Chapter 9: Security Monitoring

Information Security

Dr. Ayman Aljarbouh

9.2 Network Security Data

Module Objectives

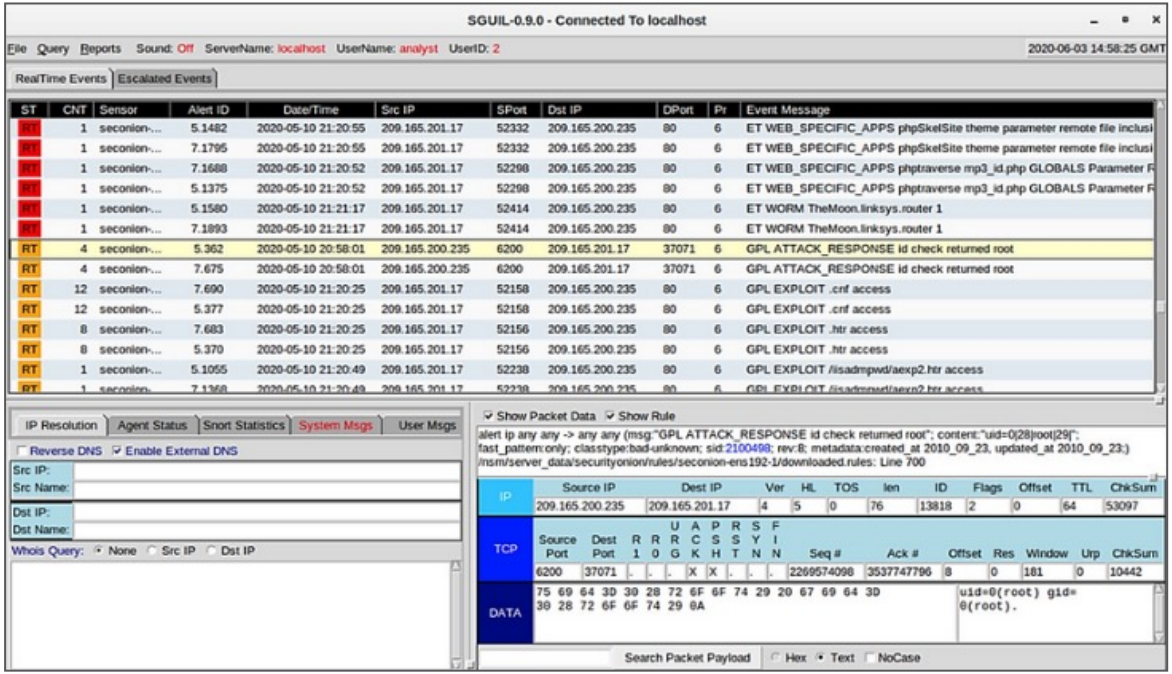
Module Title: Network Security Data

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.

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 Console Showing Test Alert from Snort IDS

Session and Transaction Data

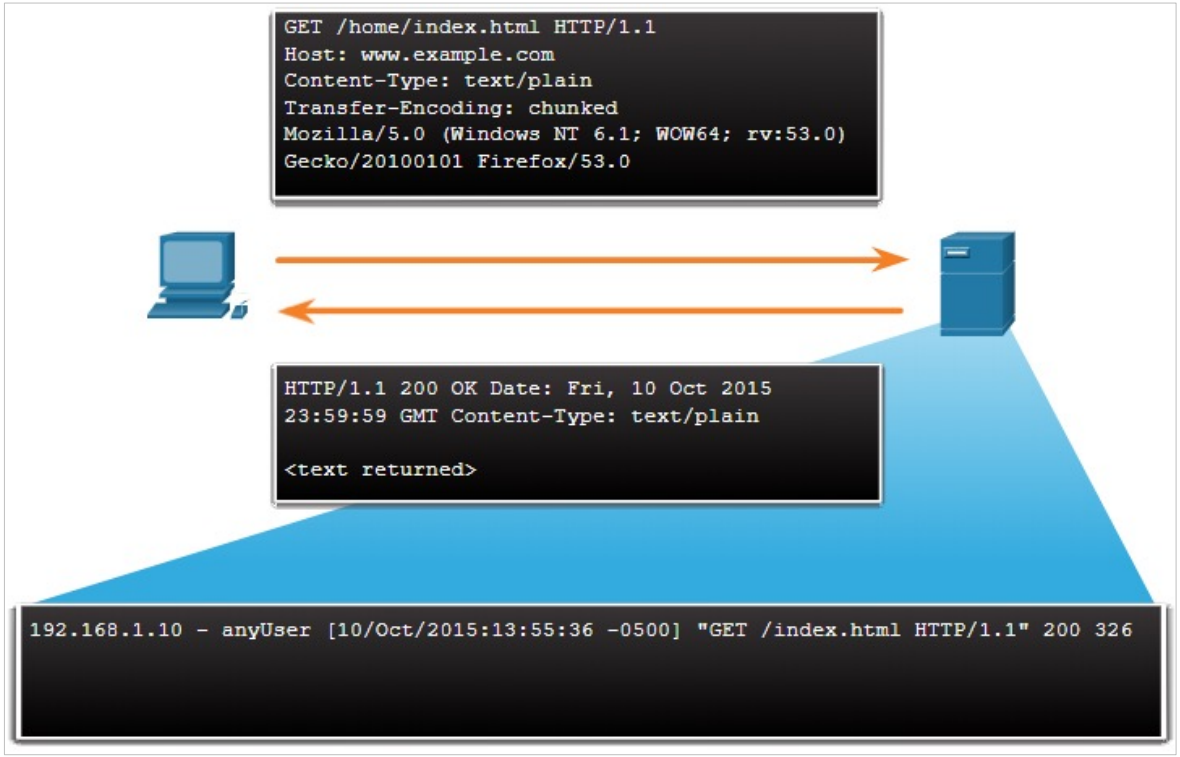
- Session data is a record of a conversation between two network endpoints.
- It includes **the five tuples** of source and destination IP addresses, source and destination port numbers, and the IP code for the protocol in use.
- Data about the session includes a session ID, the amount of data transferred 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	CaTMSv1Sb8HtFunqjj	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

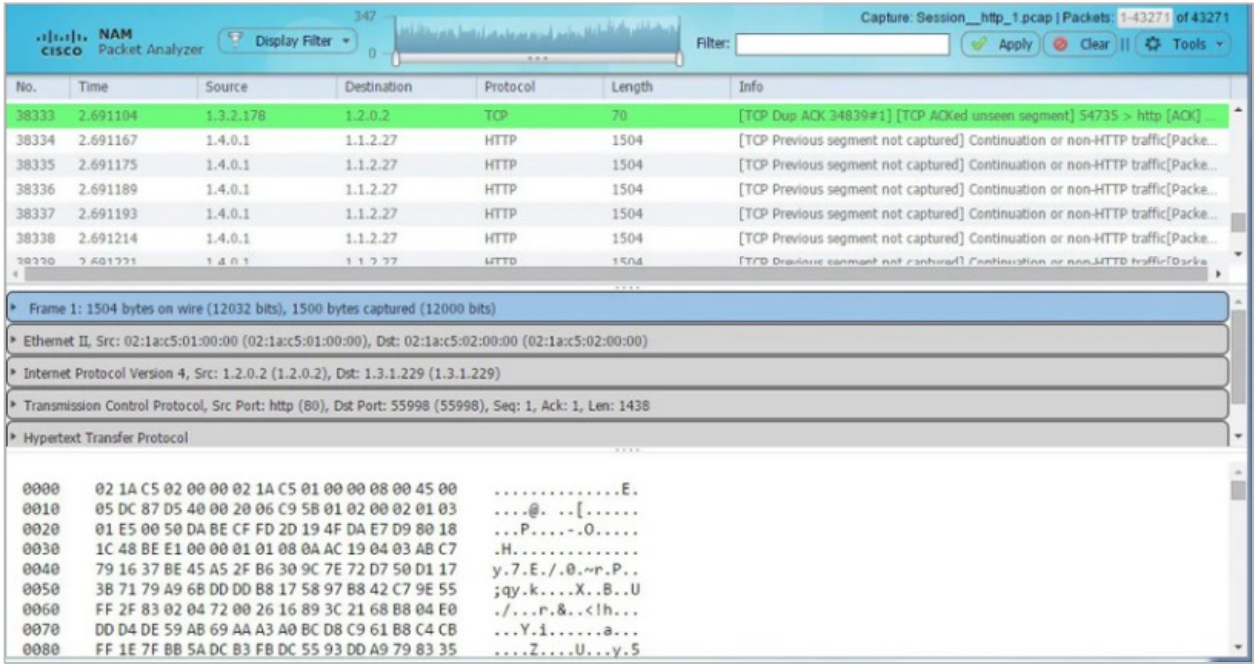
Session and Transaction Data (Contd.)

- 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.



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.
- The figure here shows the interface for the Network Analysis Monitor component of Cisco Prime Infrastructure system, which can display full packet captures.



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.

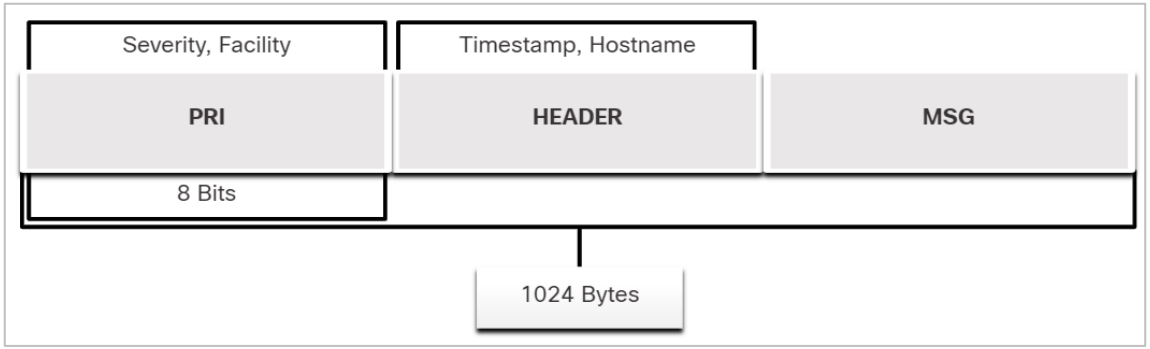
Host Logs (Contd.)

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.

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.



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

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 <>.

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

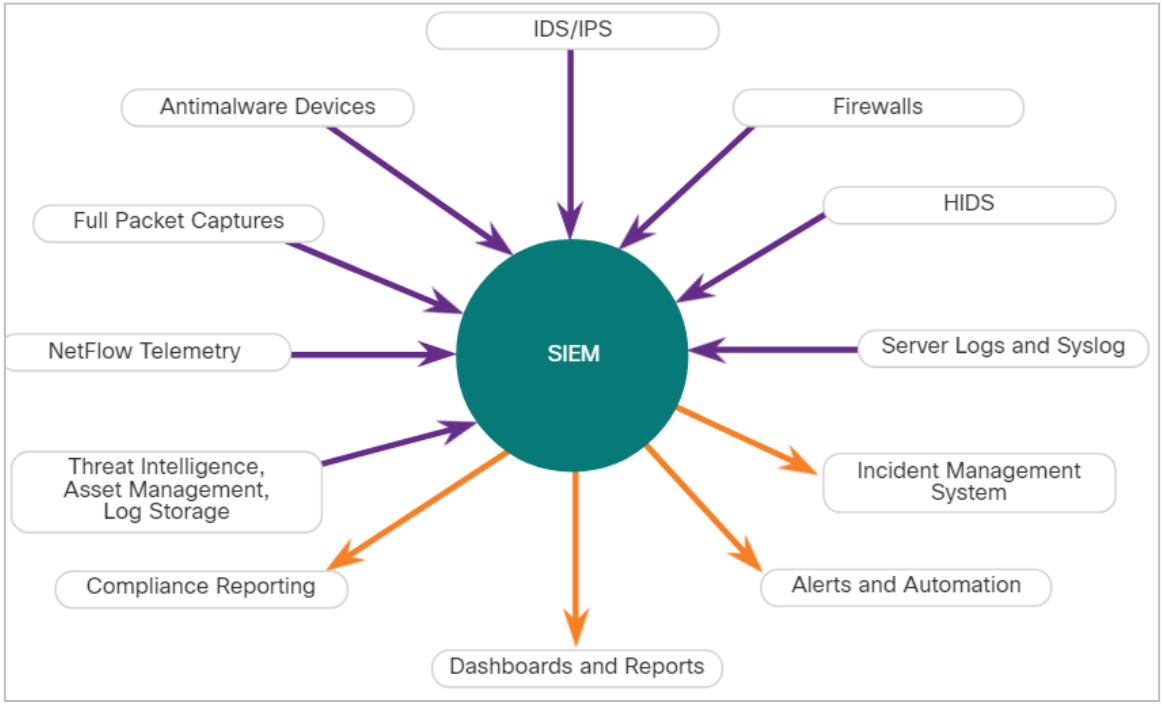
```
203.0.113.127 – dsmith [10/Oct/2016:10:26:57 - 0500] "GET /logo_sm.gif HTTP/1.0“ 200 2254
""http://www.example.com/links.html"" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101
Firefox/47.0"
```

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
```

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

SIEM and Log Collection (Contd.)

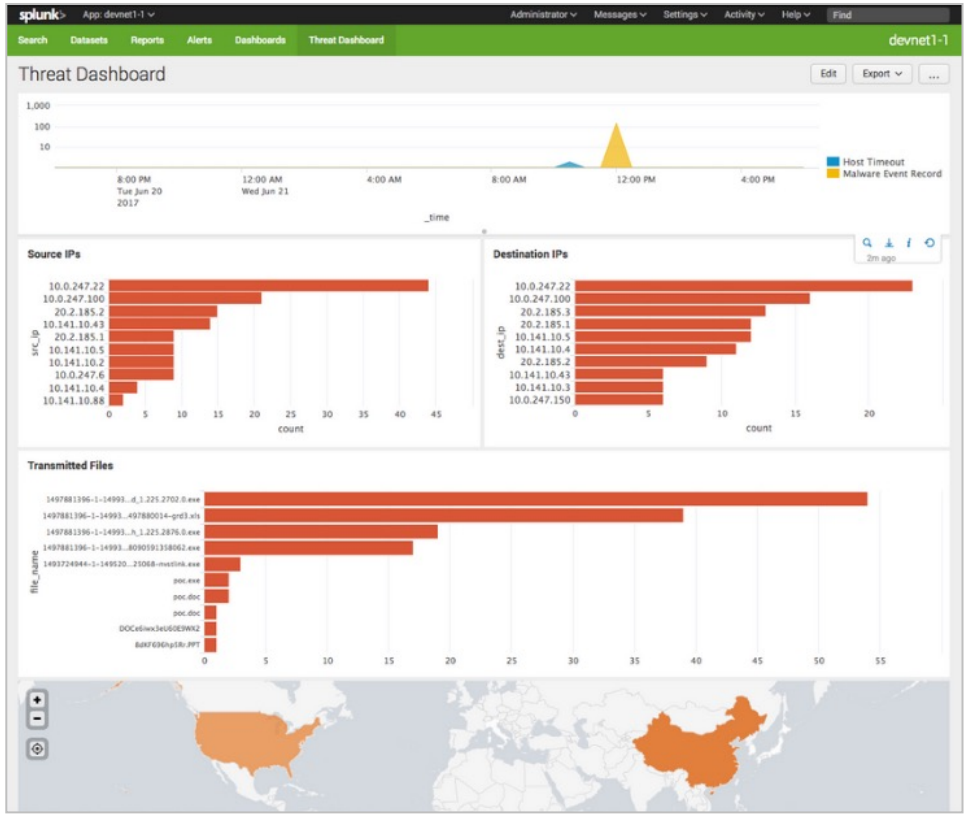
SIEM combines the essential functions of SEM and SIM tools to provide a view of the enterprise network using the following functions:

- **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.

SIEM and Log Collection (Contd.)

- A popular SIEM is Splunk, which is made by a Cisco partner.
- 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



New Terms and Commands

• Session data • Squil	• Snort • Transaction data

Lab 33 - Explore a NetFlow Implementation

In this lab, you will do the following:

- Explore an implementation of NetFlow.