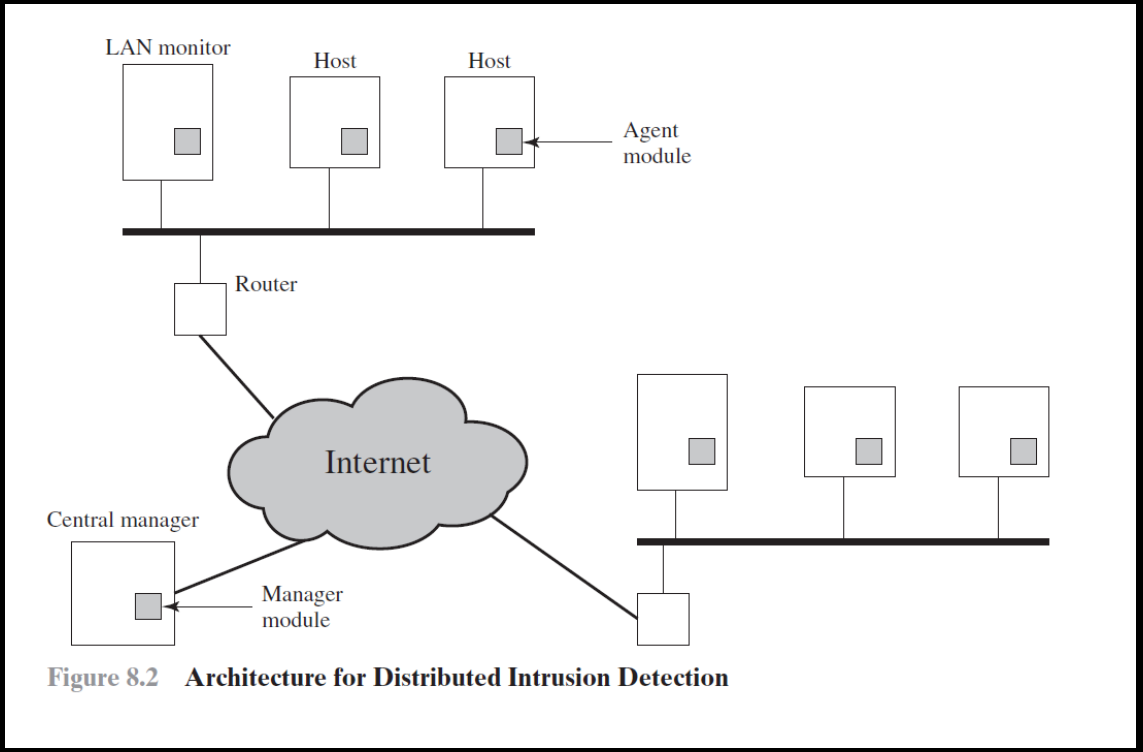


Figure 8.2 **Architecture for Distributed Intrusion Detection**

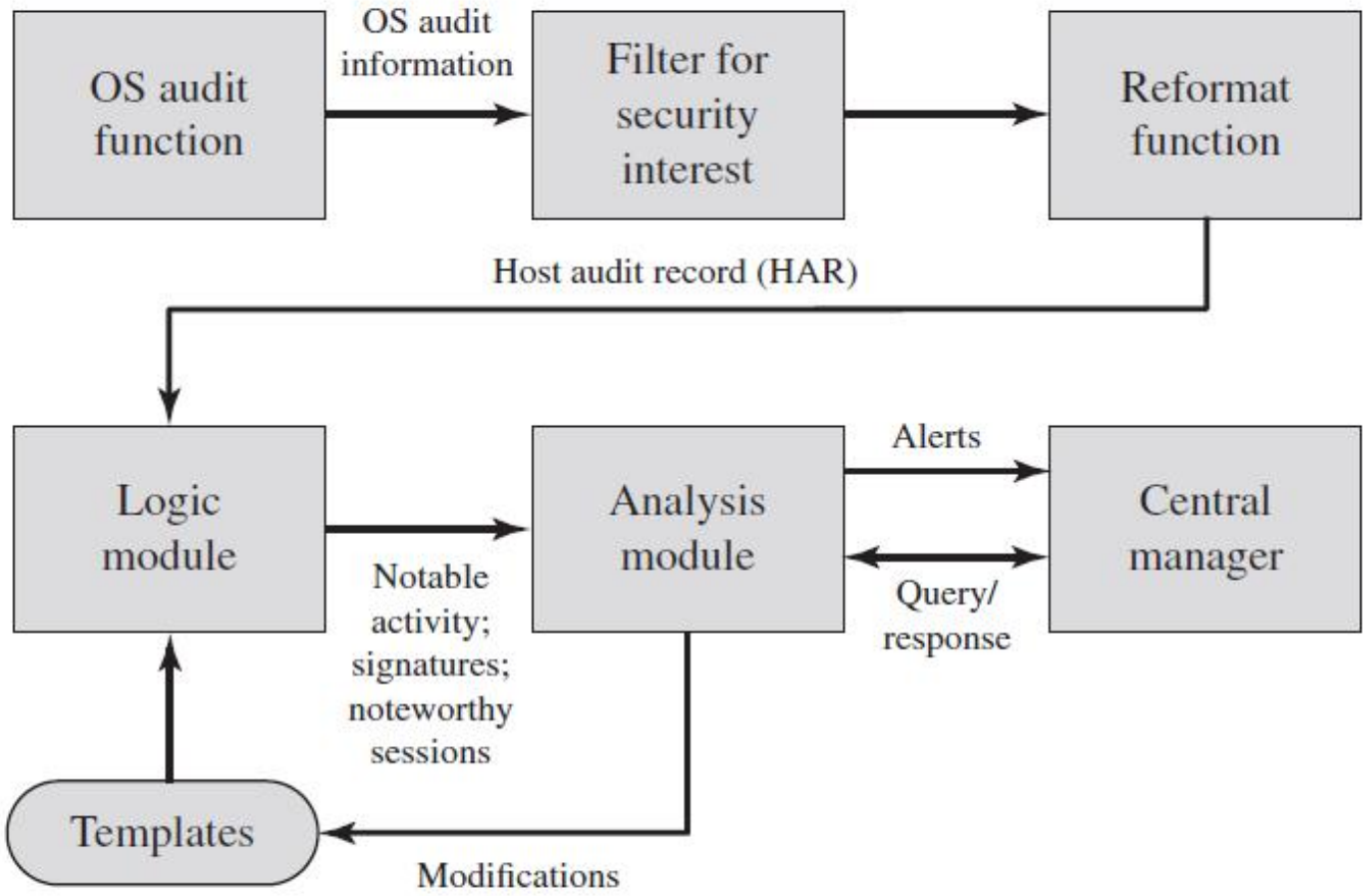


Figure 8.3 Agent Architecture

NIDS

- A network-based IDS (NIDS) monitors traffic at selected points on a network or interconnected set of networks.
- The NIDS examines the traffic packet by packet in real time, or close to real time, to attempt to detect intrusion patterns.
- The NIDS may examine network-, transport-, and/or application-level protocol activity.

Types of Network Sensors

- An **inline sensor** is inserted into a network segment so that the traffic that it is monitoring must pass through the sensor
- A **passive sensor** monitors a copy of network traffic; the actual traffic does not pass through the device

NIDS Sensor Deployment

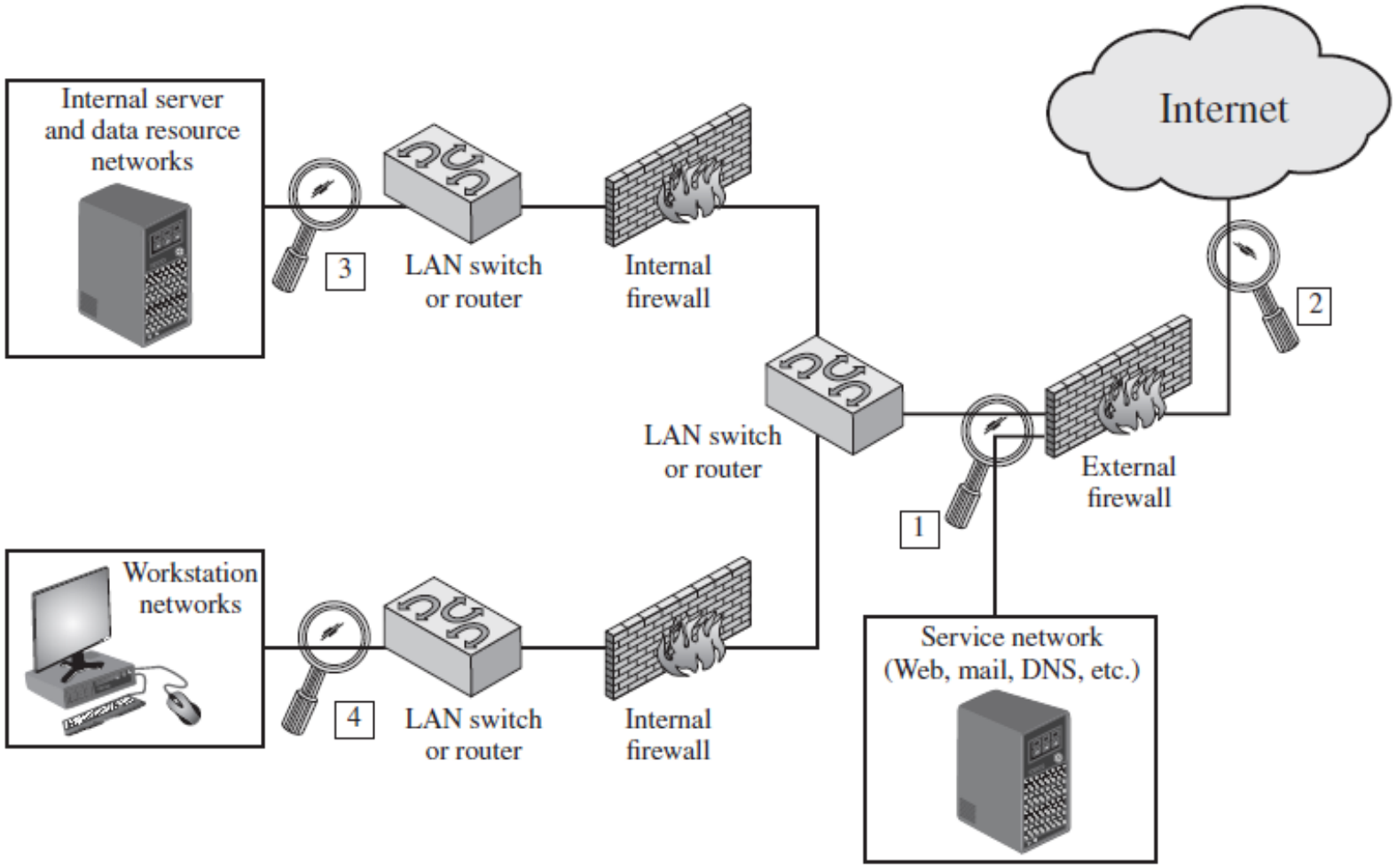


Figure 8.5 **Example of NIDS Sensor Deployment**

Intrusion Detection Techniques - Signature Detection

- **Application layer reconnaissance and attacks**: Most NIDS technologies analyze. several dozen application protocols The NIDS is looking for attack patterns that have been identified as targeting these protocols
- **Transport layer reconnaissance and attacks**: NIDSs analyze TCP and UDP traffic and perhaps other transport layer protocols. Examples of attacks are unusual packet fragmentation, scans for vulnerable ports, and TCP-specific attacks such as SYN floods.
- **Network layer reconnaissance and attacks:** NIDSs typically analyze IPv4, IPv6, ICMP, and IGMP at this level. Examples of attacks are spoofed IP addresses and illegal IP header values.
- **Unexpected application services:** NIDS attempts to determine if the activity on a transport connection is consistent with the expected application protocol. An example is a host running an unauthorized application service
- **Policy violations:** Examples include use of inappropriate Web sites and use of forbidden application protocols

Intrusion Detection Techniques - Anomaly Detection

- Denial-of-service (DoS) attacks
- Scanning
- Worms

Honeypots

- A further component of intrusion detection technology is the honeypot. Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems. Honeypots are designed to:
  - Divert an attacker from accessing critical systems.
  - Collect information about the attacker’s activity.
  - Encourage the attacker to stay on the system long enough for administrators to respond.

Types of Honeypots

- **Low interaction honeypot:** Consists of a software package that emulates particular IT services or systems well enough to provide a realistic initial interaction, but does not execute a full version of those services or systems.
- **High interaction honeypot:** Is a real system, with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers.

Example System: Snort

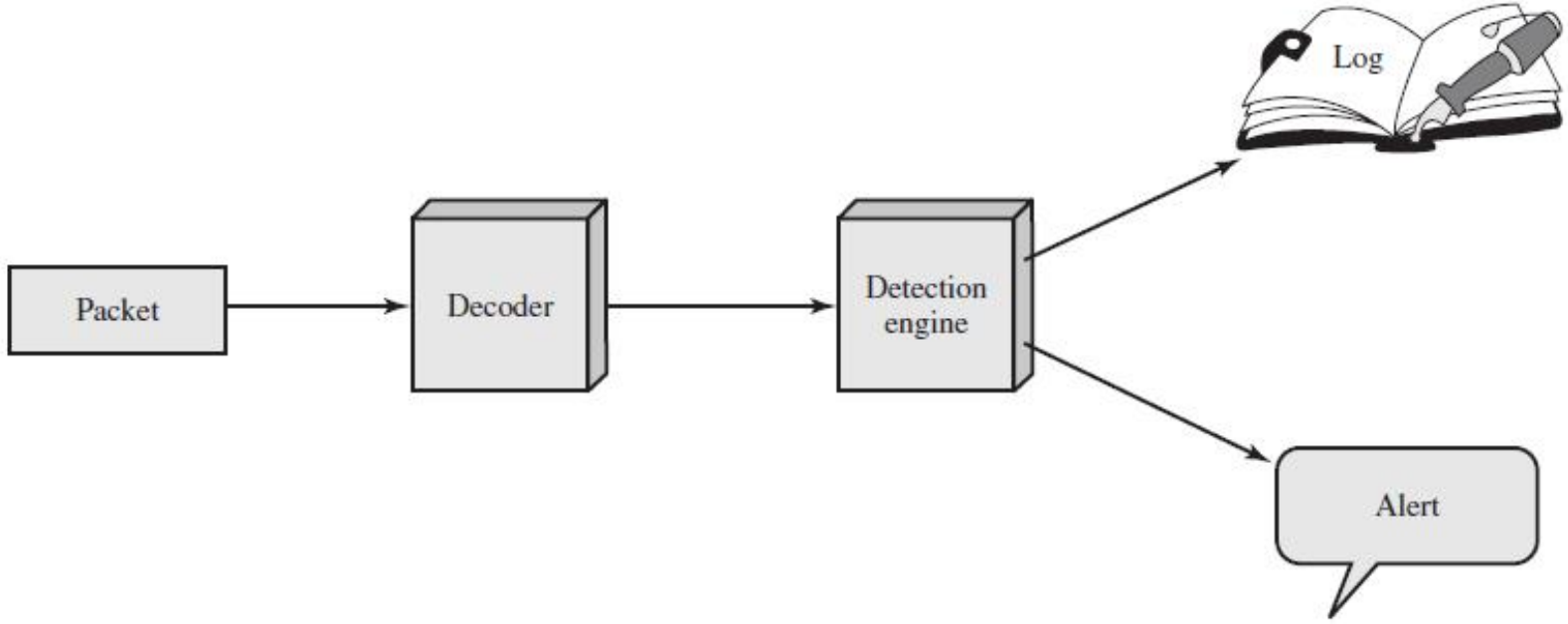


Figure 8.9 **Snort Architecture**

Example System: Snort

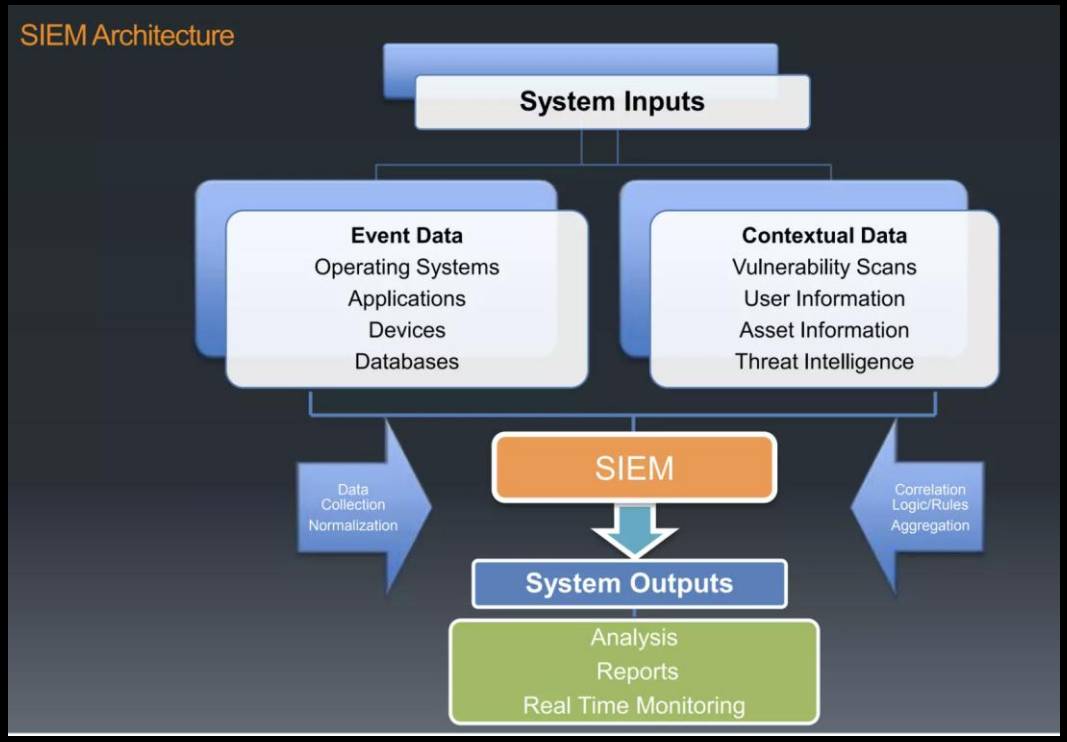
- **Packet decoder:** The packet decoder processes each captured packet to identify and isolate protocol headers at the data link, network, transport, and application
- **Detection engine:** The detection engine does the actual work of intrusion detection. This module analyzes each packet based on a set of rules defined for this configuration of Snort by the security administrator.
- For each packet that matches a rule, the rule specifies what logging and alerting options are to be taken
  - **Logger:** stores the detected packet in human readable format or in a more compact binary format in a designated log file.
  - **Alerter:** For each detected packet, an alert can be sent. The event notification can be sent to a file, to a UNIX socket, or to a database.

SIEM Tool

What is SIEM

- Security Information and event managerment
- Realtime analysys of security alert generated by network hardware and applications

SIEM Architecture



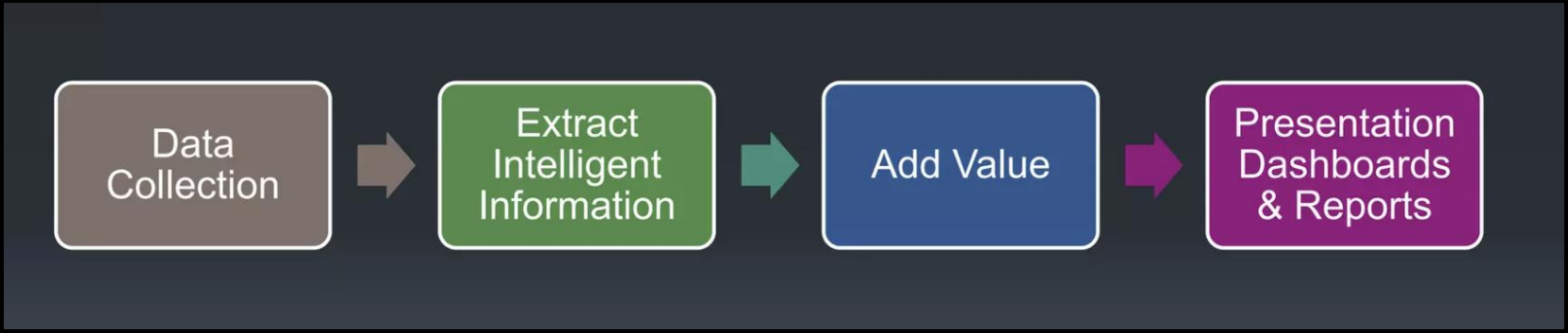
What SIEM do

- Log Management System
- Security Log/Event Management
- Security Information Management
- Security Event Correlation
- Data Aggeration
- Correlation
- Alerting
- Dashboard
- Retention
- Forensic Analysis

How it works

- SIEM tool collected logs from devices present in the Orgazination’s Infrastructure. With the collected data (mainly logs, packet), the tool provide an insight into the happening of networks.
- The SIEM tool can be configured to detect specific incident.

SIEM Process flow



How data reach SIEM

- Agent Base
  - Agent is installed in client machine from wich logs are collected.
- None Agent Base
  - The client system will send logs on it’s own using a serive like Syslog or Windows Event Collector, etc.

Type of Alert

- Repeat Attack login source
  - Early warning brute force attack, password guesing, and misconfiguration of application
- Repeat Attack Firewall
  - Early warning for scan, worm propagation, etc.
- Virus Detection/Remove
  - Alert when malware is detected on host.
- Repeat Attack-Host Intrusion Prevention System
  - Find hosts may be infected or compromised

Conclusion

- Cons
  - SIEM is necessary for better security threat awareness
  - SIME enable quick forensics
  - Enable administrators to study the root cause of error and security breachs.
- Pros
  - Excessive data might be worser than lack of data
  - Report sometime difficulty to understand
  - SIEM take too long to deploy
  - SIEM is too complex

Q/A

- Reading chapter 8 in Text book