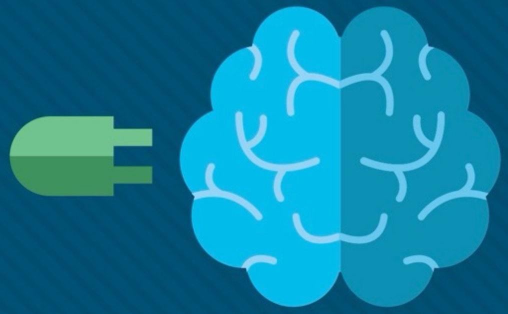


Network Defence & Security Data

IN4180, Feb 13th 2025

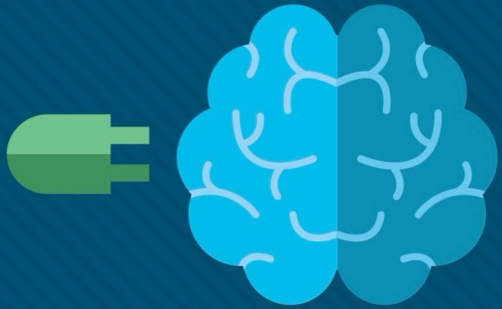
Objectives

Module: Network Security and Defence (4 lectures + workshops)

- **Topics**
  - Network security infrastructure (Feb 6th)
  - Network monitoring and tools (Feb 6th)
  - **Network defence (today)**
  - **Network security data sources and types (today)**
  - Investigating network events (Feb 20th)

Oblig 1

- Compulsory assignment available on Canvas on Monday (Feb 17th)
- There will be time for questions and clarifications after the lecture next week (Feb 20th)
- Recommended to use the Docker environment or a VM with Linux.
- If you use a VM: The version of the tools used in the assingment are from Ubuntu 22.04, but other versions/distros are likely to work as well.



Network Defence

Module Objectives

Module Title: Understanding Defense

Module Objective: Explain approaches to network security defense.

Topic Title	Topic Objective
Defense-in-Depth	Explain how the defense-in-depth strategy is used to protect networks.
Security Policies, Regulations, and Standards	Explain security policies, regulations, and standards.

Module Objectives

Module Title: Access Control

Module Objective: Explain access control as a method of protecting a network.

Topic Title	Topic Objective
Access Control Concepts	Explain how access control protects network data.
AAA Usage and Operation	Explain how AAA is used to control network access.

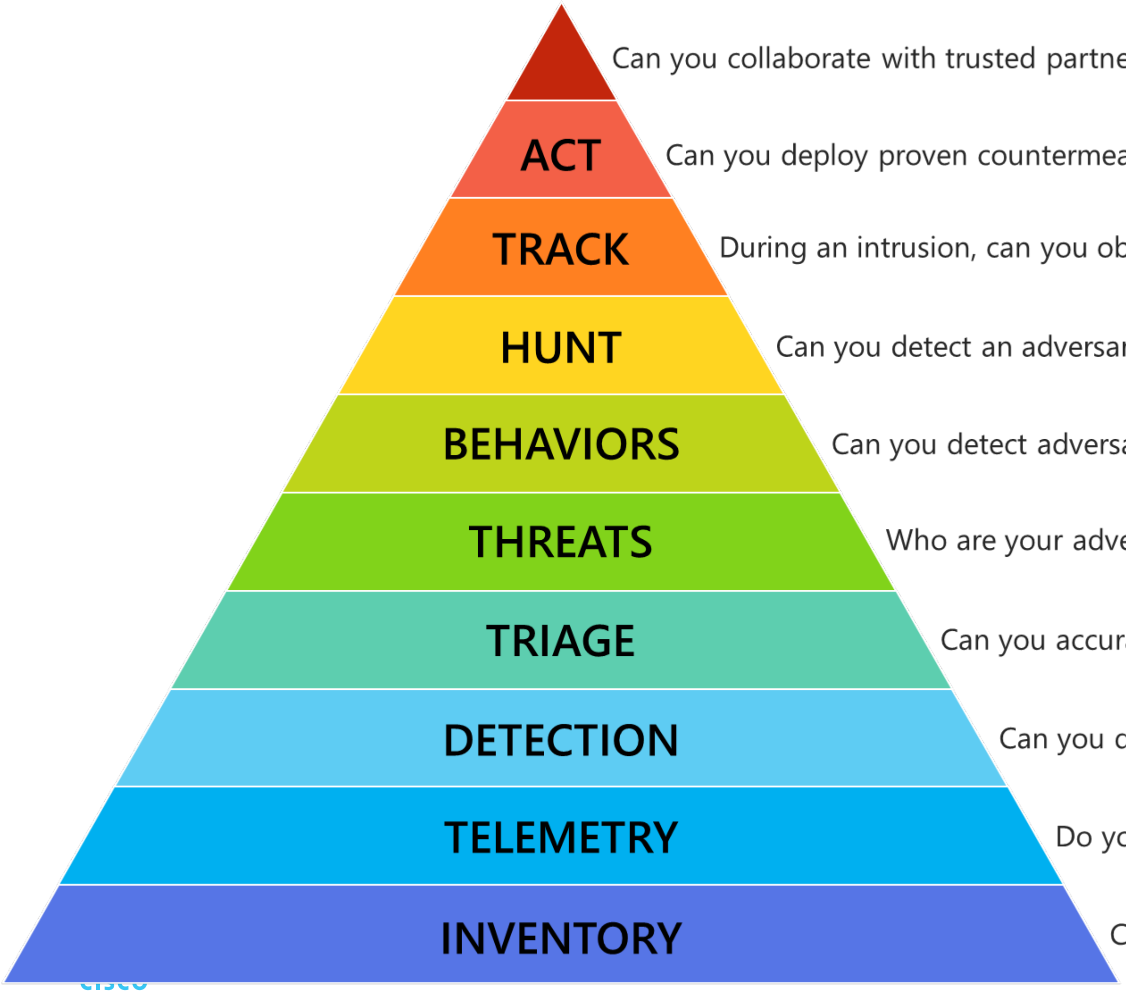
Defense-in-Depth

Understanding Defense

Assets, Vulnerabilities, Threats

- Cybersecurity analysts must prepare for any type of attack. It is their job to secure the assets of the organization’s network.
- To do this, cybersecurity analysts must first identify:
  - **Assets** - Anything of value to an organization that must be protected including servers, infrastructure devices, end devices, and the greatest asset, data.
  - **Vulnerabilities** - A weakness in a system or its design that could be exploited by a threat actor.
  - **Threats** - Any potential danger to an asset.

Identifying Assets – Inventory Management



	Can you collaborate with trusted partners to disrupt adversary campaigns?
ACT	Can you deploy proven countermeasures to evict and recover?
TRACK	During an intrusion, can you observe adversary activity in real time?
HUNT	Can you detect an adversary that is already embedded?
BEHAVIORS	Can you detect adversary activity within your environment?
THREATS	Who are your adversaries? What are their capabilities?
TRIAGE	Can you accurately classify detection results?
DETECTION	Can you detect unauthorized activity?
TELEMETRY	Do you have visibility across your assets?
INVENTORY	Can you name the assets you are defending?

M. Swann – Incident Response Hierarchy of Needs - https://github.com/swannman/ircapabilities

Understanding Defense

Identify Assets

- The collection of all the devices and information owned or managed by the organization are the assets.
- These assets must be inventoried and assessed for the level of protection needed to thwart potential attacks.
- Asset management consists of inventorying all assets, and then developing and implementing policies and procedures to protect them.
- This task can be daunting considering many organizations must protect internal users and resources, mobile workers, and cloud-based and virtual services.
- Further, organizations need to identify where critical information assets are stored, and how access is gained to that information.
- Information assets vary, as do the threats against them. Each of these assets can attract different threat actors who have different skill levels and motivations.

Inventory Management – Network monitoring approach

- Network management tools are a way of automating the inventory management and identification process
- Many tools use Simple Network Management Protocol (SNMP) to gather and organise information about devices on the network
- Provide network tomography – view the health of your network
- A comparison of common network monitoring vendors and their features can be found on:
  - https://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems
- Auto discovery features in network management tools aid in automated identification of assets
- SNMP is a standard so you do not need to configure proprietary monitoring for tools that use SNMP
- Since SNMP is a standard it is vendorless. Any device that supports SNMP can communicate with your network monitoring tool.

Example Tools - Solarwinds

- An example network monitoring tool is Solarwinds Network Management
- Provides network performance monitoring
- Auto discovery of network devices
- Alerting and telemetry
- IP address tracking
- Network topology mapping
- Not open source or free
- Demo:
  - https://oriondemo.solarwinds.com/Orion

Example Tools – LibreNMS

- Free tool that can be implemented within your network infrastructure
- Automatic discovery
- Asset tracking
- Customisable alerts and dashboards
- Demo:
  - https://demo.librenms.org/

Understanding Defense

Identify Vulnerabilities

- Vulnerability identification provides an organization with a list of likely threats for a particular environment.
- When identifying vulnerabilities, it is important to ask several questions:
  - What are the possible vulnerabilities of a system?
  - Who may want to exploit those vulnerabilities to access specific information assets?
  - What are the consequences if system vulnerabilities are exploited and assets are lost?
- Vulnerability identification can be a manual process, automated process or a combination of the two

Threat Intelligence Services

Common Vulnerabilities and Exposures (CVE) Database

- The United States government sponsored the MITRE Corporation to create and maintain a catalog of known security threats called Common Vulnerabilities and Exposures (CVE).
- The CVE serves as a dictionary of CVE Identifiers for publicly known cybersecurity vulnerabilities.
- The MITRE Corporation defines unique CVE Identifiers for publicly known information-security vulnerabilities to make it easier to share data.
- Common CVE data sources:
  - CVE – https://www.cve.org
  - CVE Details - https://www.cvedetails.com/
  - Microsoft Security Response Center - https://msrc.microsoft.com/update-guide/vulnerability
- Example CVEs:
  - https://www.cvedetails.com/cve/CVE-2022-34878/

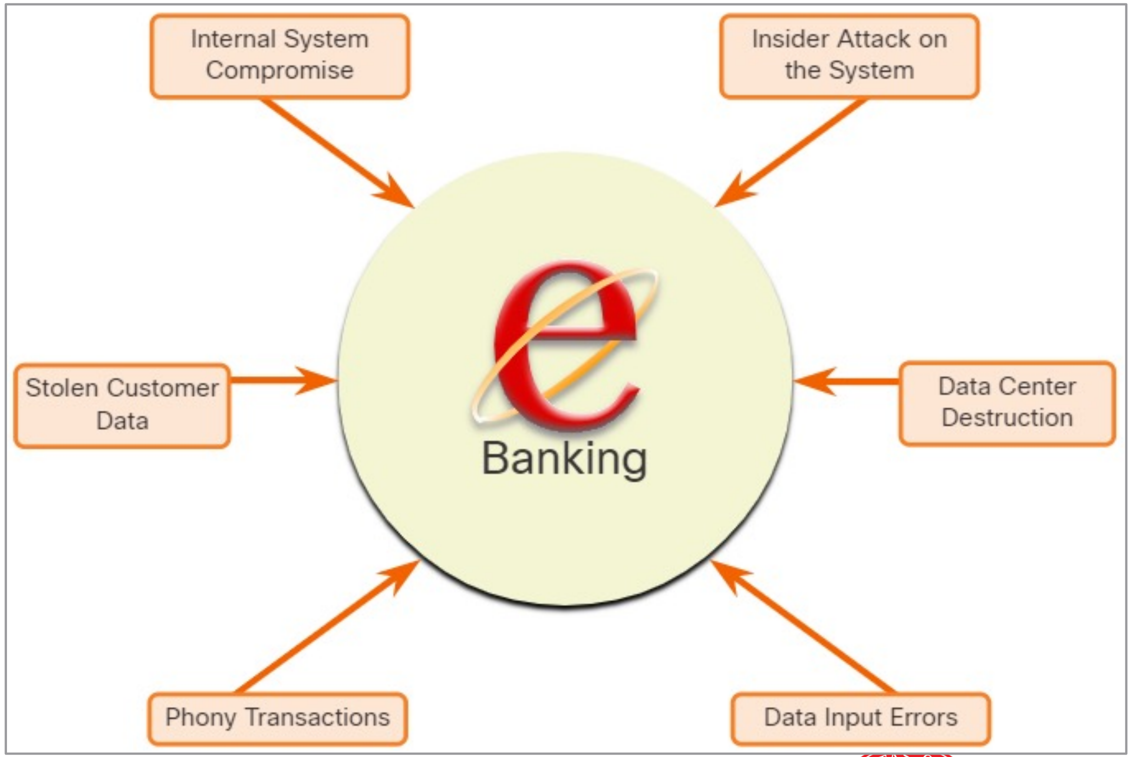
Identify Vulnerabilities Automated Approach

- OpenVAS open source vulnerability scanning and management service. Several services combined as a framework: https://openvas.org
- Utilises pre built network vulnerability tests within its curated security feed.
- About half of the tests detect vulnerabilities with a high severity class – i.e., with a severity between 7.0 and 10.0. Another 40,000 tests such with the severity class "Medium" (severity 4.0 to 6.9). [1]
- Greenbone, the company that produce OpenVAS, actively develop network vulnerability tests and routinely update their feeds
- Other solutions: Nessus (proprietary)
- Both available for free trial/demo (commercial versions)
- Also some support in inventory tools like Solarwinds: https://oriondemo.solarwinds.com/Orion

Threat Identification

The threat identification for an e-banking system would include:

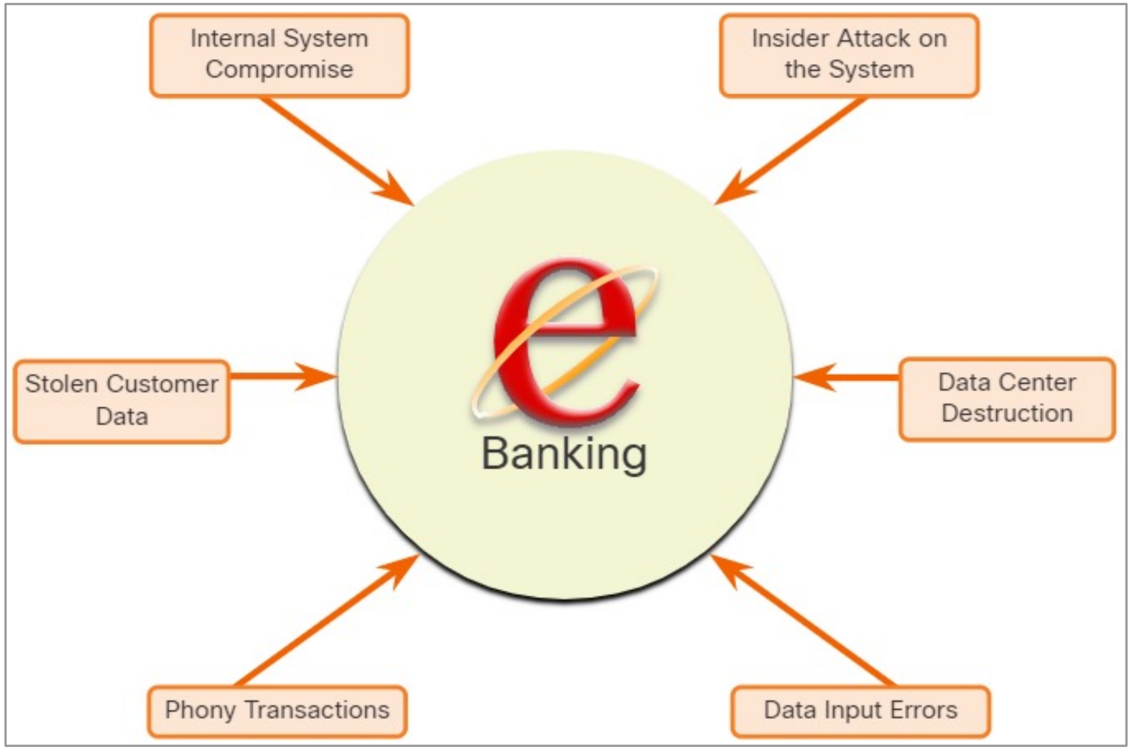
- **Internal system compromise** - The attacker uses the exposed e-banking servers to break into an internal bank system.
- **Stolen customer data** - An attacker steals the personal and financial data of bank customers from the customer database.
- **Phony transactions from an external server** - An attacker alters the code of the e-banking application and makes transactions by impersonating a legitimate user.



Understanding Defense

Threat Identification

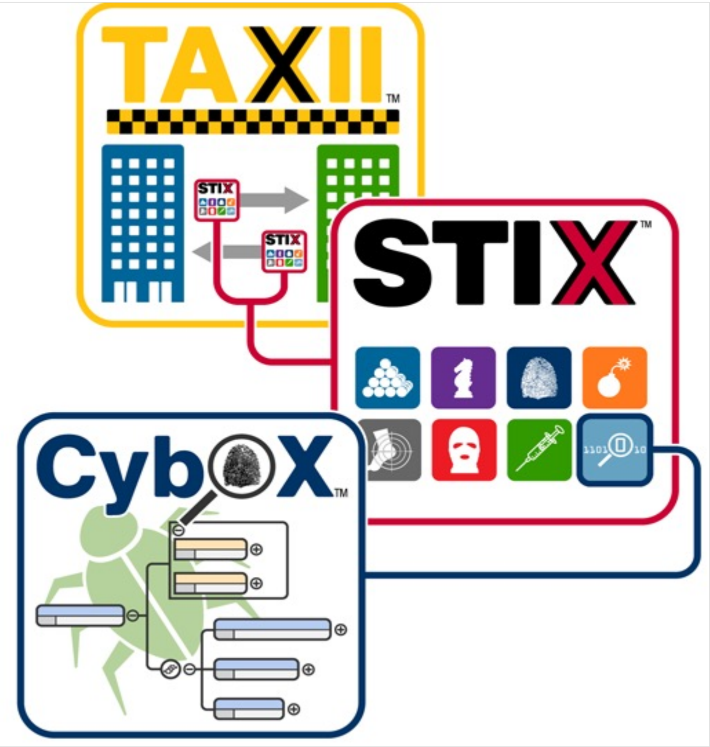
- **Phony transactions using a stolen customer PIN or smart card** - An attacker steals the identity of a customer and completes malicious transactions from the compromised account.
- **Data input errors** - A user inputs incorrect data or makes incorrect transaction requests.
- **Data center destruction** - A cataclysmic event severely damages or destroys the data center.



Threat Intelligence Communication Standards

Common threat intelligence sharing standards include the following:

- **Structured Threat Information Expression (STIX)** - This is a set of specifications for exchanging cyber threat information between organizations.
- **Trusted Automated Exchange of Indicator Information (TAXII)** – This is the specification for an application layer protocol that allows the communication of CTI over HTTPS. TAXII is designed to support STIX.
- **CybOX** – A structured language for cyber observables, now integrated into **STIX**



Threat Intelligence Services

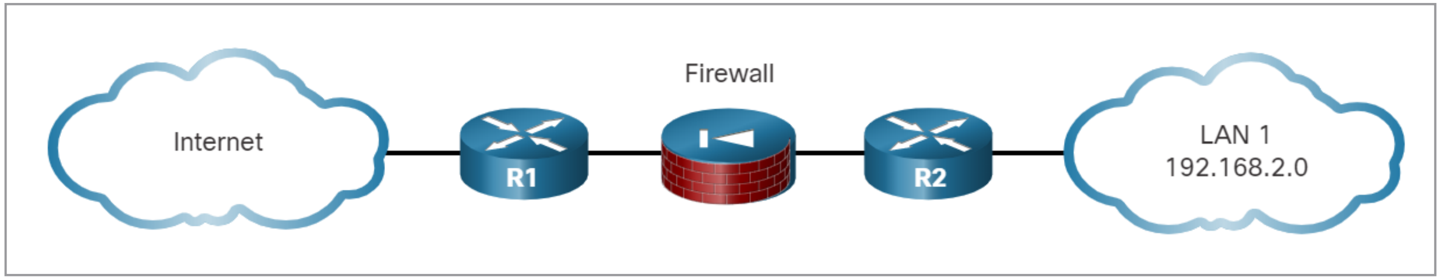
Threat Intelligence Communication Standards (Contd.)

- The Malware Information Sharing Platform (MISP) is an open source platform for sharing IOCs for newly discovered threats.
- MISP is supported by the European Union and is used by over 6,000 organizations globally.
- MISP enables automated sharing of IOCs between people and machines by using STIX and other export formats.
- MISP is open source: https://github.com/MISP and https://www.misp-project.org

Understanding Defense

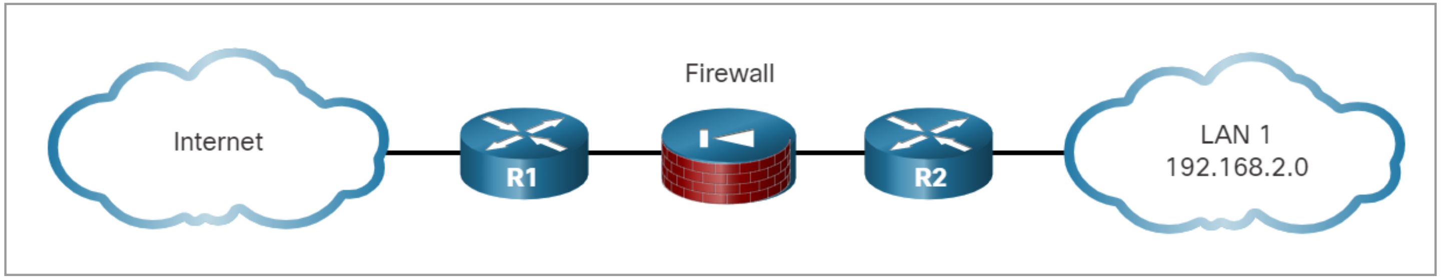
Defense-in-depth

- Organizations must use a defense-in-depth approach to identify threats and secure vulnerable assets.
- This approach uses multiple layers of security at the network edge, within the network, and on network endpoints.
- The figure displays a simple topology of a defense-in-depth approach:



Defense-in-depth (Contd.)

- **Edge router -** The first line of defense is known as an edge router (R1 in the figure). The edge router has a set of rules specifying which traffic it allows or denies. It passes all connections that are intended for the internal LAN to the firewall.
- **Firewall -** A second line of defense is the firewall. The firewall is a checkpoint device that performs additional filtering and tracks the state of the connections. It denies the initiation of connections from the untrusted networks to the trusted network while enabling internal users to establish two-way connections to the untrusted networks.
- **Internal router -** Another line of defense is the internal router (R2 in the figure). It can apply final filtering rules on the traffic before it is forwarded to its destination.



Understanding Defense

Defense-in-depth (Contd.)

- In this approach, a router first screens the traffic before forwarding it to a dedicated firewall appliance, for example, the Cisco ASA.
- Routers and firewalls are not the only devices that are used in a defense-in-depth approach.
- Other security devices include Intrusion Prevention Systems (IPS), advanced malware protection (AMP), web and email content security systems, identity services, network access controls and more.
- In the layered defense-in-depth security approach, the different layers work together to create a security architecture in which the failure of one safeguard does not affect the effectiveness of the other safeguards.

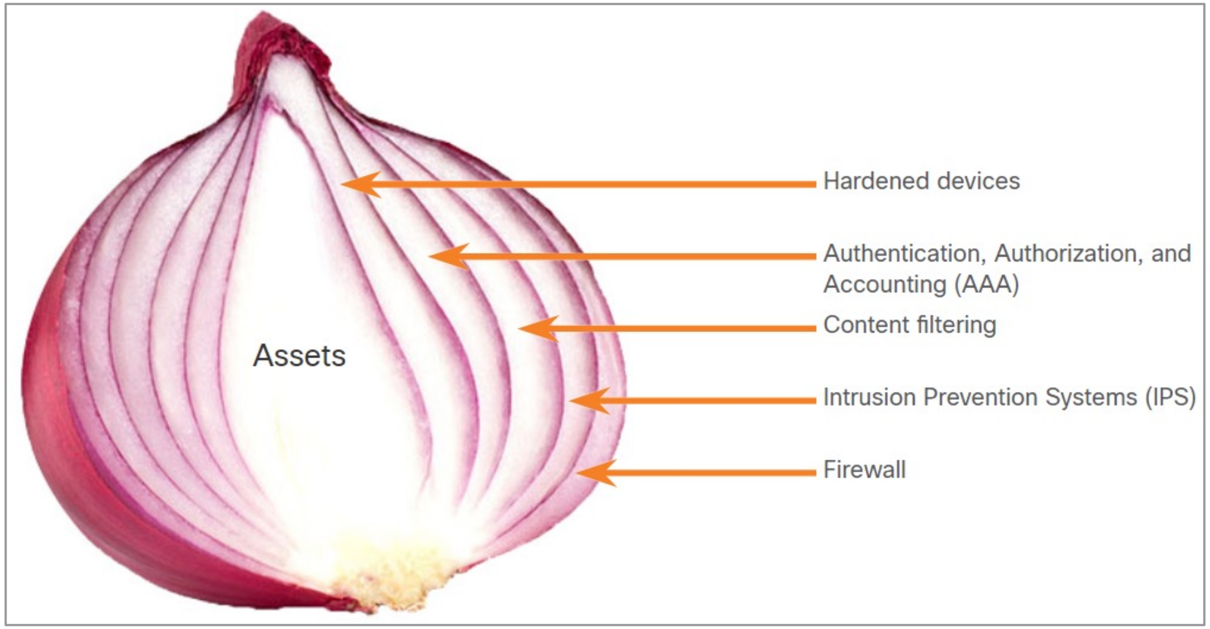
Understanding Defense

The Security Onion and The Security Artichoke

There are two common analogies that are used to describe a defense-in-depth approach.

Security Onion

- A common analogy used to describe a defense-in-depth approach is called "the security onion."
- As illustrated in figure, a threat actor would have to peel away at a network's defenses layer by layer in a manner similar to peeling an onion.
- Only after penetrating each layer would the threat actor reach the target data or system.


Hardened devices
Authentication, Authorization, and Accounting (AAA)
Content filtering
Intrusion Prevention Systems (IPS)
Firewall
Assets

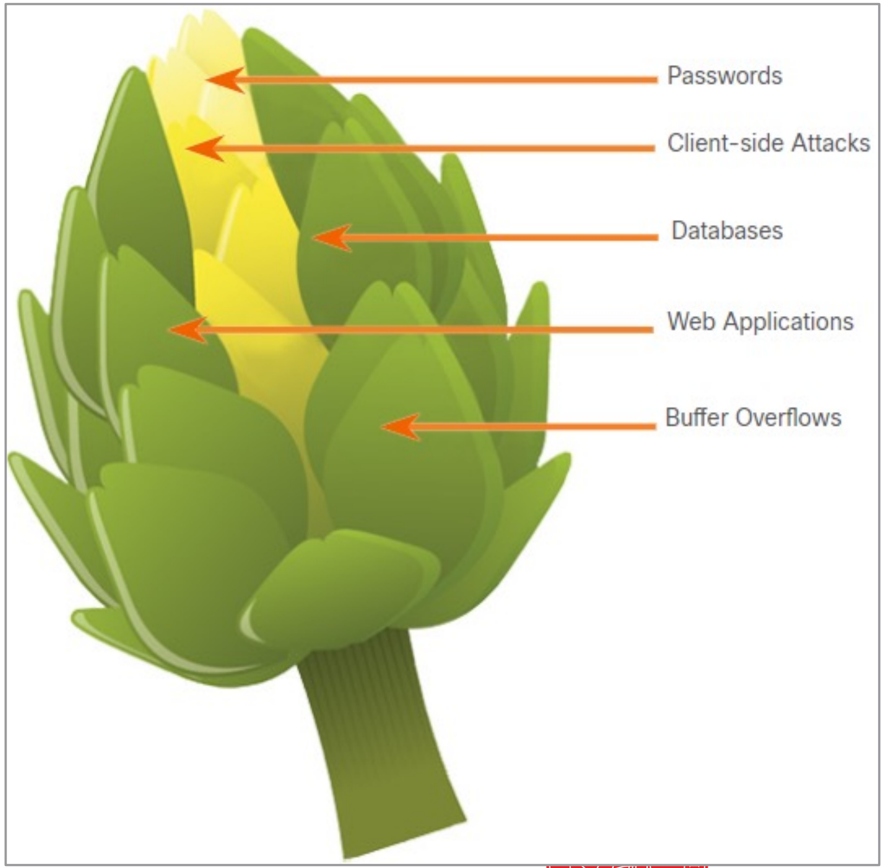
Note: *The security onion described on this page is a way of visualizing defense-in-depth. This is not to be confused with the Security Onion suite of network security tools.*

Understanding Defense

The Security Onion and The Security Artichoke (Contd.)

Security Artichoke

- The evolution of borderless networks has changed the analogy to the "security artichoke", which benefits the threat actor.
- As illustrated in the figure, threat actors no longer have to peel away each layer. They only need to remove certain "artichoke leaves."
- The bonus is that each "leaf" of the network may reveal sensitive data that is not well secured.
- In order to get at the heart of the artichoke, the hacker chips away at the security armor along the perimeter.
- While internet-facing systems are very well protected, persistent hackers do find a gap in that hard-core exterior through which they can enter.



Security Policies, Regulations, and Standards

Security Policies, Regulations, and Standards

Business Policies

- Business policies are the guidelines that are developed by an organization to govern its actions.
- The policies define standards of correct behavior for the business and its employees.
- In networking, policies define the activities that are allowed on the network.
- This sets a baseline of acceptable use. If behavior that violates business policy is detected on the network, it is possible that a security breach has occurred.

Security Policies, Regulations, and Standards

Business Policies (Contd.)

An organization may have several guiding policies, as listed in the table.

Policy	Description
Company policies	• It establishes the rules of conduct and the responsibilities of both employees and employers. • It protect the rights of workers as well as the business interests of employers. • Depending on the needs of the organization, various policies and procedures establish rules regarding employee conduct, attendance, dress code, privacy and other areas related to the terms and conditions of employment.
Employee policies	• These policies are created and maintained by human resources staff to identify employee salary, pay schedule, employee benefits, work schedule, vacations, and more. • They are often provided to new employees to review and sign.
Security policies	• These policies identify a set of security objectives for a company, define the rules of behavior for users and administrators, and specify system requirements. • These objectives, rules, and requirements collectively ensure the security of a network and the computer systems in an organization. • It is a constantly evolving document based on changes in the threat landscape, vulnerabilities, and business and employee requirements.

Security Policies, Regulations, and Standards

Security Policy

- Security policies are used to inform users, staff, and managers of an organization’s requirements for protecting technology and information assets.
- A comprehensive security policy has a number of benefits, including the following:
  - Demonstrates an organization’s commitment to security
  - Sets the rules for expected behavior
  - Ensures consistency in system operations, software and hardware acquisition and use, and maintenance
  - Defines the legal consequences of violations
  - Gives security staff the backing of management
- A security policy also specifies the mechanisms that are needed to meet security requirements and provides a baseline from which to acquire, configure, and audit computer systems and networks for compliance.

Security Policy (Contd.)

The following table lists the policies that may be included in a security policy:

Policy	Description
Identification and authentication policy	It specifies authorized persons that can have access to network resources and identity verification procedures.
Password policies	These ensure passwords meet minimum requirements and are changed regularly.
Acceptable use policy (AUP)	It identifies network applications and uses that are acceptable to the organization. It may also identify ramifications if this policy is violated.
Remote access policy	It identifies how remote users can access a network and what is accessible via remote connectivity.
Network maintenance policy	It specifies network device operating systems and end user application update procedures.
Incident handling procedures	These describe how security incidents are handled.

Example security policy templates provided by SANS: https://www.sans.org/information-security-policy/

Security Policies, Regulations, and Standards

BYOD Policies

- Bring Your Own Device (BYOD) enables employees to use their own mobile devices to access company systems, software, networks, or information.
- It provides key benefits to enterprises, including increased productivity, reduced costs, better mobility for employees, and so on. These benefits also bring an increased security risk as BYOD can lead to data breaches and greater liability for the organization.
- Therefore, a BYOD security policy should be developed to accomplish the following:
  - Specify the goals of the BYOD program
  - Identify which employees can bring their own devices
  - Identify which devices will be supported
  - Identify the level of access employees are granted when using personal devices
  - Describe the rights to access and activities permitted to security personnel on the device
  - Identify which regulations must be adhered to when using employee devices
  - Identify safeguards to put in place if a device is compromised

Security Policies, Regulations, and Standards

BYOD Policies (Contd.)

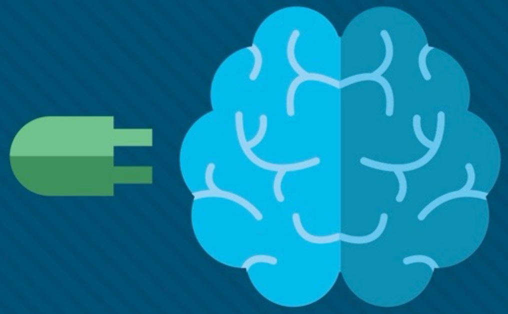
The following table lists the BYOD security best practices to help mitigate BYOD vulnerabilities:

Best Practice	Description
Password protect access	Use unique passwords for each device and account.
Manually control wireless connectivity	Turn off Wi-Fi and Bluetooth connectivity when not in use. Connect only to trusted networks.
Keep updated	Always keep the device OS and other software updated. Updated software often contains security patches to mitigate against the latest threats or exploits.
Back up data	Enable backup of the device in case it is lost or stolen.
Enable "Find my Device"	Subscribe to a device locator service with remote wipe feature.
Provide antivirus software	Provide antivirus software for approved BYOD devices.
Use Mobile Device Management (MDM) software	MDM software enables IT teams to implement security settings and software configurations on all devices that connect to company networks.

Security Policies, Regulations, and Standards

Regulatory and Standards Compliance

- There are also external regulations regarding network security.
- Network security professionals must be familiar with the laws and codes of ethics that are binding on Information Systems Security (INFOSEC) professionals.
- Many organizations are mandated to develop and implement security policies.
- Compliance regulations define what organizations are responsible for providing and the liability if they fail to comply.
- The compliance regulations that an organization is obligated to follow depend on the type of organization and the data that the organization handles.
- Example standard:
  - Payment Card Industry Data Security Standard (PCIDSS)
  - GDPR



Access Control

Access Control Concepts

Access Control

Communications Security: CIA

Information security deals with protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

CIA Triad

The CIA triad consists of three components of information security:

- **Confidentiality -** Only authorized individuals, entities, or processes can access sensitive information.
- **Integrity -** This refers to the protection of data from unauthorized alteration.
- **Availability -** Authorized users must have uninterrupted access to the network resources and data that they require.

Confidentiality
Integrity
Availability

Access Control

Zero Trust Security

- Zero trust is a comprehensive approach to securing all access across networks, applications, and environments.
- This approach helps secure access from users, end-user devices, APIs, IoT, microservices, containers, and more.
- The principle of a zero trust approach is "never trust always verify".
- A zero trust security framework helps to prevent unauthorized access, contain breaches, and reduce the risk of an attacker's lateral movement through a network.
- In a Zero trust approach, any place at which an access control decision is required should be considered a perimeter.

Access Control

Zero Trust Security (Contd.)

The three pillars of zero trust are workforce, workloads, and workplace.

- **Zero Trust for the Workforce -** consists of *people* who access work applications by using their personal or corporate-managed devices. It ensures only the right users and secure devices can access applications, regardless of location.
- **Zero Trust for Workloads -** is concerned with *applications* that are running in the cloud, in data centers, and other virtualized environments that interact with one another. It focuses on secure access when an API, a microservice, or a container is accessing a database within an application.
- **Zero Trust for the Workplace -** focuses on secure access for all *devices*, including on the internet of things (IoT), that connect to internal networks, such as user endpoints, physical and virtual servers, printers, cameras and more.

See e.g. ESG Whitepaper, Strategic Zero Trust, Jan 22
https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/esg-zt-workplace-wp.pdf

Access Control

Access Control Models

- An organization must implement proper access controls to protect its network resources, information system resources, and information.
- A security analyst should understand the different basic access control models to have a better understanding of how attackers can break the access controls.
- The following table lists various types of access control models:

Access Control Models	Description
Discretionary access control (DAC)	• This is the least restrictive model and allows users to control access to their data as owners of that data. • It may use ACLs or other methods to specify which users or groups of users have access to the information.
Mandatory access control (MAC)	• This applies the strictest access control and is used in military or mission critical applications. • It assigns security level labels to information and enables users with access based on their security level clearance.

Access Control Models (Contd.)

Access Control Models	Description
Role-based access control (RBAC)	• Access decisions are based on an individual's roles and responsibilities within the organization. • Different roles are assigned security privileges, and individuals are assigned to the RBAC profile for the role. • Also known as a type of non-discretionary access control.
Attribute-based access control (ABAC)	It allows access based on attributes of the object to be accessed, the subject accessing the resource, and environmental factors regarding how the object is to be accessed.
Rule-based access control (RBAC)	• Network security staff specify sets of rules or conditions that are associated with access to data or systems. • These rules may specify permitted or denied IP addresses, or certain protocols and other conditions. • Also known as Rule Based RBAC.
Time-based access control (TAC)	It allows access to network resources based on time and day.

AAA Usage and Operation

AAA Usage and Operation

AAA Operation

- A network must be designed to control who is allowed to connect to it and what they are allowed to do when they are connected. These design requirements are identified in the network security policy.
- The policy specifies how network administrators, corporate users, remote users, business partners, and clients access network resources.
- The network security policy can also mandate the implementation of an accounting system that tracks who logged in and when and what they did while logged in.
- The Authentication, Authorization, and Accounting (AAA) protocol provides the necessary framework to enable scalable access security.

AAA Usage and Operation

AAA Operation (Contd.)

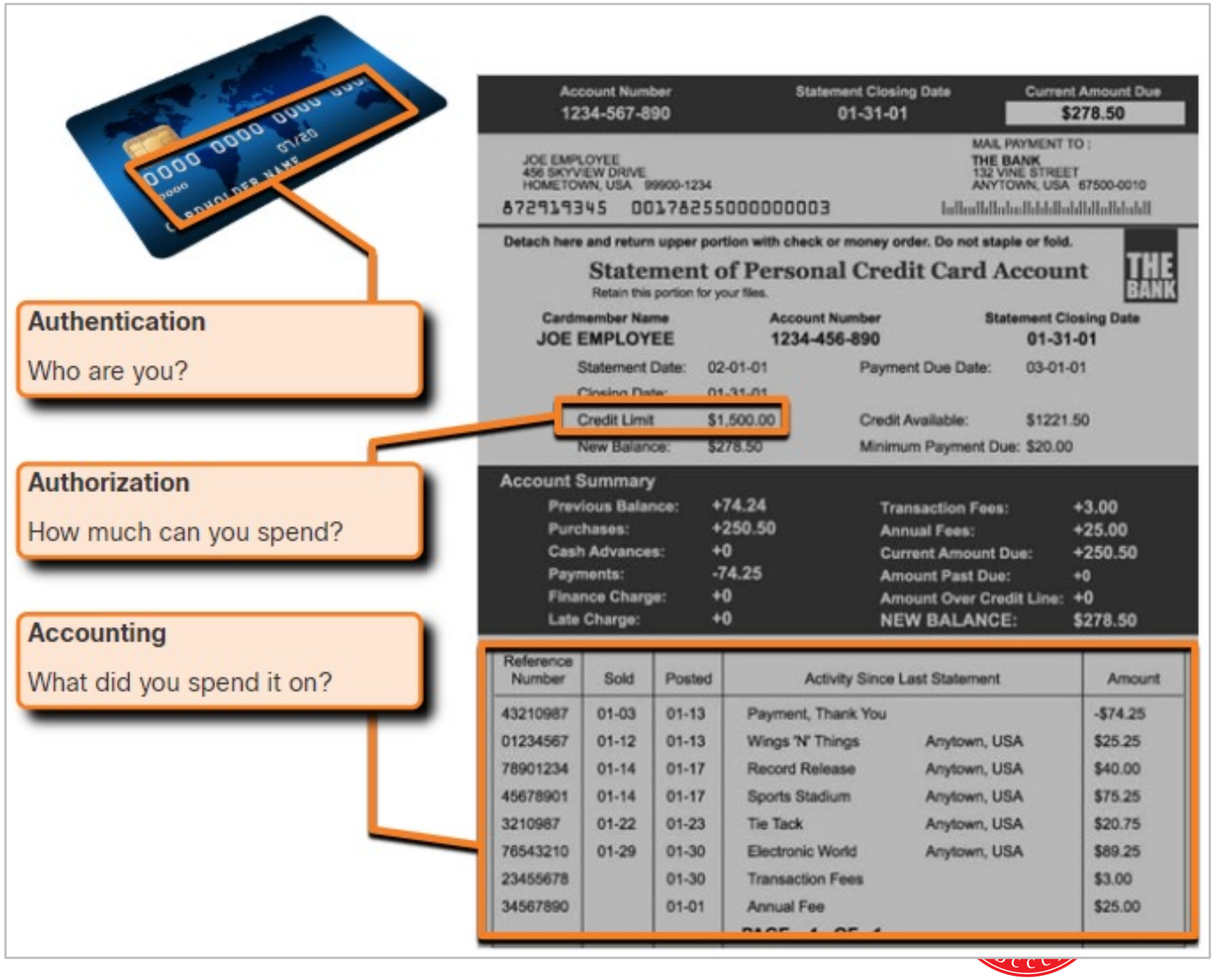
The following table lists the three independent security functions provided by the AAA architectural framework:

AAA Component	Description
Authentication	• Authentication can be established using username and password combinations, challenge and response questions, token cards, and other methods. • AAA authentication provides a centralized way to control access to the network.
Authorization	• After the user is authenticated, authorization services determine which resources the user can access and which operations the user is allowed to perform. • An example is "User can access host server XYZ using SSH only."
Accounting	• Accounting records what the user does, including what is accessed, the amount of time the resource is accessed, and any changes that were made. • Accounting keeps track of how network resources are used. • An example is "User accessed host server XYZ using SSH for 15 minutes."

AAA Usage and Operation

AAA Operation (Contd.)

This concept is similar to the use of a credit card, as indicated by the figure. The credit card identifies who can use it, how much that user can spend, and keeps account of what items the user spent money on.



Authentication

Who are you?

Authorization

How much can you spend?

Accounting

What did you spend it on?

Account Number	Statement Closing Date	Current Amount Due
1234-567-890	01-31-01	$278.50

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA 99900-1234

MAIL PAYMENT TO :
THE BANK
132 VINE STREET
ANYTOWN, USA 67500-0010

872919345 00178255000000003

Detach here and return upper portion with check or money order. Do not staple or fold.

THE BANK

Statement of Personal Credit Card Account

Retain this portion for your files.

Cardmember Name	Account Number	Statement Closing Date
JOE EMPLOYEE	1234-456-890	01-31-01

Statement Date:	02-01-01	Payment Due Date:	03-01-01
Closing Date:	01-31-01		
Credit Limit	$1,500.00	Credit Available:	$1221.50
New Balance:	$278.50	Minimum Payment Due:	$20.00

Account Summary

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	$278.50

Reference Number	Sold	Posted	Activity Since Last Statement		Amount
43210987	01-03	01-13	Payment, Thank You		-$74.25
01234567	01-12	01-13	Wings 'N' Things	Anytown, USA	$25.25
78901234	01-14	01-17	Record Release	Anytown, USA	$40.00
45678901	01-14	01-17	Sports Stadium	Anytown, USA	$75.25
3210987	01-22	01-23	Tie Tack	Anytown, USA	$20.75
76543210	01-29	01-30	Electronic World	Anytown, USA	$89.25
23455678		01-30	Transaction Fees		$3.00
34567890		01-01	Annual Fee		$25.00
			PAGE 1 OF 1		

AAA Usage and Operation

AAA Authentication

- AAA Authentication can be used to authenticate users for administrative access or it can be used to authenticate users for remote network access.
- Cisco provides two common methods for implementing AAA Services:

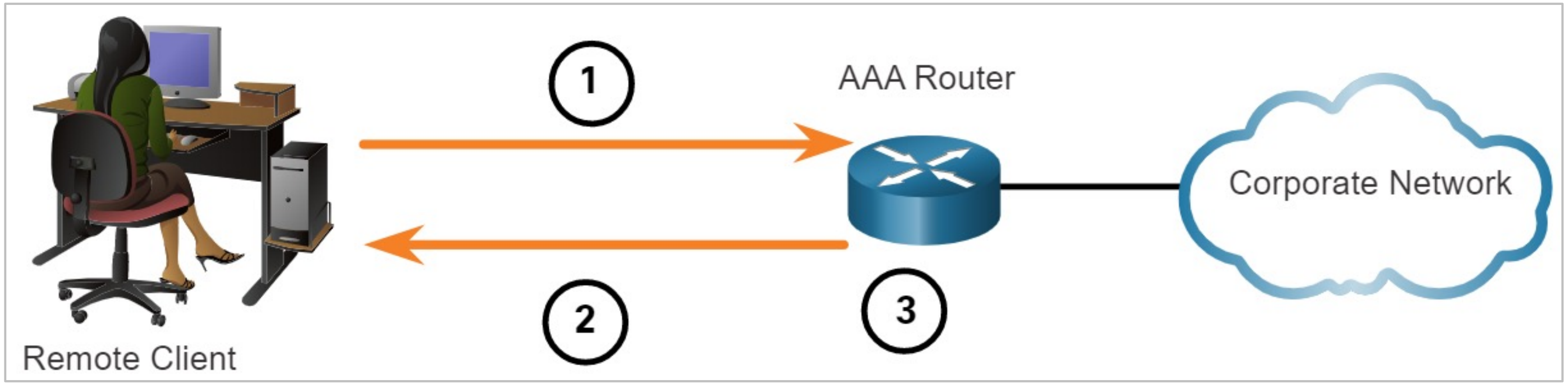
Local AAA Authentication

- This method is known as self-contained authentication because it authenticates users against locally stored usernames and passwords.
- Local AAA is ideal for small networks.

AAA Usage and Operation

AAA Authentication (Contd.)

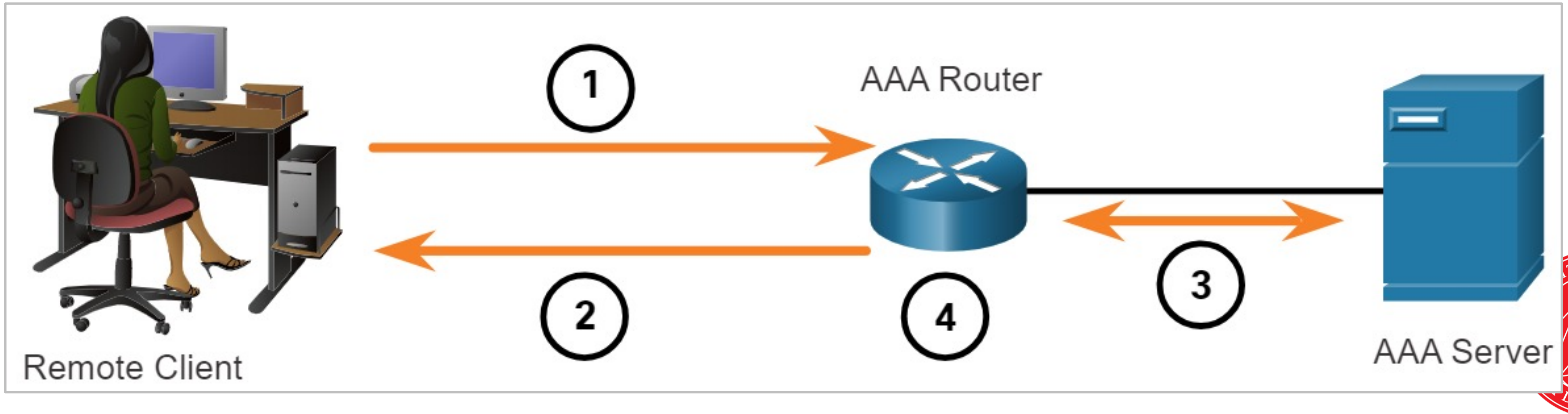
- The client establishes a connection with the router.
- The AAA router prompts the user for a username and password.
- The router authenticated the username and password using the local database and the user is provided access to the network based on information in the local database.



AAA Authentication (Contd.)

Server-based AAA Authentication

- This method authenticates against a central AAA server that contains the usernames and passwords for all users. This is ideal for medium-to-large networks.
- The client establishes a connection with the router.
- The AAA router prompts the user for a username and password.
- The router authenticates the username and password using a AAA server.
- The user is provided access to the network based on information in the remote AAA server.



AAA Usage and Operation

AAA Authentication (Contd.)

Centralized AAA

- Centralized AAA is more scalable and manageable than local AAA authentication, and therefore, it is the preferred AAA implementation.
- A centralized AAA system may independently maintain databases for authentication, authorization, and accounting.
- It can leverage Active Directory or Lightweight Directory Access Protocol (LDAP) for user authentication and group membership, while maintaining its own authorization and accounting databases.
- Devices communicate with the centralized AAA server using either the Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) protocols.

AAA Usage and Operation

AAA Authentication (Contd.)

The following table lists the differences between the two protocols:

Functions	TACACS+	RADIUS
Functionality	It separates authentication, authorization, and accounting functions according to the AAA architecture. This allows modularity of the security server implementation.	It combines authentication and authorization but separates accounting, which allows less flexibility in implementation than TACACS+.
Standard	Mostly Cisco supported	Open/RFC standard
Transport	TCP port 49	UDP ports 1812 and 1813, or 1645 and 1646
Protocol CHAP	Bidirectional challenge and response as used in Challenge Handshake Authentication Protocol (CHAP)	Unidirectional challenge and response from the RADIUS security server to the RADIUS client

AAA Usage and Operation

AAA Authentication (Contd.)

Functions	TACACS+	RADIUS
Confidentiality	Encrypts the entire body of the packet but leaves a standard TACACS+ header.	Encrypts only the password in the access-request packet from the client to the server. The remainder of the packet is unencrypted, leaving the username, authorized services, and accounting unprotected.
Customization	Provides authorization of router commands on a per-user or per-group basis.	Has no option to authorize router commands on a per-user or per-group basis.
Accounting	Limited	Extensive

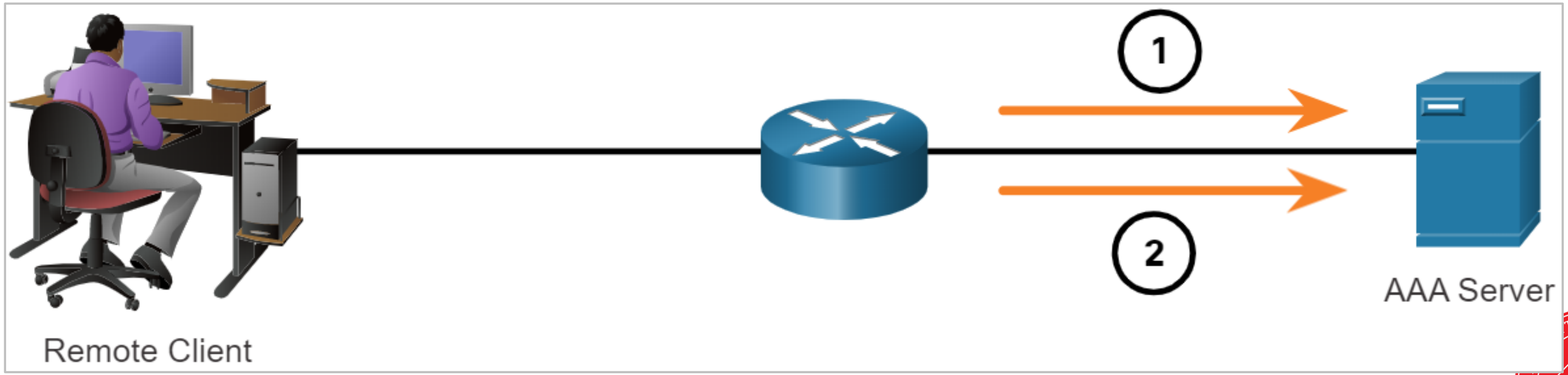
AAA Usage and Operation

AAA Accounting Logs

- Centralized AAA also enables the use of the Accounting method.
- Accounting records from all devices are sent to centralized repositories, which simplifies auditing of user actions.
- AAA Accounting collects and reports usage data in AAA logs. These logs are useful for security auditing.
- The collected data might include the start and stop connection times, executed commands, number of packets, and number of bytes.
- One widely deployed use of accounting is to combine it with AAA authentication. This helps with managing access to internetworking devices by network administrative staff.

AAA Accounting Logs (Contd.)

- Accounting provides more security than just authentication. The AAA servers keep a detailed log of exactly what the authenticated user does on the device.
- This includes all EXEC and configuration commands issued by the user.
- When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
- When the user finishes, a stop message is recorded and the accounting process ends.



AAA Usage and Operation

AAA Accounting Logs (Contd.)

The following table describes the types of accounting information that can be collected:

Types of Accounting Information	Description
Network Accounting	It captures information for all Point-to-Point Protocol (PPP) sessions, including packet and byte counts.
Connection Accounting	It captures information about all outbound connections that are made from the AAA client, such as by SSH.
EXEC Accounting	It captures information about user EXEC terminal sessions on the network access server, including username, date, start and stop times, and the access server IP address.
System Accounting	It captures information about all system-level events.
Command Accounting	It captures information about the EXEC shell commands for a specified privilege level ,as well as the date and time each command was executed, and the user who executed it.
Resource Accounting	It captures 'start' and 'stop' record support for connections that have passed user authentication.

Understanding Defense Summary

What Did I Learn in this Module?

- The starting point for network defense is the identification of assets, vulnerabilities, and threats.
- Assets are anything of value to an organization that must be protected including servers, infrastructure devices, end devices, and the greatest asset, data.
- Vulnerabilities are weaknesses in a system or its design that could be exploited by a threat actor.
- Threats are any potential danger to an asset.
- Organizations must use a defense-in-depth approach to identify threats and secure vulnerable assets.
- Organizations must have a set of policies that define the activities that are allowed on the network.
- Business policies define standards of correct behavior for the business and its employees.

Understanding Defense Summary

What Did I Learn in this Module? (Contd.)

- Security policies are used to inform users, staff, and managers of an organization’s requirements for protecting technology and information assets.
- The purpose of a BYOD (Bring Your Own Device) policy is to enable employees to use their own mobile devices to access company systems, software, networks, or information.
- The compliance regulations that an organization is obligated to follow depend on the type of organization and the data that the organization handles.

Access Control Summary

What Did I Learn in this Module (Contd.)

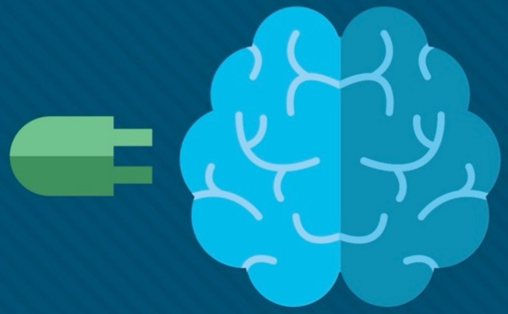
- The CIA triad consists of the primary three components of information security: confidentiality, integrity, and availability.
- Zero trust is a comprehensive approach to securing all access across networks, applications, and environments.
- The principle of zero trust is "never trust, always verify". The pillars of trust are zero trust for workforce, zero trust for workloads, and zero trust for workplace.
- In a zero trust approach, any place at which an access control decision is required should be considered a perimeter.
- Access control methods include discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), attribute-based control (ABAC), rule-based access (RBAC), and time-based access control (TAC).
- A network must be designed to control who is allowed to connect to it and what they are allowed to do when they are connected which is specified in the network security policy.

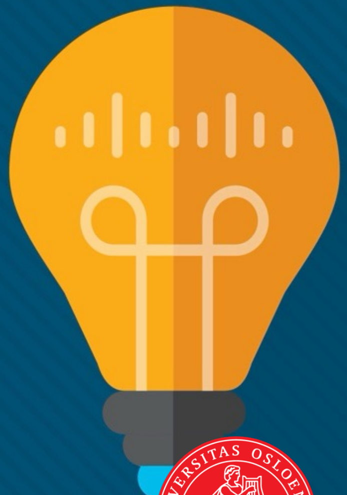
Access Control Summary

What Did I Learn in this Module? (Contd.)

- Authentication, Authorization, and Accounting (AAA) systems provide the necessary framework to enable scalable security.
- Cisco provides two common methods of implementing AAA services: Local AAA Authentication and Server-based AAA Authentication.
- Centralized AAA is more scalable and manageable than local AAA and is the preferred AAA implementation.
- Devices communicate with the centralized AAA server using with the Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control Systems (TACACS+) protocols.
- Centralized AAA also enables the use of the accounting method. AAA accounting collects and reports usage data in AAA logs.
- Various types of accounting information that can be collected are network accounting, connection accounting, EXEC accounting, system accounting, command accounting, and resource accounting.

Security Data





Module Objectives

Module Title: Network Security Data

Module Objective: Explain the types of network security data used in security monitoring.

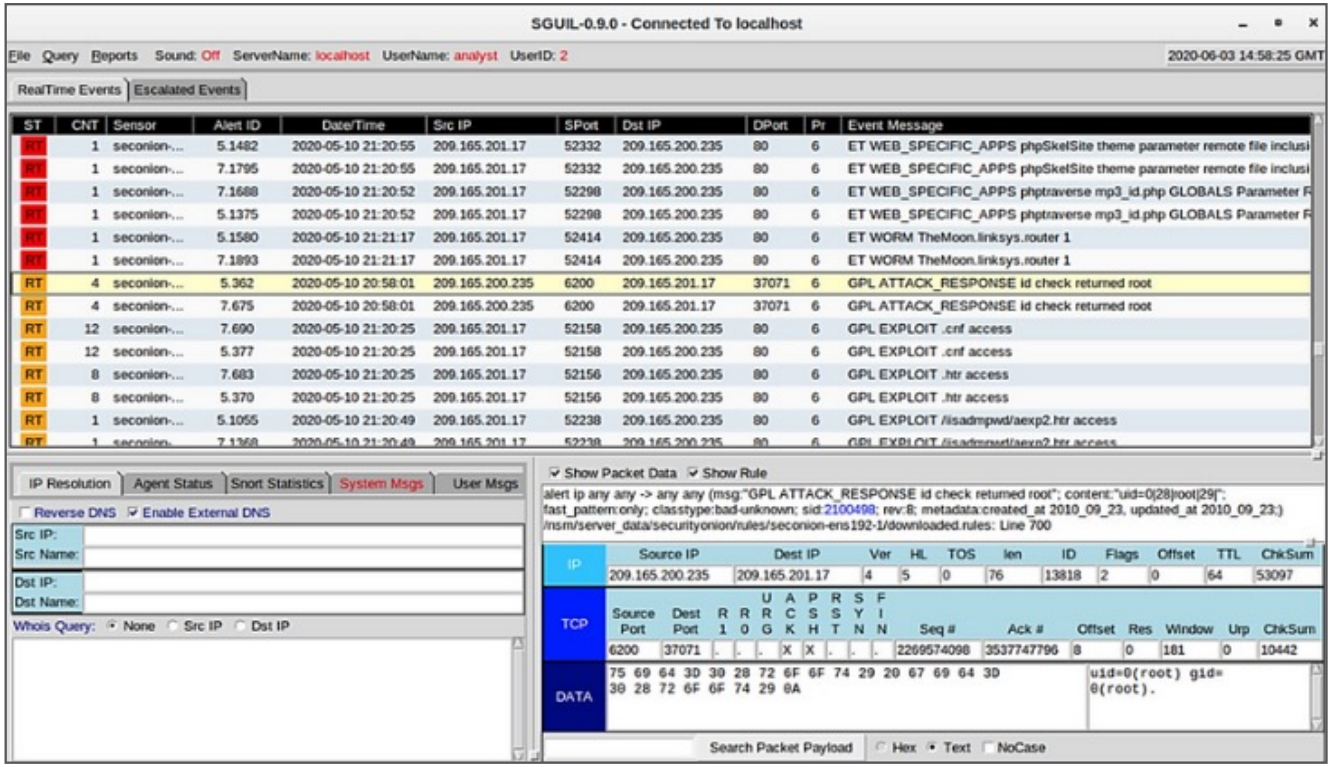
Topic Title	Topic Objective
Types of Security Data	Describe the types of data used in security monitoring.
End Device Logs	Describe the elements of an end device log file.
Network Logs	Describe the elements of a network device log file.

Types of Security Data

Network Security Data

Alert Data

- Alert data consists of messages generated by intrusion prevention systems (IPSs) or intrusion detection systems (IDSs) in response to traffic that violates a rule or matches the signature of a known exploit.
- A network IDS (NIDS), such as Snort, comes configured with rules for known exploits.
- Alerts are generated by Snort and are made readable and searchable by the Sguil and Squert applications, which are part of the Security Onion suite of NSM tools.



SGUIL-0.9.0 - Connected To localhost

Sound: Off ServerName: localhost UserName: analyst UserID: 2 2020-06-03 14:58:25 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion-...	5.1482	2020-05-10 21:20:55	209.165.201.17	52332	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS phpSkelSite theme parameter remote file inclusi
RT	1	seconion-...	7.1795	2020-05-10 21:20:55	209.165.201.17	52332	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS phpSkelSite theme parameter remote file inclusi
RT	1	seconion-...	7.1688	2020-05-10 21:20:52	209.165.201.17	52298	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS phptraverse mp3_id.php GLOBALS Parameter R
RT	1	seconion-...	5.1375	2020-05-10 21:20:52	209.165.201.17	52298	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS phptraverse mp3_id.php GLOBALS Parameter R
RT	1	seconion-...	5.1580	2020-05-10 21:21:17	209.165.201.17	52414	209.165.200.235	80	6	ET WORM TheMoon.linksys.router 1
RT	1	seconion-...	7.1893	2020-05-10 21:21:17	209.165.201.17	52414	209.165.200.235	80	6	ET WORM TheMoon.linksys.router 1
RT	4	seconion-...	5.362	2020-05-10 20:58:01	209.165.200.235	6200	209.165.201.17	37071	6	GPL ATTACK_RESPONSE id check returned root
RT	4	seconion-...	7.675	2020-05-10 20:58:01	209.165.200.235	6200	209.165.201.17	37071	6	GPL ATTACK_RESPONSE id check returned root
RT	12	seconion-...	7.690	2020-05-10 21:20:25	209.165.201.17	52158	209.165.200.235	80	6	GPL EXPLOIT .cnf access
RT	12	seconion-...	5.377	2020-05-10 21:20:25	209.165.201.17	52158	209.165.200.235	80	6	GPL EXPLOIT .cnf access
RT	8	seconion-...	7.683	2020-05-10 21:20:25	209.165.201.17	52156	209.165.200.235	80	6	GPL EXPLOIT .htr access
RT	8	seconion-...	5.370	2020-05-10 21:20:25	209.165.201.17	52156	209.165.200.235	80	6	GPL EXPLOIT .htr access
RT	1	seconion-...	5.1055	2020-05-10 21:20:49	209.165.201.17	52238	209.165.200.235	80	6	GPL EXPLOIT /isadmpwd/aexp2.htr access
RT	1	seconion-...	7.1368	2020-05-10 21:20:49	209.165.201.17	52238	209.165.200.235	80	6	GPL EXPLOIT /isadmpwd/aexp2.htr access

IP Resolution | Agent Status | Snort Statistics | System Msgs | User Msgs

□ Reverse DNS ☑ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0|28|root|29|";
fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8; metadata:created_at 2010_09_23, updated_at 2010_09_23;)
/nsm/server_data/securityonion/rules/seconion-ens192-1/downloaded.rules: Line 700
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	209.165.200.235	209.165.201.17	4	5	0	76	13818	2	0	64	53097

TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	6200	37071	.	.	.	X	X	.	.	.	2269574098	3537747796	8	0	181	0	10442

DATA

```
75 69 64 3D 30 28 72 6F 6F 74 29 20 67 69 64 3D     uid=0(root) gid=
30 28 72 6F 6F 74 29 0A                              0(root).
```

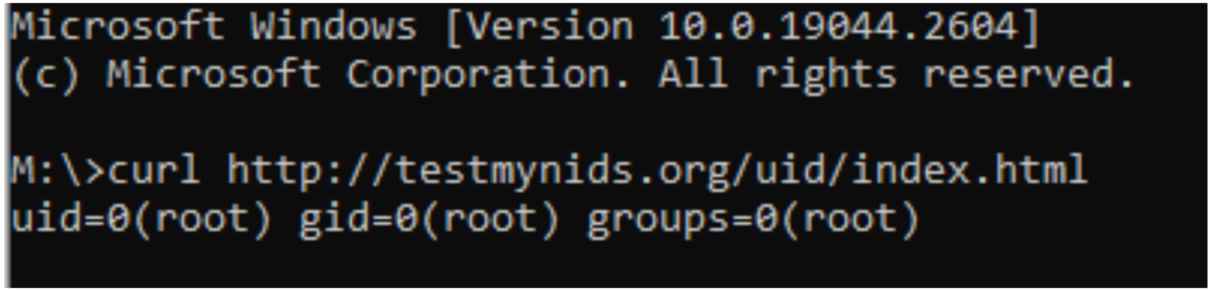
Search Packet Payload ○ Hex ● Text □ NoCase

Sguil Console Showing Test Alert from Snort IDS

Network Security Data
Snort Rule Alerting

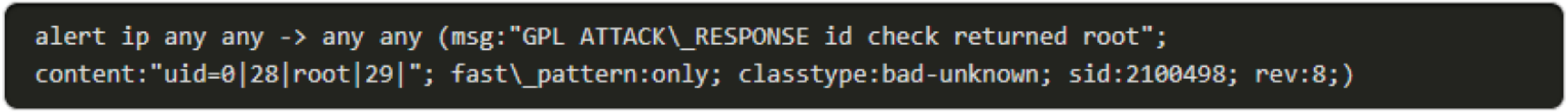
uid=0(root) gid=0(root) groups=0(root)

Signature generated by testmyids - https://testmyids.com



```
Microsoft Windows [Version 10.0.19044.2604]
(c) Microsoft Corporation. All rights reserved.

M:\>curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
```

Signature response returned from HTTP curl request to testmyids website



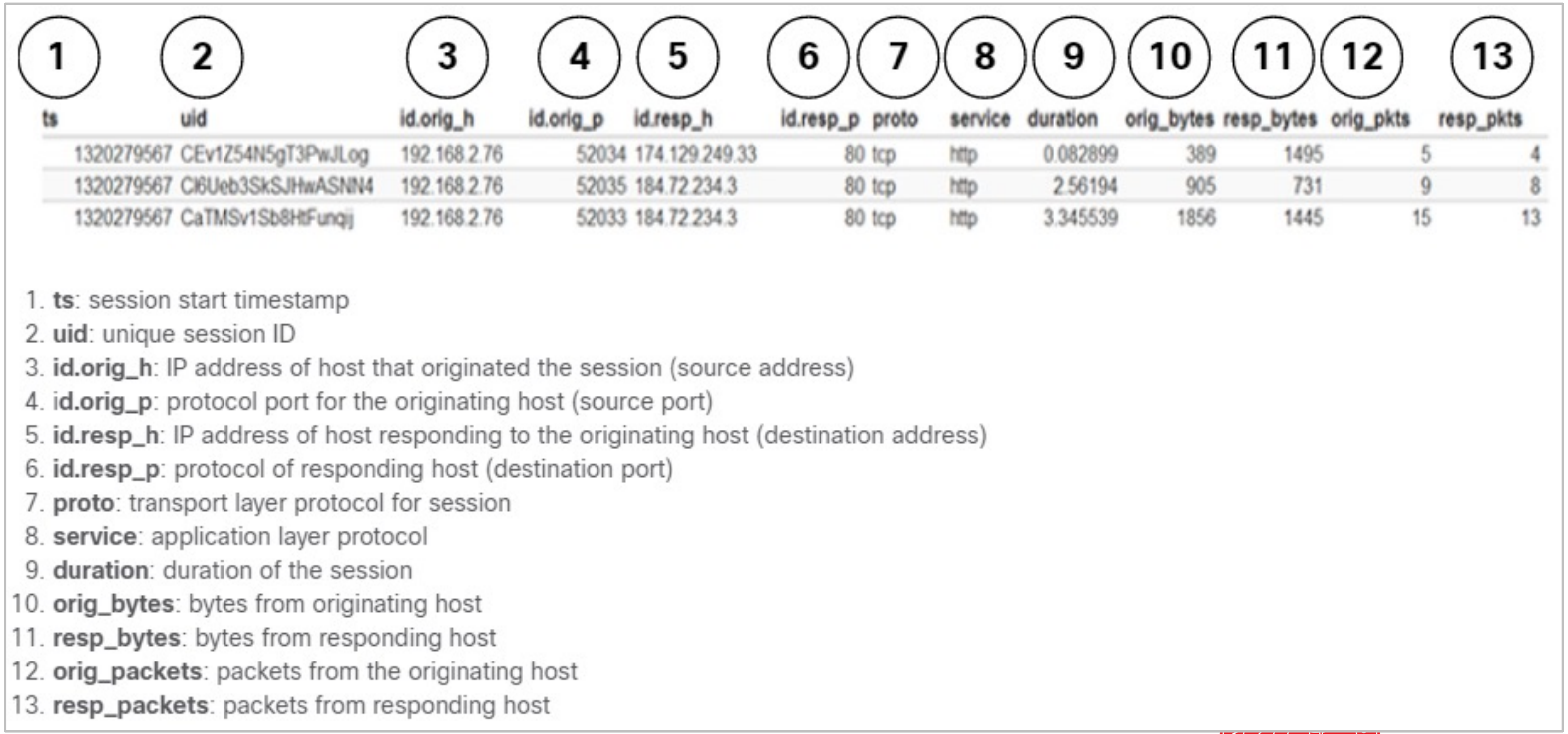
```
alert ip any any -> any any (msg:"GPL ATTACK\_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast\_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;)
```

Example Snort Rule for generating an alert based on testmyids signature in message content

Network Security Data

Session and Transaction Data

- Session data is a record of a conversation between two network endpoints.
- It includes **the five tuples** of source and destination IP addresses, source and destination port numbers, and the IP code for the protocol in use.
- Data about the session includes a session ID, the amount of data transferred by source and destination and information related to the duration of the session.
- The figure shows a partial output for three HTTP sessions from a Zeek connection log.



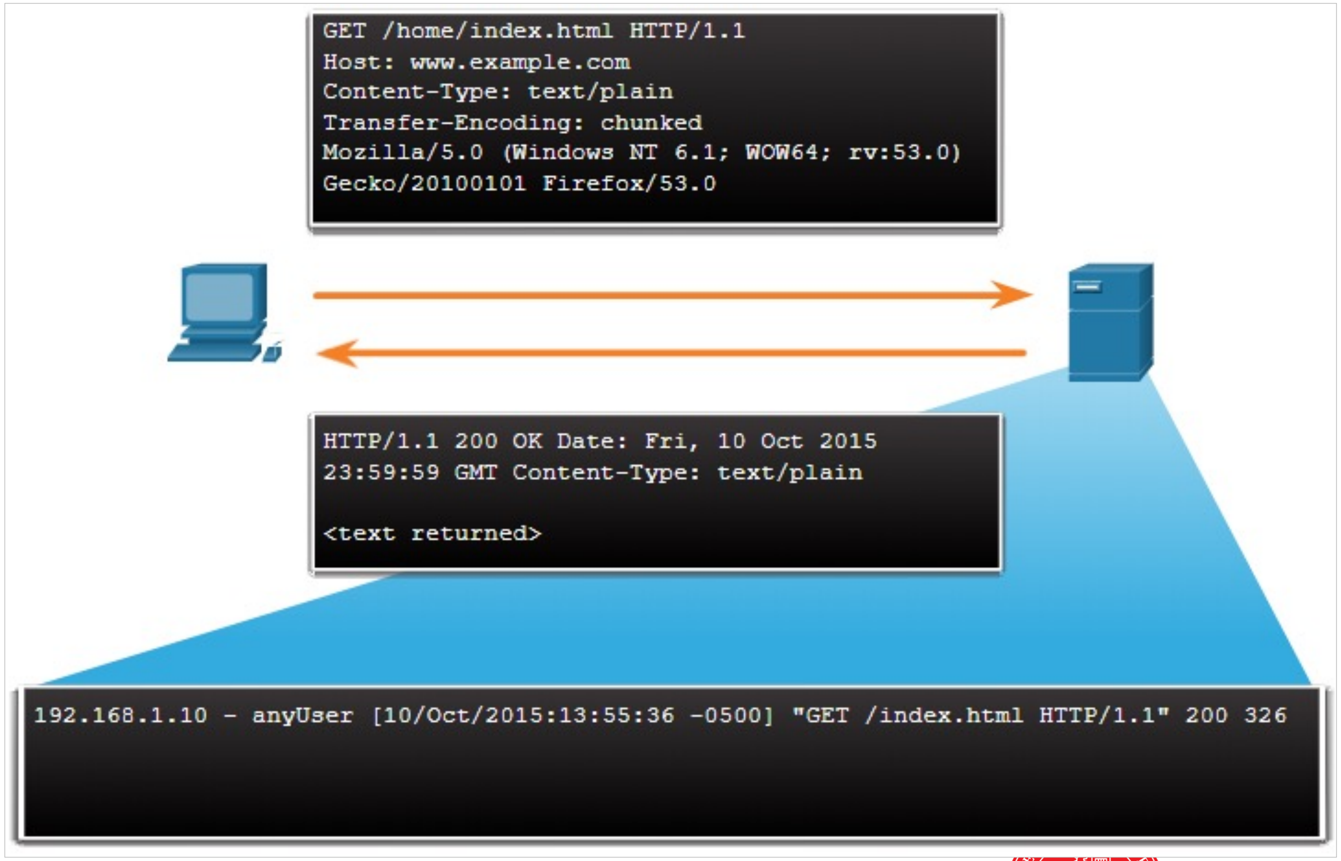
1	2	3	4	5	6	7	8	9	10	11	12	13
ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service	duration	orig_bytes	resp_bytes	orig_pkts	resp_pkts
1320279567	CEv1Z54N5gT3PwJLog	192.168.2.76	52034	174.129.249.33	80	tcp	http	0.082899	389	1495	5	4
1320279567	Cl6Ueb3SkSJHwASNN4	192.168.2.76	52035	184.72.234.3	80	tcp	http	2.56194	905	731	9	8
1320279567	CaTMSv1Sb8HtFunqij	192.168.2.76	52033	184.72.234.3	80	tcp	http	3.345539	1856	1445	15	13

1. **ts**: session start timestamp
2. **uid**: unique session ID
3. **id.orig_h**: IP address of host that originated the session (source address)
4. **id.orig_p**: protocol port for the originating host (source port)
5. **id.resp_h**: IP address of host responding to the originating host (destination address)
6. **id.resp_p**: protocol of responding host (destination port)
7. **proto**: transport layer protocol for session
8. **service**: application layer protocol
9. **duration**: duration of the session
10. **orig_bytes**: bytes from originating host
11. **resp_bytes**: bytes from responding host
12. **orig_packets**: packets from the originating host
13. **resp_packets**: packets from responding host

Network Security Data

Session and Transaction Data (Contd.)

- Transaction data consists of the messages that are exchanged during network sessions.
- These transactions can be viewed in packet capture transcripts.
- The transactions that represent the requests and replies would be logged in an access log on a server or by a NIDS like Zeek.
- A session might include the downloading of content from a webserver, as shown in the figure.



```
GET /home/index.html HTTP/1.1
Host: www.example.com
Content-Type: text/plain
Transfer-Encoding: chunked
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:53.0)
Gecko/20100101 Firefox/53.0
```

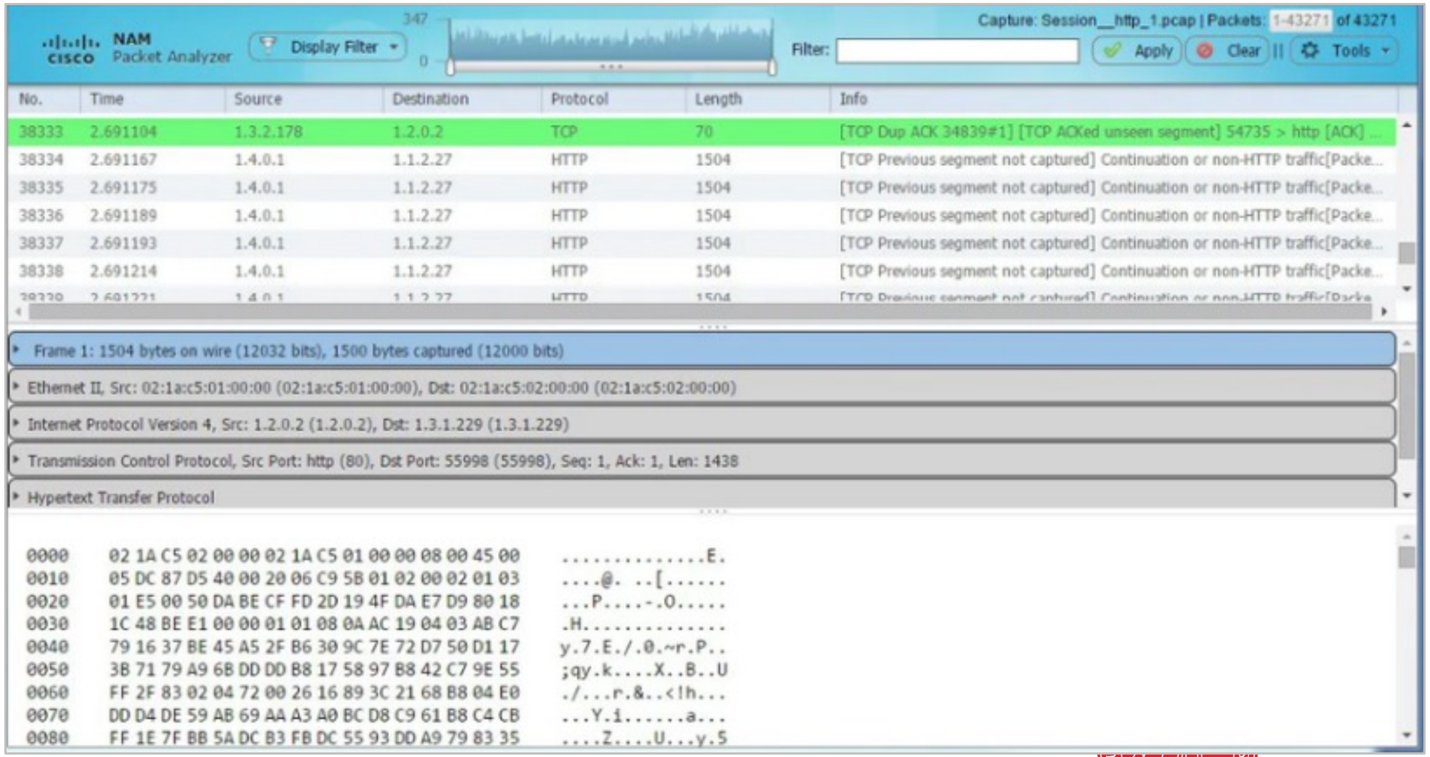
```
HTTP/1.1 200 OK Date: Fri, 10 Oct 2015
23:59:59 GMT Content-Type: text/plain

<text returned>
```

```
192.168.1.10 - anyUser [10/Oct/2015:13:55:36 -0500] "GET /index.html HTTP/1.1" 200 326
```

Network Security Data

Full Packet Captures

- Full packet captures are the most detailed network data that is generally collected.
- It contains the actual content of the conversations such as text of email messages, the HTML in web pages, and the files that enter or leave the network.
- Extracted content can be recovered from full packet captures and analyzed for malware or user behavior that violates business and security policies.
- We can use Wireshark for analysis. The figure here shows the interface for the Network Analysis Monitor component of Cisco Prime Infrastructure system, an alternative application to Wireshark.



Capture: Session__http_1.pcap | Packets: 1-43271 of 43271

No.	Time	Source	Destination	Protocol	Length	Info
38333	2.691104	1.3.2.178	1.2.0.2	TCP	70	[TCP Dup ACK 34839#1] [TCP ACKed unseen segment] 54735 > http [ACK] ...
38334	2.691167	1.4.0.1	1.1.2.27	HTTP	1504	[TCP Previous segment not captured] Continuation or non-HTTP traffic[Packe...
38335	2.691175	1.4.0.1	1.1.2.27	HTTP	1504	[TCP Previous segment not captured] Continuation or non-HTTP traffic[Packe...
38336	2.691189	1.4.0.1	1.1.2.27	HTTP	1504	[TCP Previous segment not captured] Continuation or non-HTTP traffic[Packe...
38337	2.691193	1.4.0.1	1.1.2.27	HTTP	1504	[TCP Previous segment not captured] Continuation or non-HTTP traffic[Packe...
38338	2.691214	1.4.0.1	1.1.2.27	HTTP	1504	[TCP Previous segment not captured] Continuation or non-HTTP traffic[Packe...
38339	2.691221	1.4.0.1	1.1.2.27	HTTP	1504	[TCP Previous segment not captured] Continuation or non-HTTP traffic[Packe

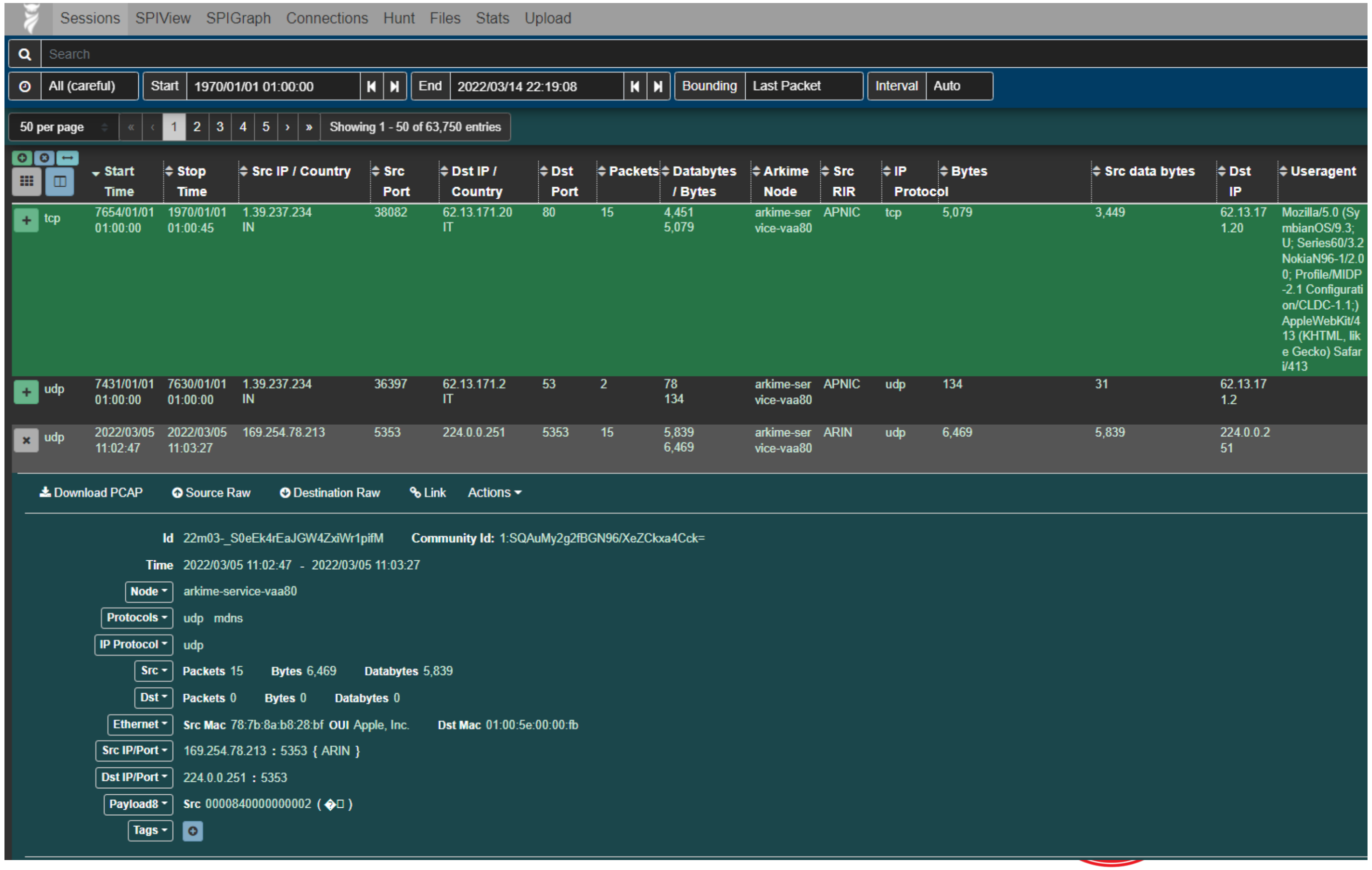
```
▸ Frame 1: 1504 bytes on wire (12032 bits), 1500 bytes captured (12000 bits)
▸ Ethernet II, Src: 02:1a:c5:01:00:00 (02:1a:c5:01:00:00), Dst: 02:1a:c5:02:00:00 (02:1a:c5:02:00:00)
▸ Internet Protocol Version 4, Src: 1.2.0.2 (1.2.0.2), Dst: 1.3.1.229 (1.3.1.229)
▸ Transmission Control Protocol, Src Port: http (80), Dst Port: 55998 (55998), Seq: 1, Ack: 1, Len: 1438
▸ Hypertext Transfer Protocol
```

```
0000    02 1A C5 02 00 00 02 1A C5 01 00 00 08 00 45 00    ..............E.
0010    05 DC 87 D5 40 00 20 06 C9 5B 01 02 00 02 01 03    ....@. ..[......
0020    01 E5 00 50 DA BE CF FD 2D 19 4F DA E7 D9 80 18    ...P....-.O.....
0030    1C 48 BE E1 00 00 01 01 08 0A AC 19 04 03 AB C7    .H..............
0040    79 16 37 BE 45 A5 2F B6 30 9C 7E 72 D7 50 D1 17    y.7.E./.0.~r.P..
0050    3B 71 79 A9 6B DD DD B8 17 58 97 B8 42 C7 9E 55    ;qy.k....X..B..U
0060    FF 2F 83 02 04 72 00 26 16 89 3C 21 68 B8 04 E0    ./...r.&..<!h...
0070    DD D4 DE 59 AB 69 AA A3 A0 BC D8 C9 61 B8 C4 CB    ...Y.i......a...
0080    FF 1E 7F BB 5A DC B3 FB DC 55 93 DD A9 79 83 35    ....Z....U...y.5
```

Network Security Data

Full Packet Captures (Contd.)

- Arkime is a scalable, open source, indexed packet capture and search tool
- Allows historic searching of PCAPs across multiple devices
- Stores data in PCAP format
- Can be integrated with SIEM
- View unique session values
- Visualisation tools
- Network connection graphs
- https://arkime.com/demo



Start 1970/01/01 01:00:00 End 2022/03/14 22:19:08

Showing 1 - 50 of 63,750 entries

	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Arkime Node	Src RIR	IP Protocol	Bytes	Src data bytes	Dst IP	Useragent
+ tcp	7654/01/01 01:00:00	1970/01/01 01:00:45	1.39.237.234 IN	38082	62.13.171.20 IT	80	15	4,451 5,079	arkime-service-vaa80	APNIC	tcp	5,079	3,449	62.13.171.20	Mozilla/5.0 (SymbianOS/9.3; U; Series60/3.2 NokiaN96-1/2.00; Profile/MIDP-2.1 Configuration/CLDC-1.1;) AppleWebKit/413 (KHTML, like Gecko) Safari/413
+ udp	7431/01/01 01:00:00	7630/01/01 01:00:00	1.39.237.234 IN	36397	62.13.171.2 IT	53	2	78 134	arkime-service-vaa80	APNIC	udp	134	31	62.13.171.2	
× udp	2022/03/05 11:02:47	2022/03/05 11:03:27	169.254.78.213	5353	224.0.0.251	5353	15	5,839 6,469	arkime-service-vaa80	ARIN	udp	6,469	5,839	224.0.0.251	

Id 22m03-_S0eEk4rEaJGW4ZxiWr1pifM **Community Id:** 1:SQAuMy2g2fBGN96/XeZCkxa4Cck=

Time 2022/03/05 11:02:47 - 2022/03/05 11:03:27

Node arkime-service-vaa80

Protocols udp mdns

IP Protocol udp

Src **Packets** 15 **Bytes** 6,469 **Databytes** 5,839

Dst **Packets** 0 **Bytes** 0 **Databytes** 0

Ethernet **Src Mac** 78:7b:8a:b8:28:bf **OUI** Apple, Inc. **Dst Mac** 01:00:5e:00:00:fb

Src IP/Port 169.254.78.213 : 5353 { ARIN }

Dst IP/Port 224.0.0.251 : 5353

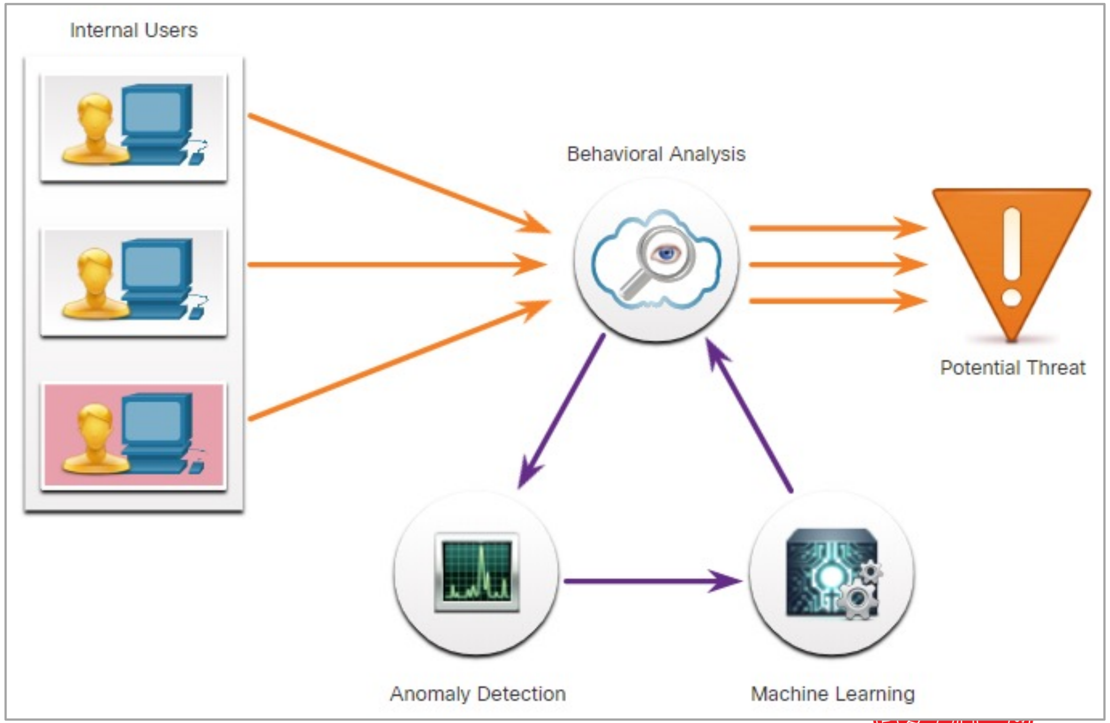
Payload8 **Src** 0000840000000002 (�□)

Tags

Network Security Data

Statistical Data

- Statistical data is about network traffic which is created through the analysis of other forms of network data.
- Statistics can be used to characterize normal amounts of variation in network traffic patterns in order to identify network conditions that are significantly outside of those ranges.
- An example of an NSM tool that utilizes statistical analysis is Cisco Cognitive Threat Analytics.
- It is able to find malicious activity that has bypassed security controls or entered the network through unmonitored channels (including removable media) and is operating inside an organization’s environment.
- The figure shows an architecture for Cisco Cognitive Threat Analytics.



End Device Logs

End Device Logs

Host Logs

- Host-based intrusion detection systems (HIDS) run on individual hosts.
- Many host-based protections submit logs to a centralized log management servers which can be searched from a central location using NSM tools.
- Microsoft Windows host logs are visible locally through Event Viewer. Event Viewer keeps four types of logs:
    - **Application logs** – These contain events logged by various applications.
    - **System logs** – These include events regarding the operation of drivers, processes, and hardware.
    - **Setup logs** – These record information about the installation of software, including Windows updates.
    - **Security logs** – These record events related to security, such as logon attempts and operations related to file or object management and access.
    - **Command-line logs** – Attackers who have gained access to a system, and some types of malware, execute commands from the command-line interface (CLI) rather than a GUI. Logging command line execution will provide visibility into this type of incident.

End Device Logs

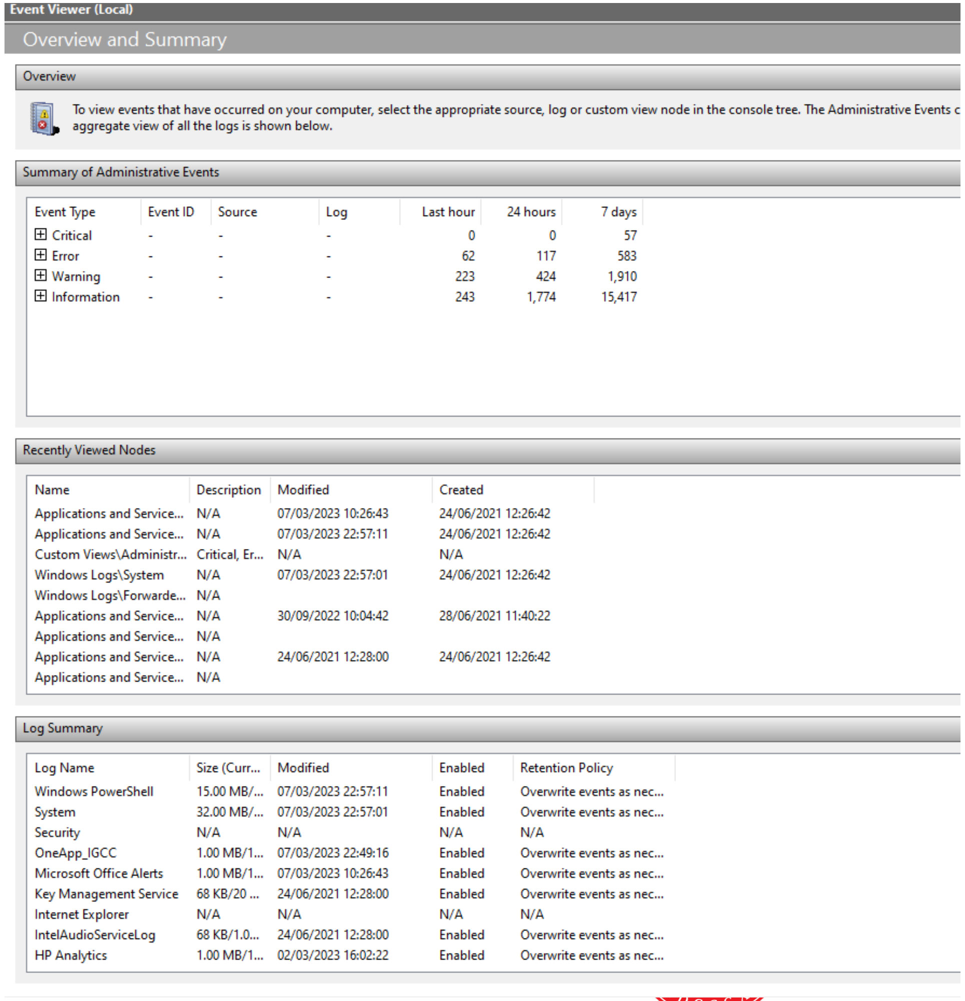
Host Logs (Contd.)

The table explains the meaning of the five Windows host log event types.

Event Type	Description
Error	It is an event that indicates a significant problem such as loss of data or functionality. For example, if a service fails to load during startup, an error event is logged.
Warning	It is an event that is not necessarily significant but may indicate a possible future problem. For example, when disk space is low, a warning event is logged. If an application recovers from an event without loss of functionality or data, it can classify the event as a warning event.
Information	It describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, it may be appropriate to log an information event. Note that it is generally inappropriate for a desktop application to log an event each time it starts.
Success Audit	It is an event that records an audited security access attempt that is successful. For example, a user’s successful attempt to log on to the system is a success audit event.
Failure Audit	It is an event that records an audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt is logged as a failure audit event.

Host Logs – Windows Event Viewer

- Can be launched in the Windows Operating System to view logged events in a graphical user interface
- Provides ability to define custom views for a variety of purposes
- Event data can be exported in a variety of file formats including .evtx, Xml, CSV, and text delimited data
- Can store application specific logs from software installed on the device



Event Viewer (Local)

Overview and Summary

Overview

To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events c aggregate view of all the logs is shown below.

Summary of Administrative Events

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
⊞ Critical	-	-	-	0	0	57
⊞ Error	-	-	-	62	117	583
⊞ Warning	-	-	-	223	424	1,910
⊞ Information	-	-	-	243	1,774	15,417

Recently Viewed Nodes

Name	Description	Modified	Created
Applications and Service...	N/A	07/03/2023 10:26:43	24/06/2021 12:26:42
Applications and Service...	N/A	07/03/2023 22:57:11	24/06/2021 12:26:42
Custom Views\Administr...	Critical, Er...	N/A	N/A
Windows Logs\System	N/A	07/03/2023 22:57:01	24/06/2021 12:26:42
Windows Logs\Forwarde...	N/A		
Applications and Service...	N/A	30/09/2022 10:04:42	28/06/2021 11:40:22
Applications and Service...	N/A		
Applications and Service...	N/A	24/06/2021 12:28:00	24/06/2021 12:26:42
Applications and Service...	N/A		

Log Summary

Log Name	Size (Curr...	Modified	Enabled	Retention Policy
Windows PowerShell	15.00 MB/...	07/03/2023 22:57:11	Enabled	Overwrite events as nec...
System	32.00 MB/...	07/03/2023 22:57:01	Enabled	Overwrite events as nec...
Security	N/A	N/A	N/A	N/A
OneApp_IGCC	1.00 MB/1...	07/03/2023 22:49:16	Enabled	Overwrite events as nec...
Microsoft Office Alerts	1.00 MB/1...	07/03/2023 10:26:43	Enabled	Overwrite events as nec...
Key Management Service	68 KB/20 ...	24/06/2021 12:28:00	Enabled	Overwrite events as nec...
Internet Explorer	N/A	N/A	N/A	N/A
IntelAudioServiceLog	68 KB/1.0...	24/06/2021 12:28:00	Enabled	Overwrite events as nec...
HP Analytics	1.00 MB/1...	02/03/2023 16:02:22	Enabled	Overwrite events as nec...

End Device Logs

Host Logs (Contd.)

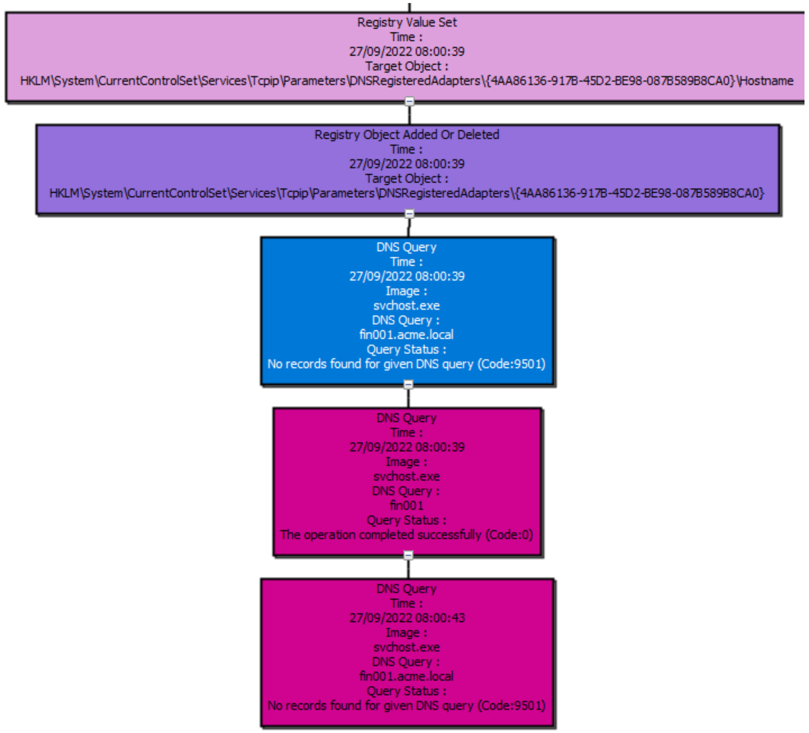
- External information sources can provide extensive detailing of Windows host logs:
  - Windows Security Log Encyclopedia (ultimatewindowssecurity.com)

SYSMON

- System Monitor (Sysmon) can be deployed on Windows and Linux systems to monitor and log system activity
- Sysmon logs the process creation, parent and child process creation and many other elements
- Records hashes of process image files
- Utilises a session GUID to correlate different events together
- Can log network connections such as DNS, IP addresses, the source process spawning a network connection
- Rule driven filtering for capturing these events.
- Popular Sysmon rule configurations include Sysmon Modular:
  - https://github.com/olafhartong/sysmon-modular

End Device Logs

Host Logs (Contd.)



Registry Value Set
Time :
27/09/2022 08:00:39
Target Object :
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DNSRegisteredAdapters\{4AA86136-917B-45D2-BE98-087B589B8CA0}\Hostname

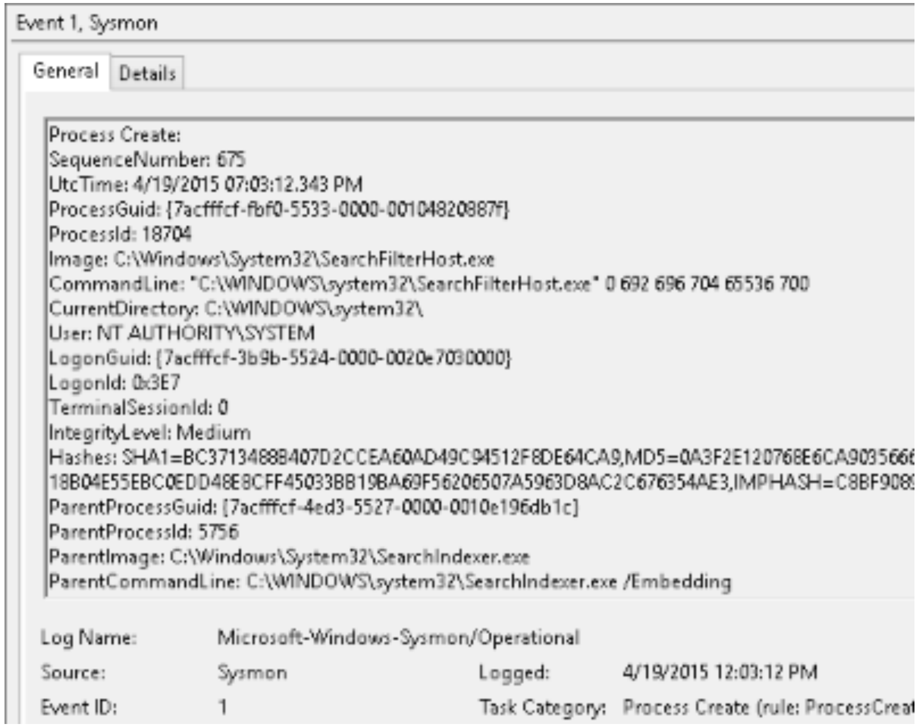
Registry Object Added Or Deleted
Time :
27/09/2022 08:00:39
Target Object :
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DNSRegisteredAdapters\{4AA86136-917B-45D2-BE98-087B589B8CA0}

DNS Query
Time :
27/09/2022 08:00:39
Image :
svchost.exe
DNS Query :
fin001.acme.local
Query Status :
No records found for given DNS query (Code:9501)

DNS Query
Time :
27/09/2022 08:00:39
Image :
svchost.exe
DNS Query :
fin001
Query Status :
The operation completed successfully (Code:0)

DNS Query
Time :
27/09/2022 08:00:43
Image :
svchost.exe
DNS Query :
fin001.acme.local
Query Status :
No records found for given DNS query (Code:9501)

Process chain and correlation of events captured by Sysmon viewed in the Sysmonview application



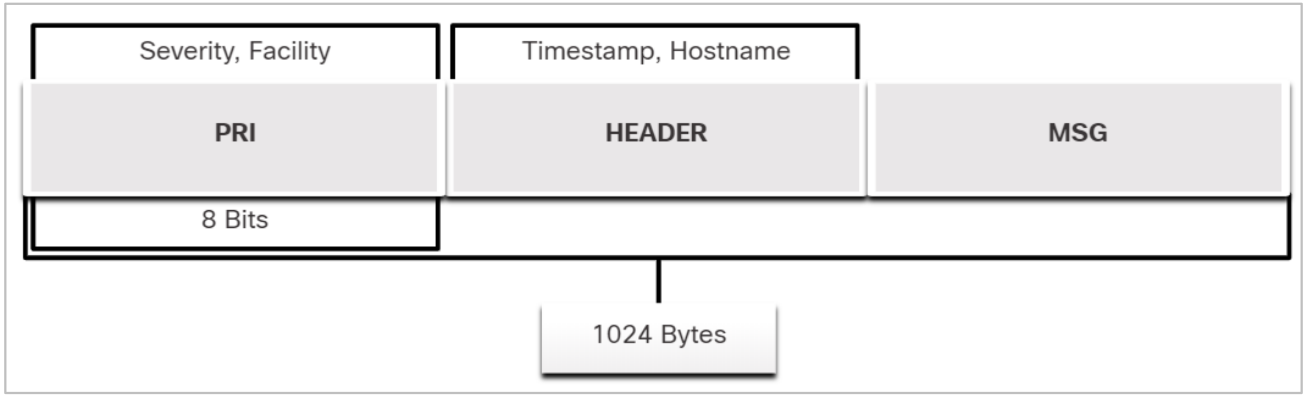
```
Process Create:
SequenceNumber: 675
UtcTime: 4/19/2015 07:03:12.343 PM
ProcessGuid: {7acfffcf-fbf0-5533-0000-00104820887f}
ProcessId: 18704
Image: C:\Windows\System32\SearchFilterHost.exe
CommandLine: "C:\WINDOWS\system32\SearchFilterHost.exe" 0 692 696 704 65536 700
CurrentDirectory: C:\WINDOWS\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {7acfffcf-3b9b-5524-0000-0020e7030000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: Medium
Hashes: SHA1=BC3713488407D2CCEA60AD49C94512F8DE64CA9,MD5=0A3F2E120768E6CA903566
18B04E55EBC0EDD48E8CFF45033BB19BA69F56206507A5963D8AC2C676354AE3,IMPHASH=C8BF908
ParentProcessGuid: {7acfffcf-4ed3-5527-0000-0010e196db1c}
ParentProcessId: 5756
ParentImage: C:\Windows\System32\SearchIndexer.exe
ParentCommandLine: C:\WINDOWS\system32\SearchIndexer.exe /Embedding

Log Name:        Microsoft-Windows-Sysmon/Operational
Source:          Sysmon                     Logged:          4/19/2015 12:03:12 PM
Event ID:        1                          Task Category:   Process Create (rule: ProcessCreat
```

Detailed process information including command line and hashes

End Device Logs

Syslog

- Syslog incudes specifications for message formats, a client-server application structure, and network protocol. It is a client/server protocol.
- Many different types of network devices can be configured to use the syslog standard to log events to centralized syslog servers.
- The full format of a Syslog message has three distinct parts: PRI (priority), HEADER, MSG (message text).
  - The PRI consists of two elements, the Facility and Severity of the message, which are both integer values.
  - The Facility consists of sources that generated the message, such as the system, process, or application.
  - The Severity is a value from 0-7 that defines the severity of the message.



End Device Logs

Syslog (Contd.)

Facility

- Facility codes between 15 and 23 (local0-local7) are not assigned a keyword or name.
- They can be assigned to different meanings depending on the use context. Also, various operating systems have been found to utilize both facilities 9 and 15 for clock messages.

Severity

Value	Severity
0	**Emergency**: system is unusable
1	**Alert**: action must be taken immediately
2	**Critical**: critical conditions that should be corrected immediately and indicates failure in a system
3	**Error**: a failure that is not urgent, should be resolved within a given time
4	**Warning**: an error does not presently exist; but, an error will occur in the future if the condition is not addressed
5	**Notice**: an event that is not an error, but that is considered unusual. Does not require immediate action.
6	**Informational**: messages issued regarding normal operation
7	**Debug**: messages of interest to developers

End Device Logs

Syslog (Contd.)

Priority

- The Priority (PRI) value is calculated by multiplying the Facility value by 8, and then adding it to the Severity value, as shown below

Priority = (Facility * 8) + Severity

- The Priority value is the first value in a packet and occurs between angled brackets <>.

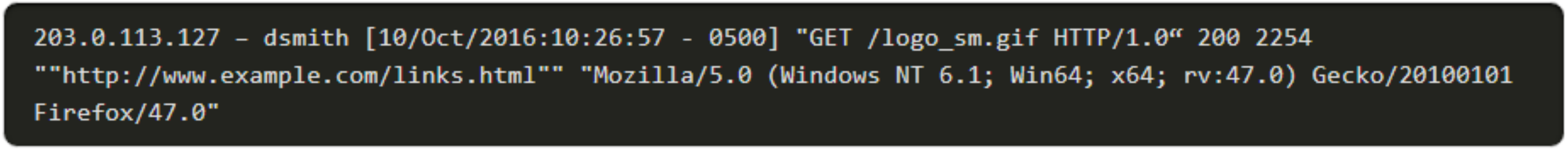
- Additional Information:
  - RFC Syslog Protocol: RFC 5424: The Syslog Protocol (rfc-editor.org)
  - Syslog Facilities and Severity Levels Explained: What are Syslog Facilities and Levels? (trendmicro.com)

End Device Logs

Server Logs

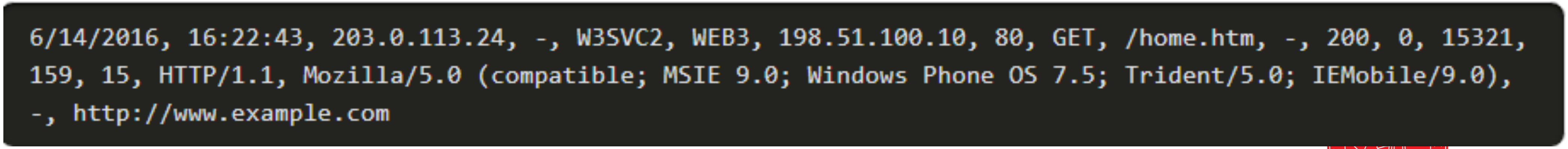
- Server logs are an essential source of data for network security monitoring.
- DNS proxy server logs which document all the DNS queries and responses that occur on the network are especially important.
- Two important log files are Apache webserver access logs and Microsoft Internet Information Server (IIS) access logs.

Apache Access Log



```
203.0.113.127 – dsmith [10/Oct/2016:10:26:57 - 0500] "GET /logo_sm.gif HTTP/1.0“ 200 2254
""http://www.example.com/links.html"" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101
Firefox/47.0"
```

IIS Access Log

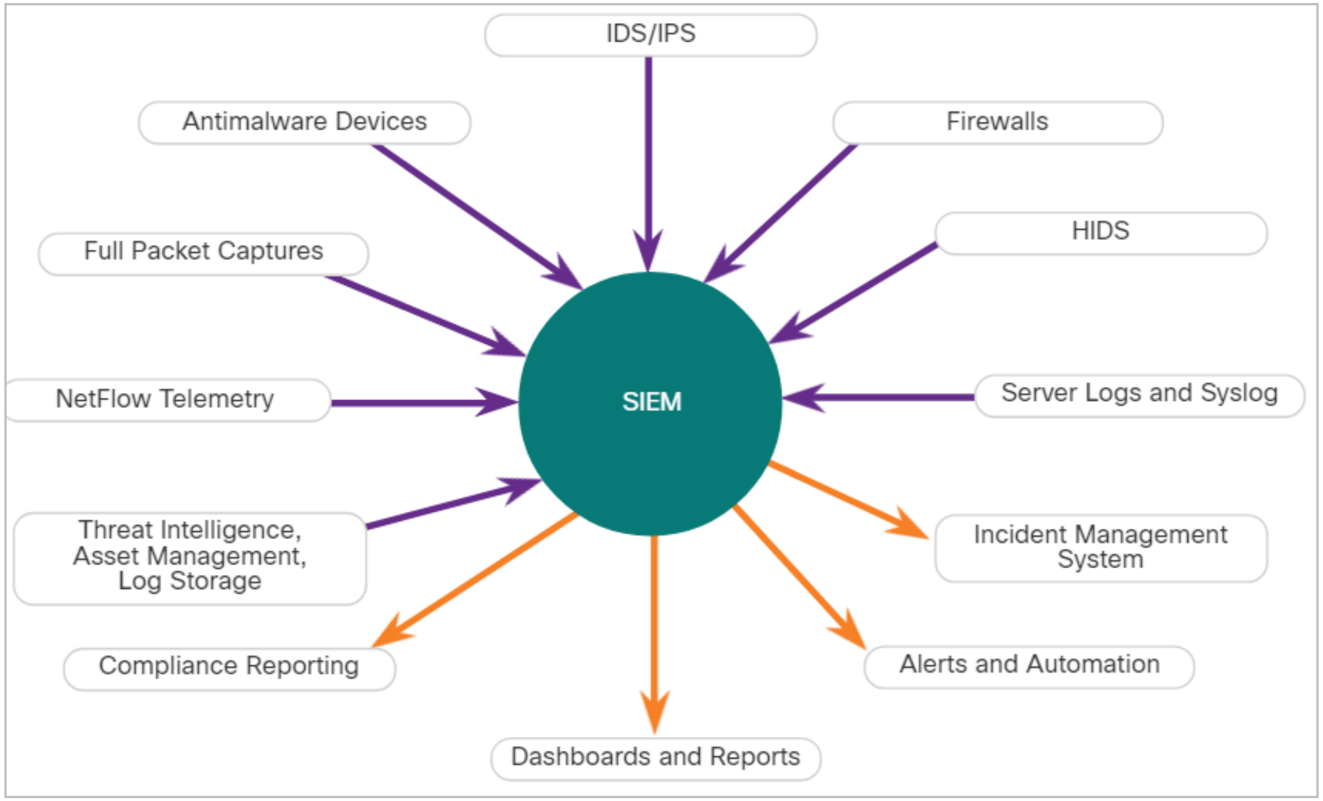


```
6/14/2016, 16:22:43, 203.0.113.24, -, W3SVC2, WEB3, 198.51.100.10, 80, GET, /home.htm, -, 200, 0, 15321,
159, 15, HTTP/1.1, Mozilla/5.0 (compatible; MSIE 9.0; Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0),
-, http://www.example.com
```

End Device Logs

SIEM and Log Collection

Security Information and Event Management (SIEM) technology is used in many organizations to provide real-time reporting and long-term analysis of security events, as shown in the figure.



SIEM Inputs and Outputs

End Device Logs

SIEM and Log Collection (Contd.)

SIEM combines the essential functions of SEM and SIM tools to provide a view of the enterprise network using the following functions:

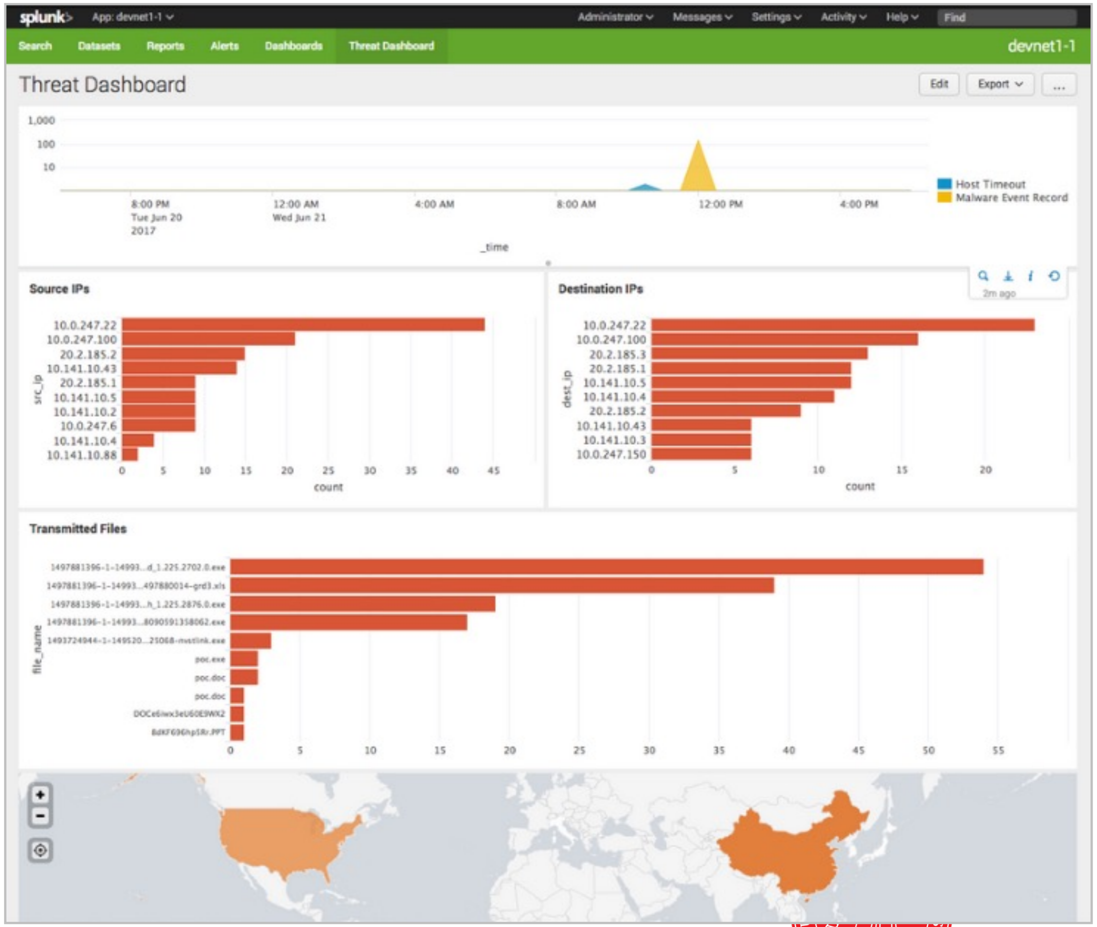
- **Log collection** – Event records from sources throughout the organization provide important forensic information and help to address compliance reporting requirements.
- **Normalization** – This maps log messages from different systems into a common data model, enabling the organization to connect and analyze related events, even if they are initially logged in different source formats.
- **Correlation** – This links logs and events from disparate systems or applications, speeding detection of and reaction to security threats.
- **Aggregation** – This reduces the volume of event data by consolidating duplicate event records.
- **Reporting** – This presents the correlated, aggregated event data in real-time monitoring and long-term summaries, including graphical interactive dashboards.
- **Compliance** – This is reporting to satisfy the requirements of various compliance regulations.

End Device Logs

SIEM and Log Collection (Contd.)

- A popular SIEM is Splunk, which is made by a Cisco partner. We can also use the ELK Stack and Security Onion.
- The figure shows a Splunk Threat Dashboard. Splunk is widely used in SOCs.
- Because of the lack of cybersecurity professionals to monitor and analyze the large volume of security data, it is important that tools from multiple vendors can be integrated into a single platform.
- Integrated security platforms go beyond SIEM and SOAR to unify multiple security technologies into a unified team.

Splunk Threat Dashboard



Threat Dashboard

Source IPs

10.0.247.22
10.0.247.100
20.2.185.2
10.141.10.43
20.2.185.1
10.141.10.5
10.141.10.2
10.0.247.6
10.141.10.4
10.141.10.88

Destination IPs

10.0.247.22
10.0.247.100
20.2.185.3
20.2.185.1
10.141.10.5
10.141.10.4
20.2.185.2
10.141.10.43
10.141.10.3
10.0.247.150

Transmitted Files

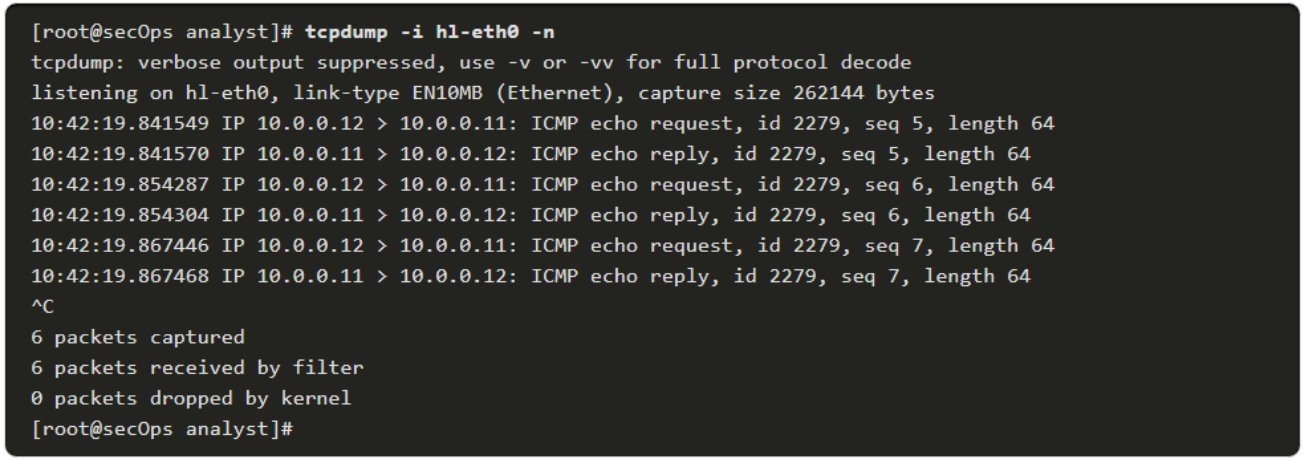
1497881396-1-14993...d_1.225.2702.0.exe
1497881396-1-14993...497880014-grd3.xls
1497881396-1-14993...h_1.225.2876.0.exe
1497881396-1-14993...8090591358062.exe
1493724944-1-149520...21068-mstlink.exe
poc.exe
poc.doc
poc.doc
DOCe6iwx3eU60E9WX2
BdKF696hp5Rr.PPT

Network Logs

Network Logs

Tcpdump

- The tcpdump command line tool is a very popular packet analyzer.
- It can display packet captures in real time or write packet captures to a file.
- It captures detailed packet protocol and content data.
- Wireshark is a GUI built on tcpdump functionality.
- The structure of tcpdump captures varies depending on the protocol captured and the fields requested.



```
[root@secOps analyst]# tcpdump -i hl-eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on hl-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:42:19.841549 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 5, length 64
10:42:19.841570 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 5, length 64
10:42:19.854287 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 6, length 64
10:42:19.854304 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 6, length 64
10:42:19.867446 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 7, length 64
10:42:19.867468 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 7, length 64
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
[root@secOps analyst]#
```

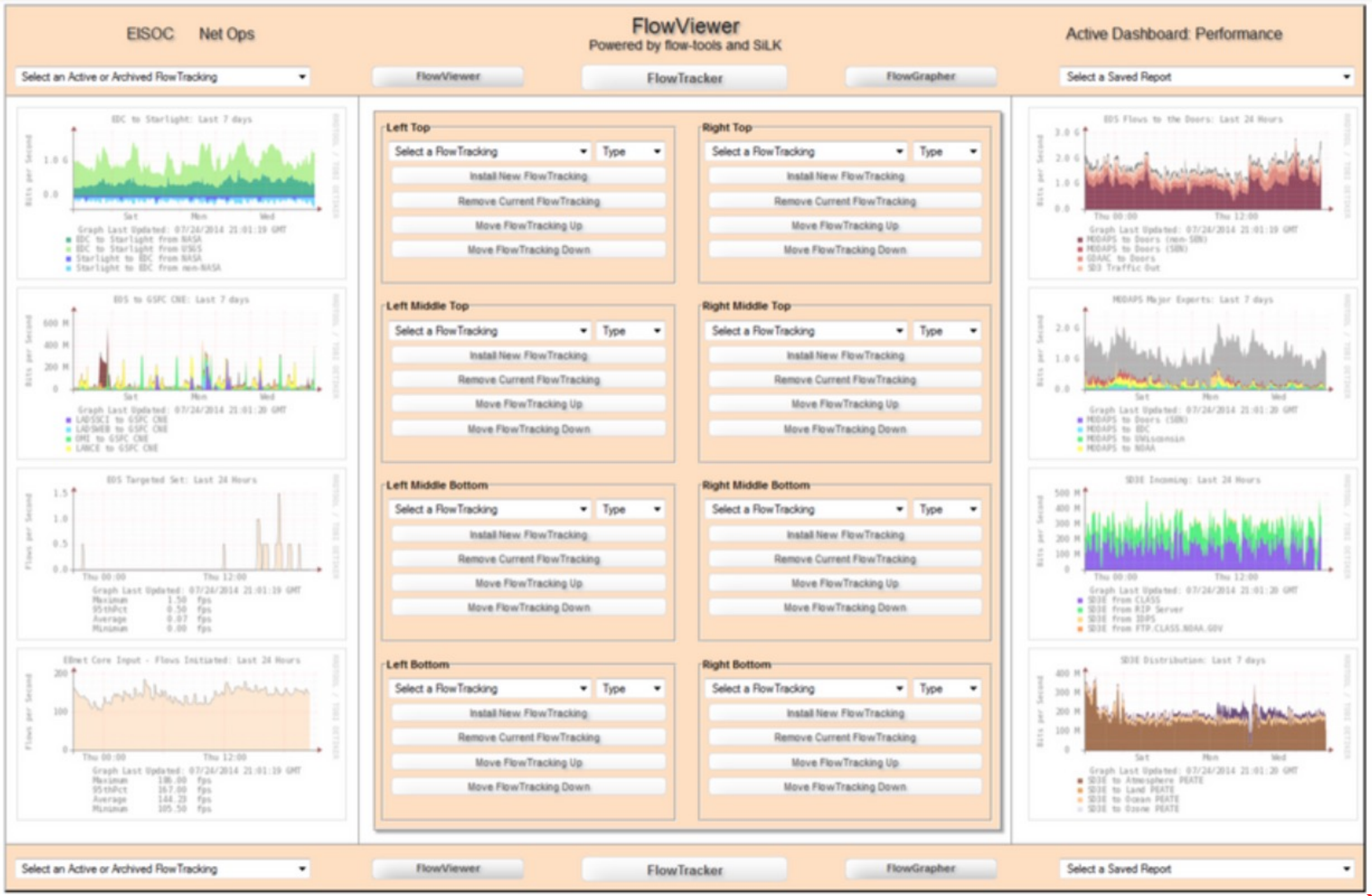
Network Logs

NetFlow

- NetFlow is a protocol that was developed by Cisco as a tool for network troubleshooting and session-based accounting.
- NetFlow provides an important set of services for IP applications, including network traffic accounting, usage-based network billing, network planning, security, Denial-of-Service monitoring capabilities, and network monitoring.
- It also provides information about network users and applications, peak usage times, and traffic routing.
- It records information about the packet flow including metadata. Cisco developed NetFlow and then allowed it to be used as a basis for an IETF standard called IPFIX.
- NetFlow information can be viewed with tools such as the nfdump.
- nfdump provides a command line utility for viewing NetFlow data from the nfcapd capture daemon, or collector.

Network Logs

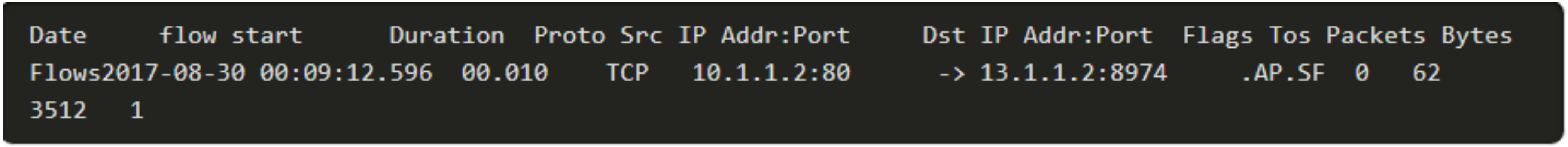
NetFlow



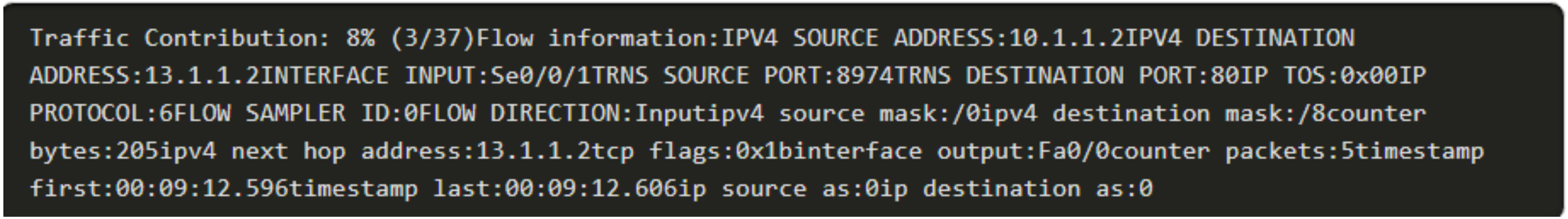
Network Logs

NetFlow (Contd.)

- An example of a basic NetFlow flow record, in two different formats, is shown in the figure.



```
Date      flow start        Duration  Proto Src IP Addr:Port      Dst IP Addr:Port   Flags Tos Packets Bytes
Flows2017-08-30 00:09:12.596  00.010    TCP   10.1.1.2:80         -> 13.1.1.2:8974      .AP.SF  0   62
3512   1
```



```
Traffic Contribution: 8% (3/37)Flow information:IPV4 SOURCE ADDRESS:10.1.1.2IPV4 DESTINATION
ADDRESS:13.1.1.2INTERFACE INPUT:Se0/0/1TRNS SOURCE PORT:8974TRNS DESTINATION PORT:80IP TOS:0x00IP
PROTOCOL:6FLOW SAMPLER ID:0FLOW DIRECTION:Inputipv4 source mask:/0ipv4 destination mask:/8counter
bytes:205ipv4 next hop address:13.1.1.2tcp flags:0x1binterface output:Fa0/0counter packets:5timestamp
first:00:09:12.596timestamp last:00:09:12.606ip source as:0ip destination as:0
```

- A large number of attributes for a flow are available. The IANA registry of IPFIX entities lists several hundred, with the first 128 being the most common.
- NetFlow is a useful tool in the analysis of network security incidents. It can be used to construct a timeline of compromise, understand individual host behavior, or to track the movement of an attacker or exploit from host to host within a network.

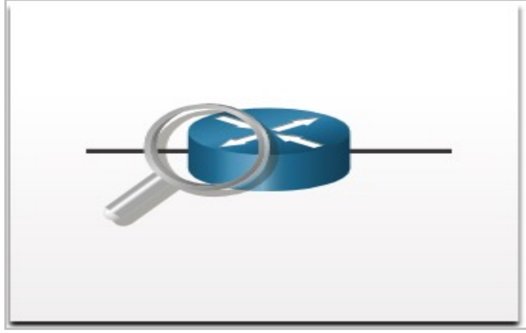
Network Logs

Application Visibility and Control

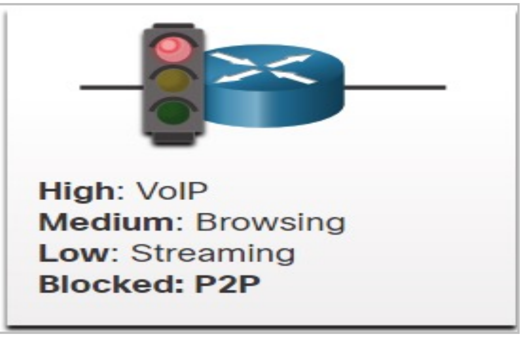
- The Cisco Application Visibility and Control (AVC) system combines multiple technologies to recognize, analyze, and control over 1000 applications.
- Other network vendors such as Juniper and Palo Alto also provide AVC systems
- AVC can analyse voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications.
- AVC uses Cisco next-generation network-based application recognition version 2 (NBAR2), also known as Next-Generation NBAR, to discover and classify the applications in use on the network.
- The NBAR2 application recognition engine supports over 1000 network applications.

Network Logs

Application Visibility and Control (Contd.)



Management and Reporting Tools



High: VoIP
Medium: Browsing
Low: Streaming
Blocked: P2P

Application Recognition
Identify applications using L3 to L7 data.
1000+ applications

- Cloud services
- Cisco WebEx
- YouTube
- Skype
- P2P

NBAR2

Metrics Collection
Collect metrics for export to management tool

- Bandwidth usage
- Response time
- Latency
- Packet loss
- Jitter
- P2P

Netflow9 Flexible Netflow IPFIX

Management and Reporting
Provision the network, collect data, and report on applications performance

- Report generation
- Policy Management

Cisco Prime Other 3rd Party Software

Control
Control application use to maximize network performance

- Application prioritizarion
- Application bandwidth enforcement

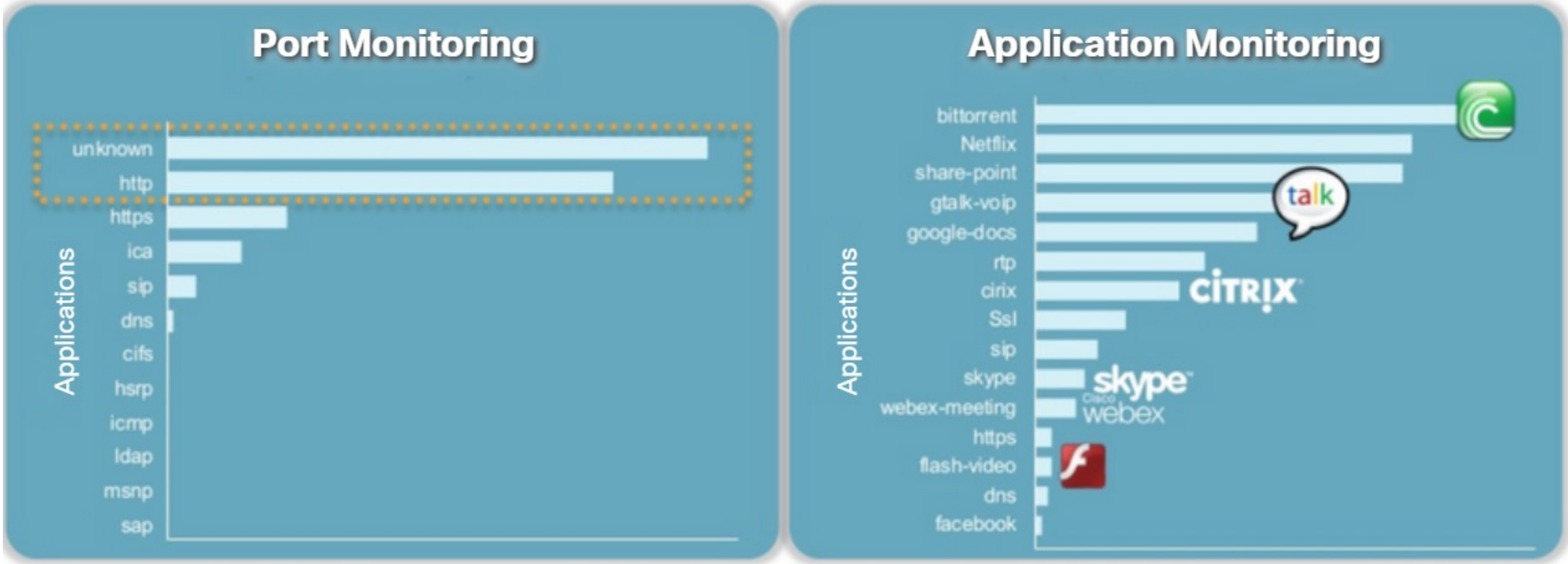
QoS

Network Logs

Application Visibility and Control (Contd.)

Port Monitoring vs. Application Monitoring

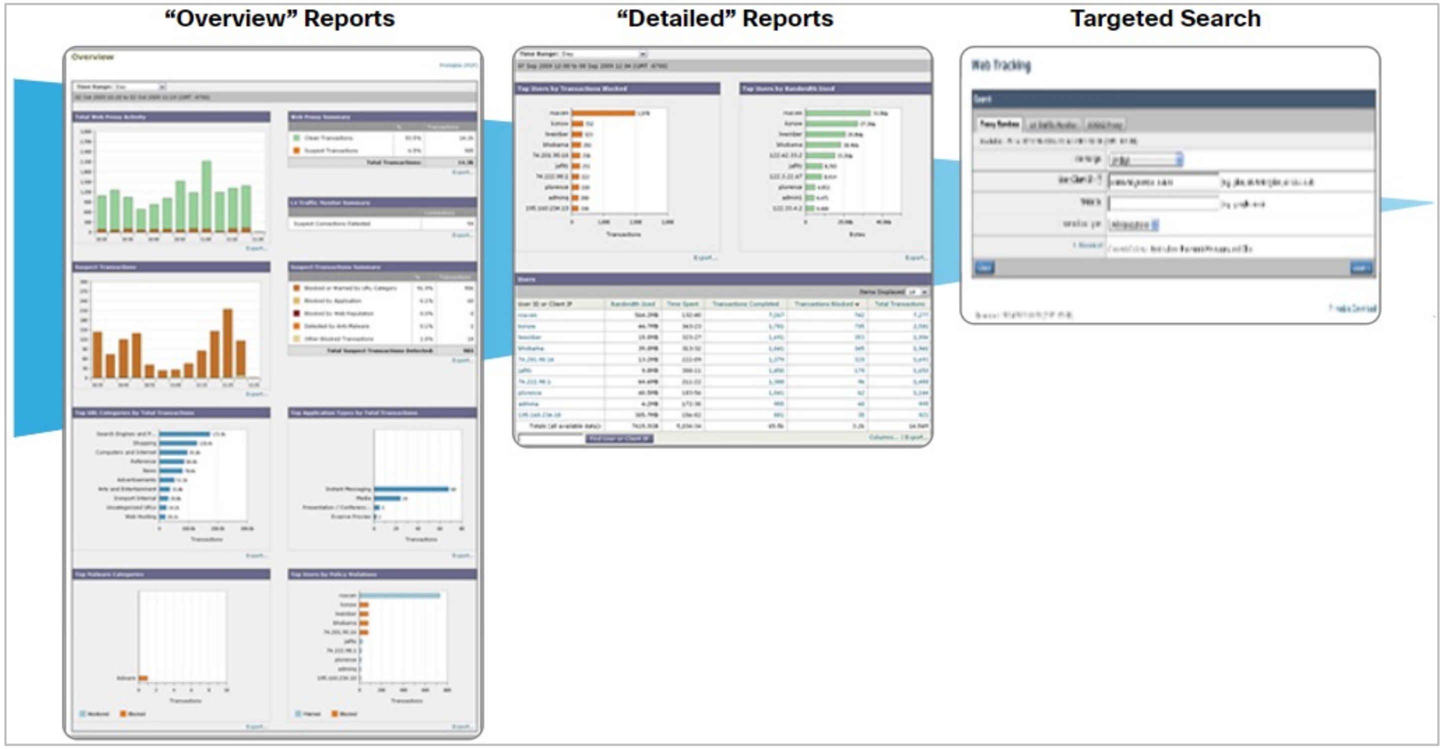
A management and reporting system analyzes and presents the application analysis data into dashboard reports for use by network monitoring personnel. Application usage can also be controlled through quality of service classification and policies based on the AVC information.



Network Logs

Content Filter Logs

- Devices that provide content filtering, such as the Cisco Email Security Appliance (ESA) and the Cisco Web Security Appliance (WSA), provide a wide range of functionalities for security monitoring.
- The figure shows the dashboards from Cisco content filtering devices. By clicking components of the Overview reports, more relevant details are displayed. Target searches provide the focused information.



Network Logs

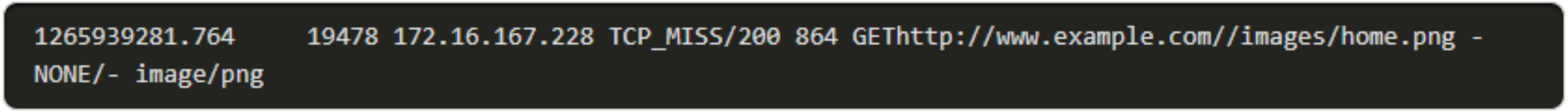
Proxy Logs

- Proxy servers, such as those used for web and DNS requests, contain valuable logs that are a primary source of data for network security monitoring.
- The proxy server requests the resources and returns them to the client and generates logs of all requests and responses.
- These logs can then be analyzed to determine which hosts are making the requests, whether the destinations are safe or potentially malicious, and to also gain insights into the kind of resources that have been downloaded.
- Web proxies provide data that helps determine whether responses from the web were generated in response to legitimate requests or have been manipulated to appear to be responses but are in fact exploits.
- It is also possible to use web proxies to inspect outgoing traffic as means of data loss prevention (DLP).
- DLP involves scanning outgoing traffic to detect whether the data that is leaving the web contains sensitive, confidential, or secret information.

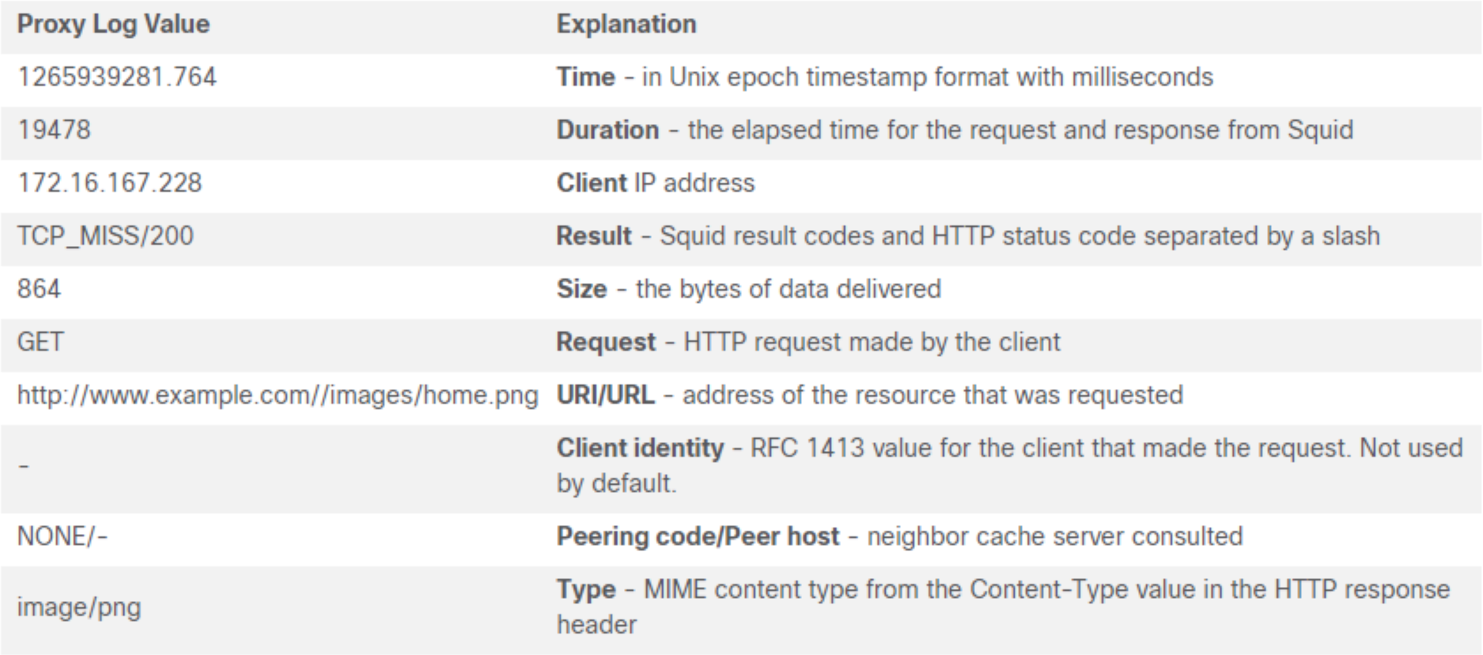
Network Logs

Proxy Logs (Contd.)

Squid Example Log



```
1265939281.764     19478 172.16.167.228 TCP_MISS/200 864 GEThttp://www.example.com//images/home.png -
NONE/- image/png
```



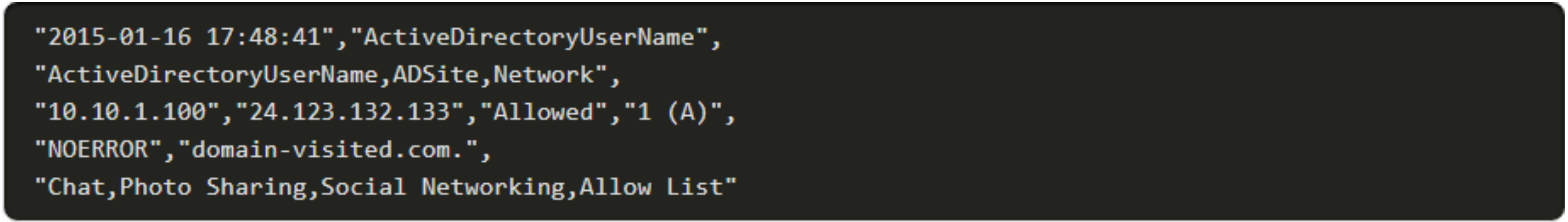
Proxy Log Value	Explanation
1265939281.764	**Time** - in Unix epoch timestamp format with milliseconds
19478	**Duration** - the elapsed time for the request and response from Squid
172.16.167.228	**Client** IP address
TCP_MISS/200	**Result** - Squid result codes and HTTP status code separated by a slash
864	**Size** - the bytes of data delivered
GET	**Request** - HTTP request made by the client
http://www.example.com//images/home.png	**URI/URL** - address of the resource that was requested
-	**Client identity** - RFC 1413 value for the client that made the request. Not used by default.
NONE/-	**Peering code/Peer host** - neighbor cache server consulted
image/png	**Type** - MIME content type from the Content-Type value in the HTTP response header

Network Logs

Proxy Logs (Contd.)

Cisco Umbrella

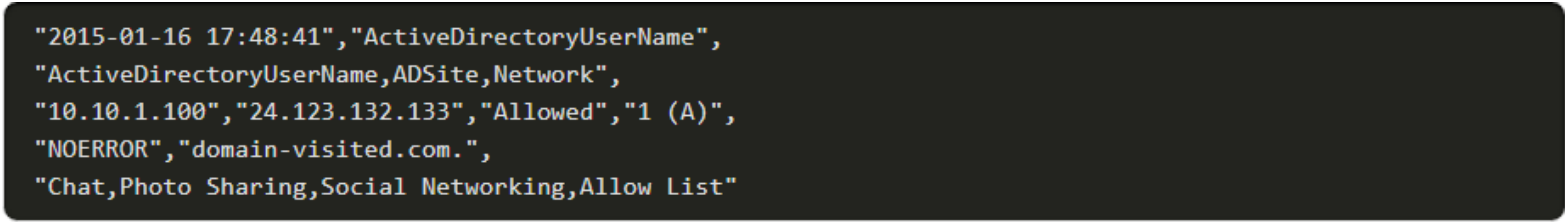
- Cisco Umbrella, formerly OpenDNS, offers a hosted DNS service that extends the capability of DNS to include security enhancements.
- Cisco Umbrella applies many more resources to managing DNS than most organizations can afford. Cisco Umbrella functions in part as a DNS super proxy in this regard.
- The Cisco Umbrella suite of security products apply real-time threat intelligence to managing DNS access and the security of DNS records.
- An example of a DNS proxy log appears below.



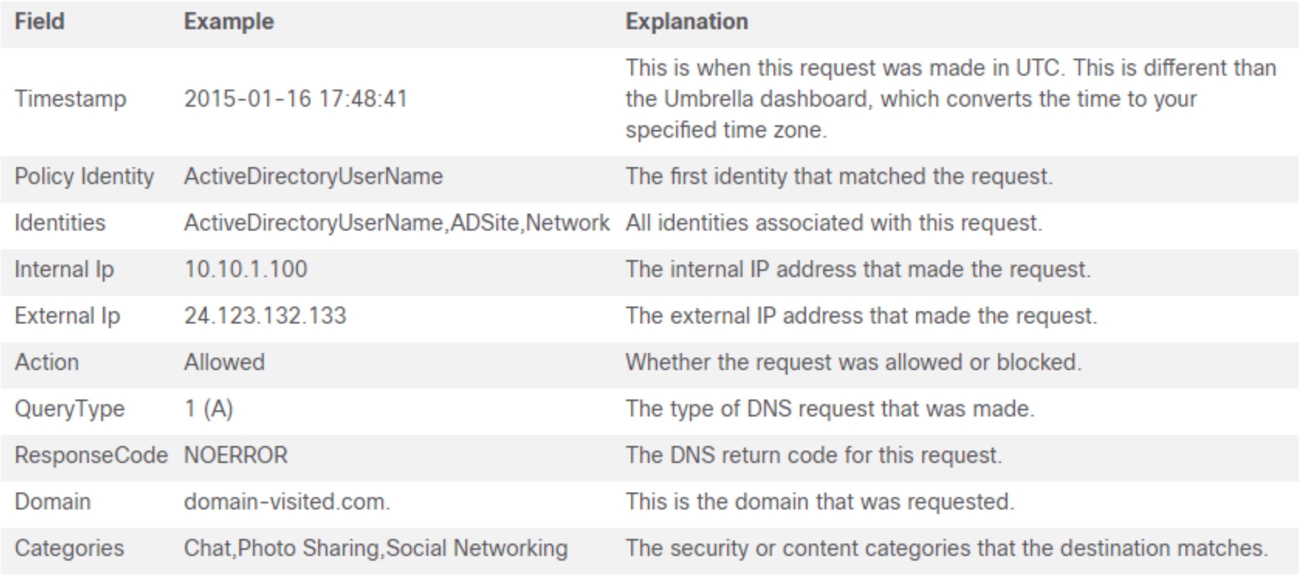
```
"2015-01-16 17:48:41","ActiveDirectoryUserName",
"ActiveDirectoryUserName,ADSite,Network",
"10.10.1.100","24.123.132.133","Allowed","1 (A)",
"NOERROR","domain-visited.com.",
"Chat,Photo Sharing,Social Networking,Allow List"
```

Network Logs

Proxy Logs (Contd.)



```
"2015-01-16 17:48:41","ActiveDirectoryUserName",
"ActiveDirectoryUserName,ADSite,Network",
"10.10.1.100","24.123.132.133","Allowed","1 (A)",
"NOERROR","domain-visited.com.",
"Chat,Photo Sharing,Social Networking,Allow List"
```



Field	Example	Explanation
Timestamp	2015-01-16 17:48:41	This is when this request was made in UTC. This is different than the Umbrella dashboard, which converts the time to your specified time zone.
Policy Identity	ActiveDirectoryUserName	The first identity that matched the request.
Identities	ActiveDirectoryUserName,ADSite,Network	All identities associated with this request.
Internal Ip	10.10.1.100	The internal IP address that made the request.
External Ip	24.123.132.133	The external IP address that made the request.
Action	Allowed	Whether the request was allowed or blocked.
QueryType	1 (A)	The type of DNS request that was made.
ResponseCode	NOERROR	The DNS return code for this request.
Domain	domain-visited.com.	This is the domain that was requested.
Categories	Chat,Photo Sharing,Social Networking	The security or content categories that the destination matches.

Network Logs

Next-Generation Firewalls

- Next-Generation or NextGen Firewall devices extend network security beyond IP addresses and Layer 4 port numbers to the application layer and beyond.
- NexGen Firewalls are advanced devices that provided much more functionality than previous generations of network security devices.
- One functionality is reporting dashboards with interactive features that allow quick point-and-click reports on very specific information without the need for SIEM or other event correlators.
- NextGen Firewall devices (NGFW) use Firepower Services to consolidate multiple security layers into a single platform.
- Firepower services include application visibility and control, Firepower Next-Generation IPS (NGIPS), reputation and category-based URL filtering, and Advanced Malware Protection (AMP).

Network Logs

Next-Generation Firewalls (Contd.)

Common NGFW events include:

- Connection Event
- Intrusion Event
- Host or Endpoint Event
- Network Discovery Event
- Netflow Event

Services Provided by NGFW

Intrusion Prevention (Subscription)

Firepower Analytics and Automation

Advanced Malware Protection and Sandboxing (Subscription)

URL Filtering (Subscription)

Application Visibility and Control

Built-in Network Profiling

Identity-Policy Control and VPN

Network Security Data Summary

Network Security Data Summary

What Did I Learn in this Module?

- Alert data consists of messages that are generated by intrusion prevention systems (IPSs) or intrusion detection systems (IDSs) in response to traffic that violates a rule or matches the signature of a known exploit.
- Within the Security Onion suite of NSM tools, alerts are generated by Snort and are made readable and searchable by the Sguil, Squert, and Kibana applications.
- Session data will include identifying information such as the five tuples of source and destination IP addresses, source and destination port numbers, and the IP code for the protocol in use.
- Data about the session typically includes a session ID, the amount of data transferred by source and destination, and information related to the duration of the session.
- Full packet captures contain the actual contents of data conversations, such as the text of email messages, the HTML in webpages, and the files that enter or leave the network.
- Statistical data is created through the analysis of various forms of network data.

Network Security Data Summary

What Did I Learn in this Module? (Contd.)

- Host-based intrusion detection systems (HIDS) run on individual hosts.
- Syslog incudes specifications for message formats, a client-server application structure, and network protocol.
- Server logs are an essential source of data for network security monitoring.
- DNS proxy server logs document all the DNS queries and responses that occur on the network.
- DNS proxy logs are useful for identifying hosts that may have visited dangerous websites and for identifying DNS data exfiltration and connections to malware command-and-control servers.
- SIEM combines the essential functions of security event management (SEM) and security information management (SIM) tools to provide a comprehensive view of the enterprise network using log collection, normalization, correlation, aggregation, reporting, and compliance.

Network Security Data Summary

What Did I Learn in this Module? (Contd.)

- The tcpdump command line tool is a very popular packet analyzer. It can display packet captures in real time or write packet captures to a file.
- NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing.
- Cisco Application Visibility and Control uses Cisco next-generation network-based application recognition version 2 (NBAR2), also known as Next-Generation NBAR.
- Devices such as the Cisco Email Security Appliance (ESA) and the Cisco Web Security Appliance (WSA), provide a wide range of functionalities for security monitoring by utilizing content filtering.
- Proxy servers are devices that act as intermediaries for network clients.
- NextGen Firewall devices extend network security beyond IP addresses and Layer 4 port numbers to the application layer and beyond.