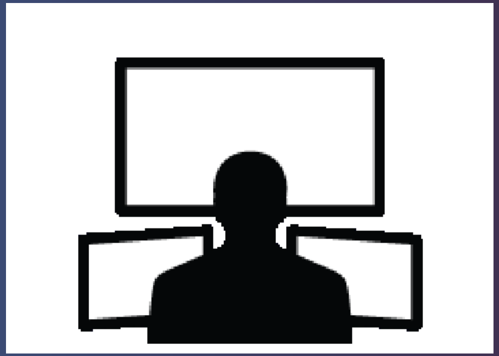
UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Prednáška 9
Security data and alerts



Riešenie bezpečnostných incidentov
(CyberOps Associate v1.02)

Mgr. Jana Uramová, PhD.
Katedra informačných sietí
Fakulta riadenia a informatiky, ŽU

Vytvorené v rámci projektu KEGA 026TUKE-4/2021.

Ktorý výsledok pokrýva táto prednáška

Výsledky vzdelávania

Študent po absolvovaní predmetu získa vedomosti a zručnosti potrebné na úspešné zvládnutie úloh, povinností a zodpovedností bezpečnostného analytika v operačnom centre bezpečnosti.
Študent po absolvovaní predmetu bude vedieť:

- Vysvetliť rolu analytika v rámci kybernetickej bezpečnosti
- Vysvetliť prostriedky operačného systému Windows
  a Linux a charakteristiky pre podporu analýzy v rámci kybernetickej bezpečnosti
- Analyzovať operácie v rámci sieťových protokolov a služieb
- Vysvetliť operácie sieťovej infraštruktúry
- Klasifikovať rôzne typy sieťových útokov
- Použiť sieťové monitorovacie nástroje na identifikáciu útokov proti sieťovým protokolom a službám
- Použiť rôzne metódy na prevenciu škodlivého prístupu do počítačových sietí, k používateľom a k dátam
- Vysvetliť vplyvy kryptografie v rámci monitorovania bezpečnostných sietí
- Vysvetliť, ako skúmať a vyhodnocovať zraniteľnosti a útoky koncových zariadení
- Identifikovať hlásenia v rámci sieťovej bezpečnosti
- Analyzovať sieťovú prevádzku na overenie potencionálneho zneužitia siete
- Aplikovať reakčné modely na incident, a získať prostriedky na manažovanie sieťových bezpečnostných incidentov

- Prerekvizity:
  - Princípy IKS, Počítačové siete 1, Úvod do OS

Preliminary version of topics for lectures

Planning

Week	CyberOps Modules in lectures	Exam from:
1	Chapter 1 The Danger Chapter 2 Fighters in the War Against Cybercrime Chapter 3: The Windows Operating System	none
2	Chapter 4: Linux Overview Chapter 5 Network Protocols Chapter 6 Ethernet and Internet Protocol (IP) Chapter 7 Connectivity Verification Chapter 8 Address Resolution Protocol Chapter 10 Network Services Chapter 11 Network Communication Devices	1-2
3	Chapter 9 The Transport Layer (+nmap) Chapter 12 Network Security Infrastructure	3-4
4	Chapter 13 Attackers and Their Tools Chapter 14 Common Threats and Attacks	5-10

Week	CyberOps Modules in Lectures	Exam from:
5	Chapter 15 Network Monitoring and Tools *(SIEM, SOAR)* Chapter 16 Attacking the Foundation *(L2, L3 protocols vulnerabilities and attacks)* Chapter 17 Attacking What We Do *(L7 vulnerabilities and attacks)*	11-12
6	Chapter 18 Understanding Defense *(security management)* Chapter 19 Access Control *(AAA)* Chapter 20 Threat Intelligence *(commercials, CVE database)*	13-17
7	Chapter 21 Cryptography Chapter 22 Endpoint Protection	18-20
8	Chapter 23 Endpoint Vulnerability Assessment Chapter 24 Technologies and Protocols	none
9	Chapter 25 Network Security Data Chapter 26 Evaualting Alerts (in Security Onion)	21-23
10	Chapter 27 Working with Network Security Data (Security Onion and ELK) Chapter 28 Digital Forensics and Incident Analysis and Response	24-25
11	Expert talk (invited lecture)	26-28

Obsah dnešnej prednášky

Čo prejdeme spolu na prednáške:

- **Chapter 25 Network Security Data**
- **Chapter 26 Evaualting Alerts (in Security Onion)**

Module 23:
Network Security Data

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

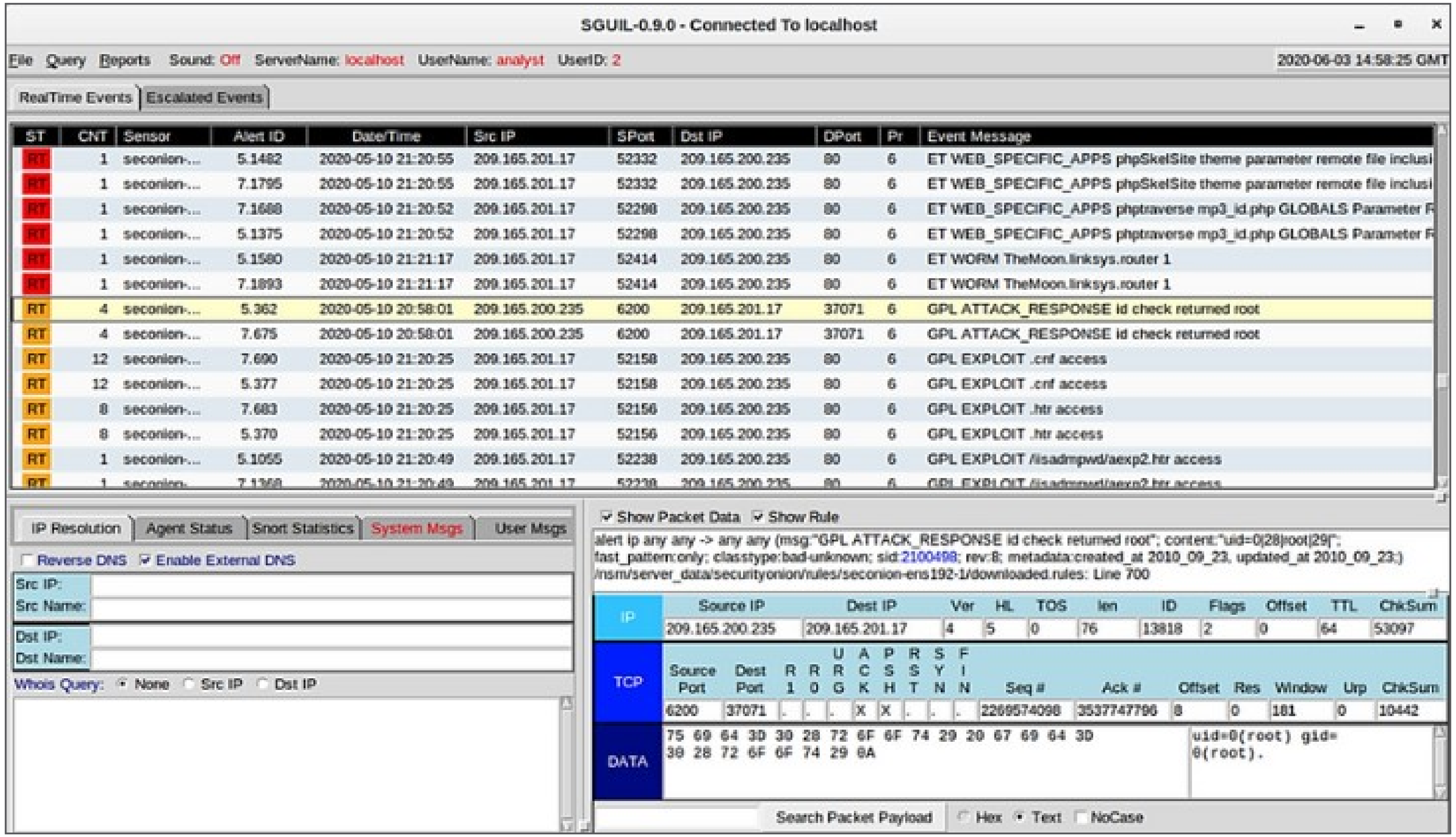
Topic Title	Topic Objective
Types of Security Data	Describe the types of data used in security monitoring.
End Device Logs	Describe the elements of an end device log file.
Network Logs	Describe the elements of a network device log file.

25.1 Types of Security Data

Network Security Data

Alert Data

- messages generated by IPS or IDS
  - in response to traffic that violates a rule
  - or matches the signature of a known exploit.
- NIDS – Snort, suricata
  - comes configured with rules for known exploits.
- Alerts are generated by Snort
  - and are made <u>readable</u> and <u>searchable</u> 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

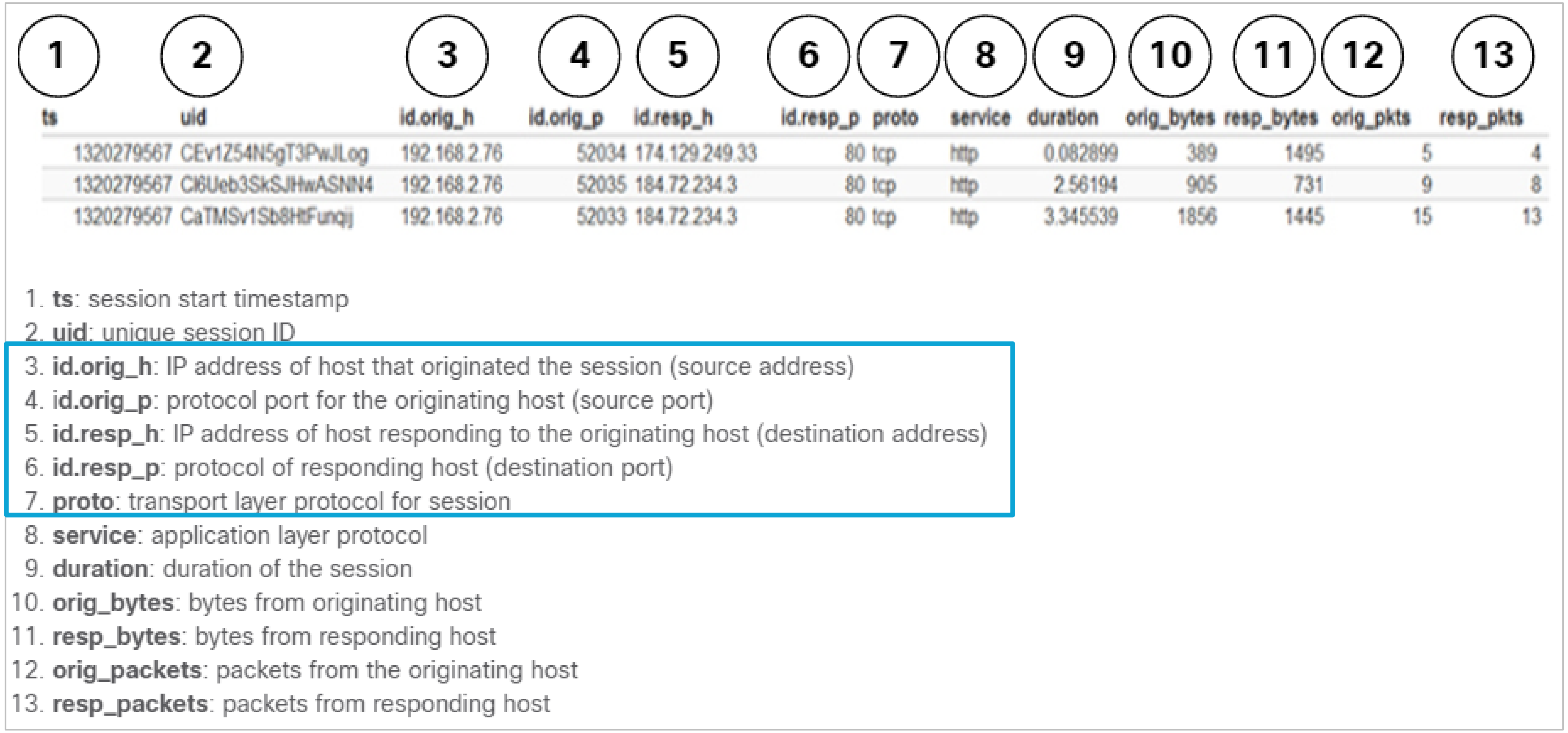
```
75 69 64 3D 30 28 72 6F 6F 74 29 20 67 69 64 3D     uid=0(root) gid=
30 28 72 6F 6F 74 29 0A                              0(root).
```

Search Packet Payload ○ Hex ● Text □ NoCase

Sguil Console Showing Test Alert from Snort IDS

Session 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.



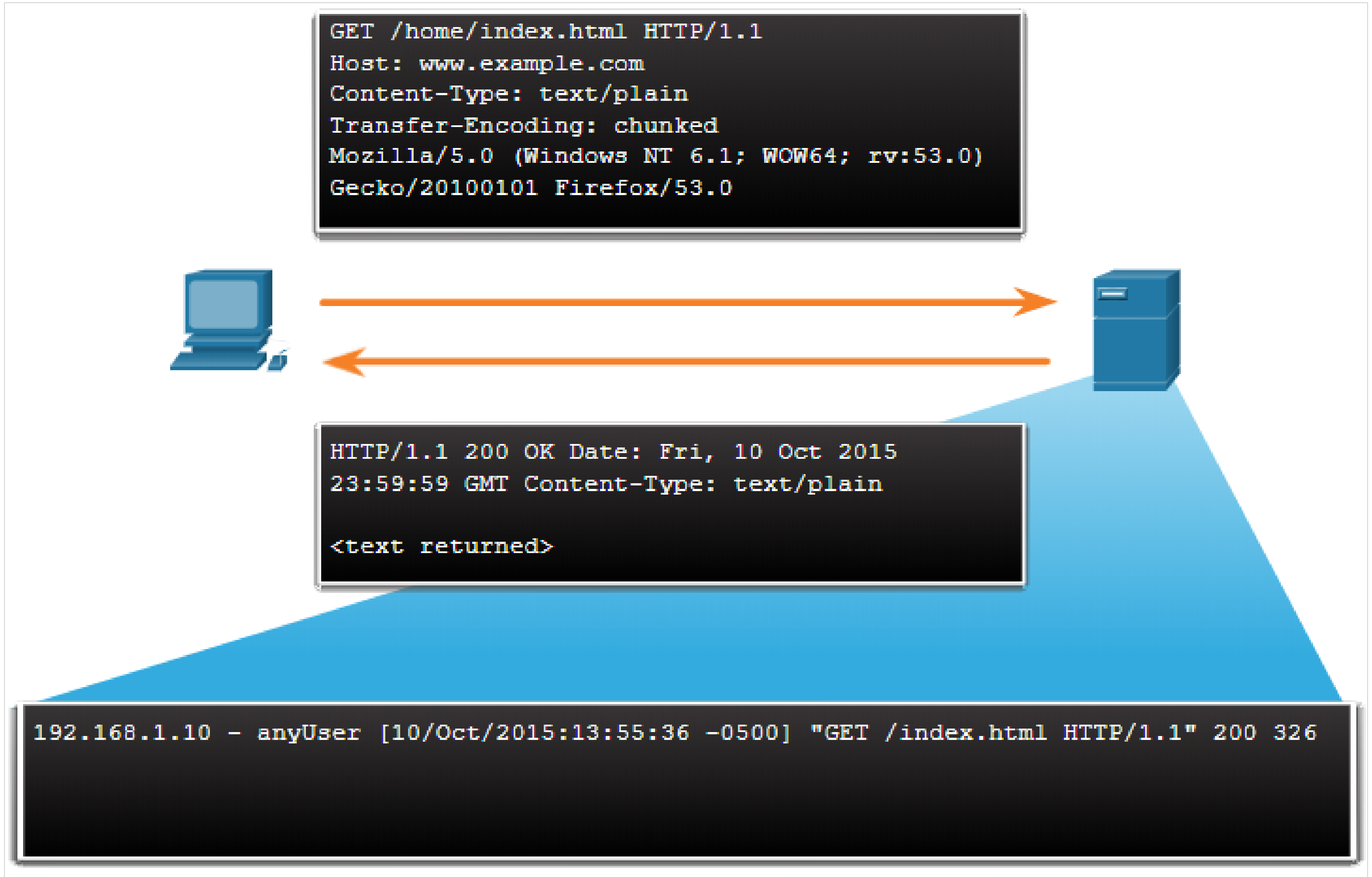
```
  1           2                    3              4      5                   6       7        8        9         10         11          12          13
ts           uid                 id.orig_h     id.orig_p id.resp_h       id.resp_p proto   service  duration  orig_bytes resp_bytes orig_pkts   resp_pkts
   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

Zeek connection log

Transaction Data

- consists of the messages that are exchanged during network sessions.
  - requests and replies
- can be viewed in packet capture transcripts.
- logged
  - in an **access log** on a server
  - or by a NIDS like **Zeek**.
- A session includes some transastion data...
  - 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
```

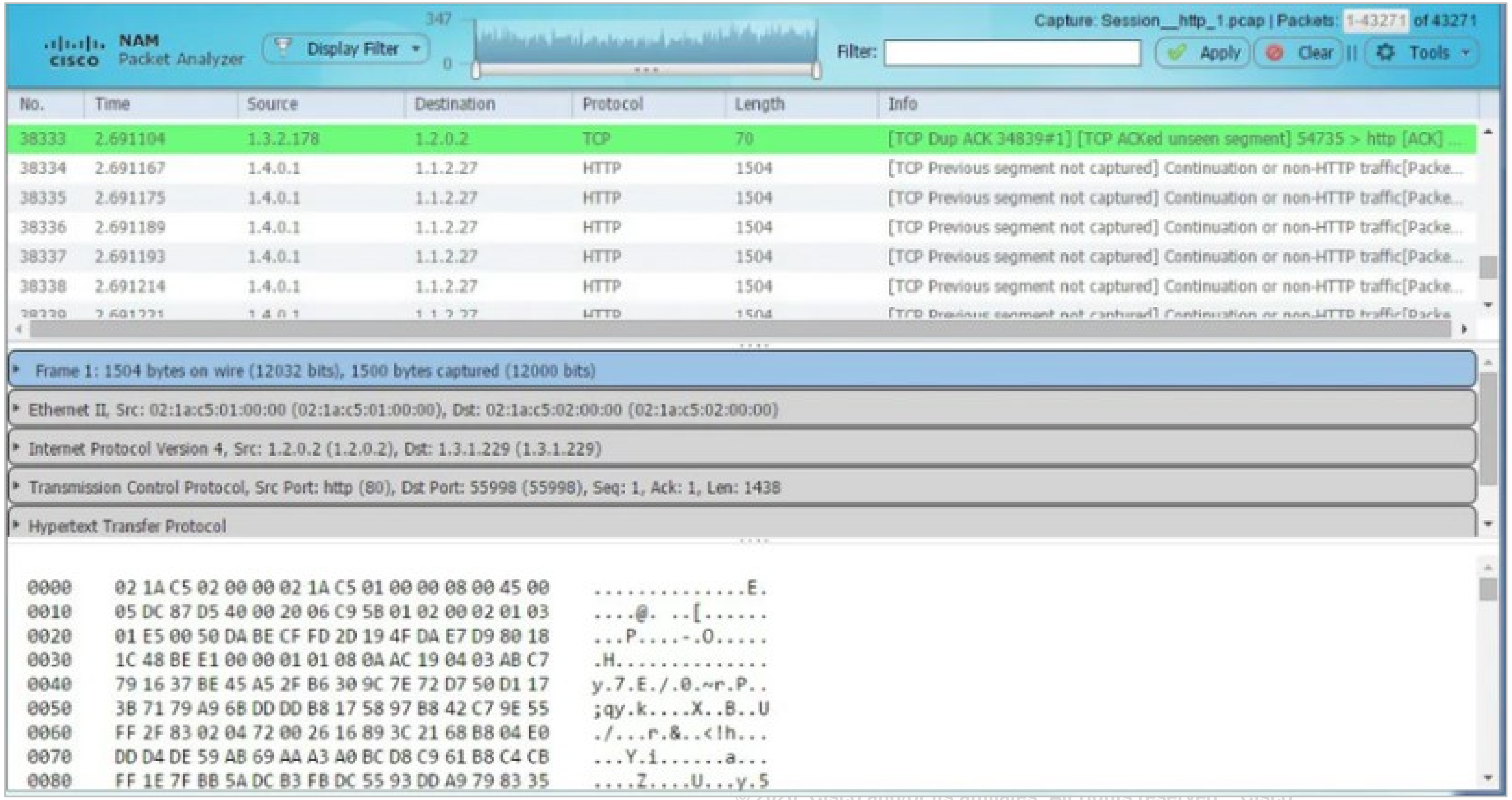
```
HTTP/1.1 200 OK Date: Fri, 10 Oct 2015
23:59:59 GMT Content-Type: text/plain

<text returned>
```

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

Full Packet Captures

- 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.



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

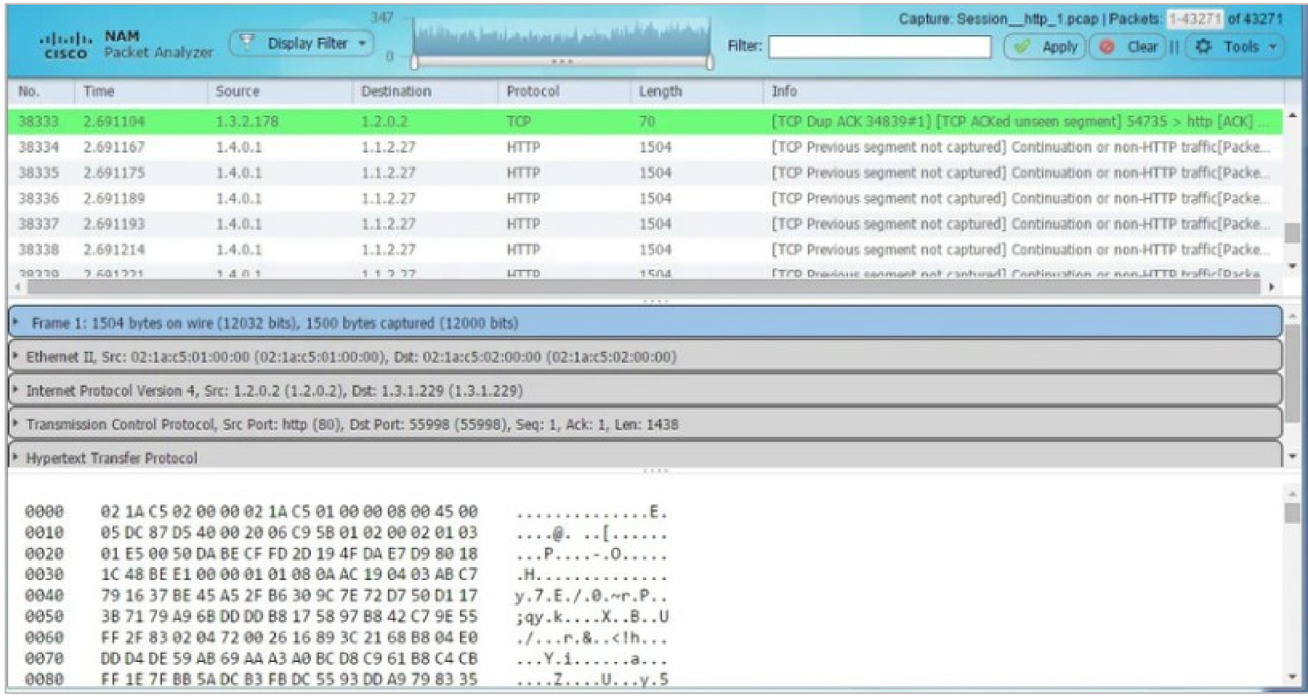
- Frame 1: 1504 bytes on wire (12032 bits), 1500 bytes captured (12000 bits)
- Ethernet II, Src: 02:1a:c5:01:00:00 (02:1a:c5:01:00:00), Dst: 02:1a:c5:02:00:00 (02:1a:c5:02:00:00)
- Internet Protocol Version 4, Src: 1.2.0.2 (1.2.0.2), Dst: 1.3.1.229 (1.3.1.229)
- Transmission Control Protocol, Src Port: 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

Cisco prime infrastructure

- single, unified solution provides
  - wired and wireless lifecycle management
  - application visibility and control
  - policy monitoring and troubleshooting with the Cisco Identity Services Engine (ISE)
  - location-based tracking of mobility devices with the Cisco Mobility Services Engine (MSE)
  - Management of the network, devices, applications, and users – all from one place.


cisco NAM Packet Analyzer
Display Filter
347
0
Filter:
Apply
Clear
Tools
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
```

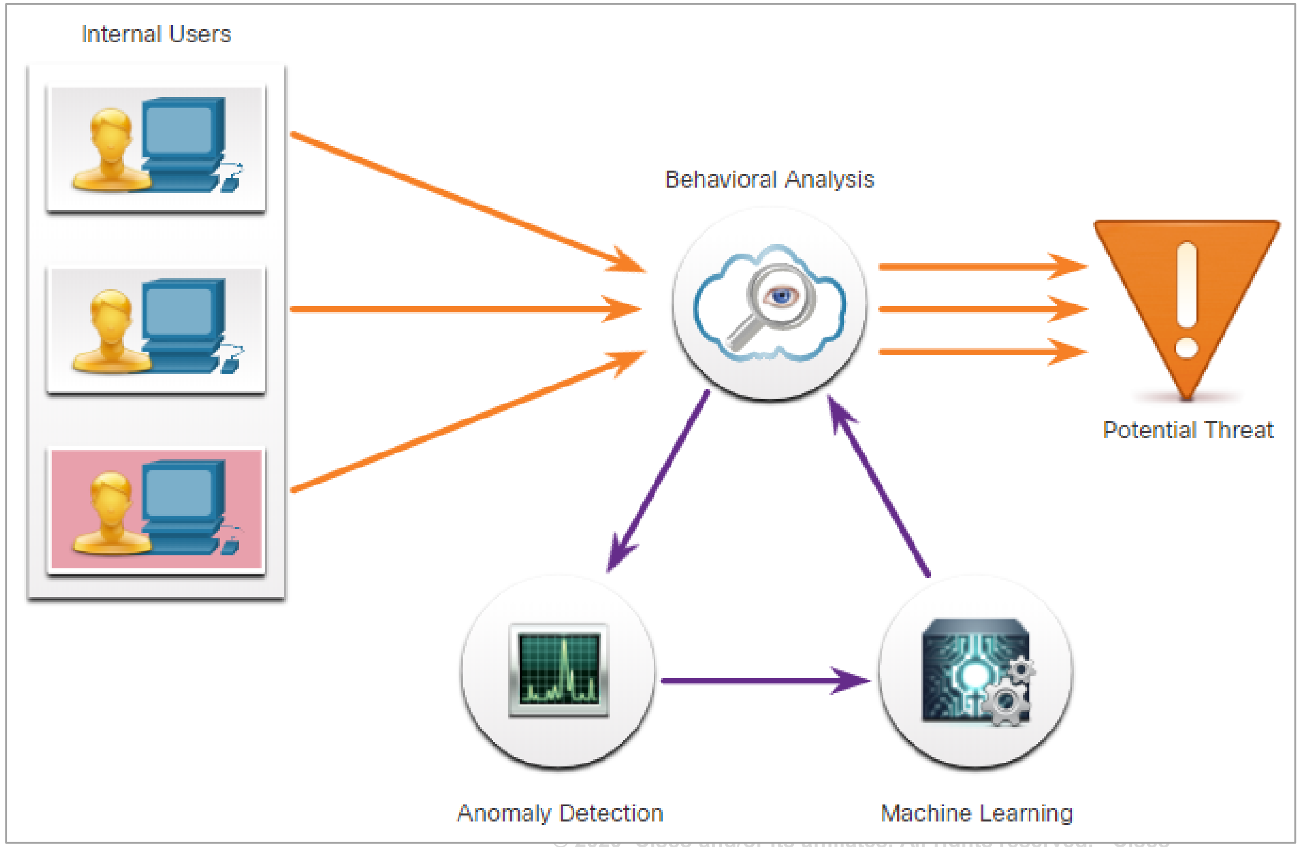
- The figure here shows the interface for the Network Analysis Monitor component of Cisco Prime Infrastructure system, which can display full packet captures.

Network Security 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.



architecture for Cisco Cognitive Threat Analytics

25.2 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 CLI execution will provide **visibility** into this type of incident.

End Device Logs

Host Logs (Contd.)

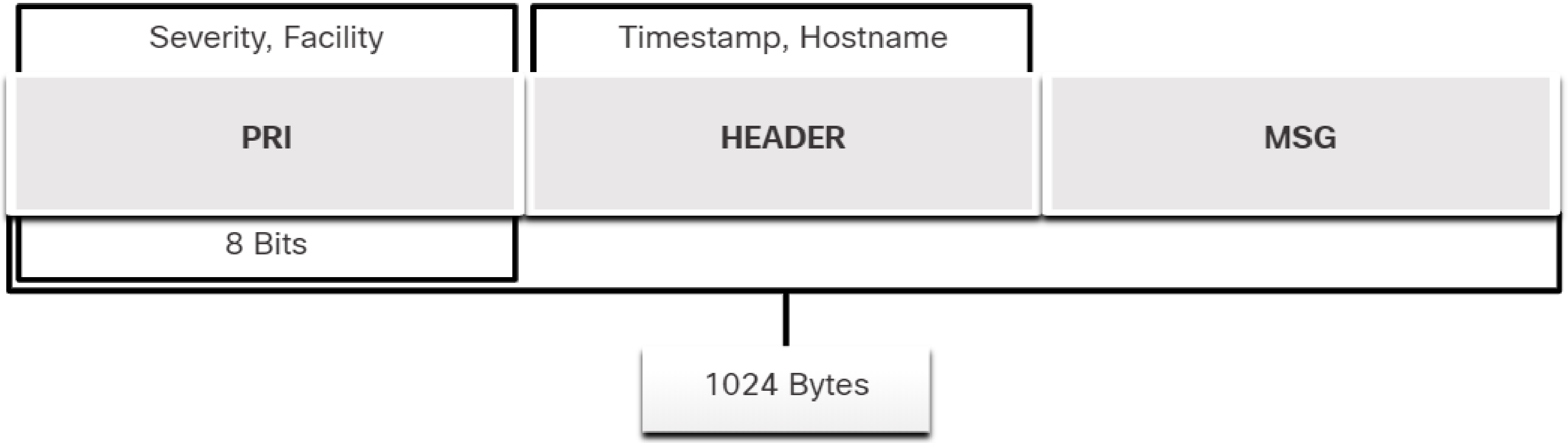
The table explains the meaning of the five Windows host log event

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.

End Device Logs

Syslog

- Syslog incudes
  - specifications for message formats
  - a client-server application structure
  - and network protocol.



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

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.
- Various operating systems have been found to utilize both facilities 9 and 15 for clock messages.

Facility Number	Facility Description	Facility Number	Facility Description
0	kernel messages	12	NTP subsystem
1	user-level messages	13	log audit
2	mail system	14	log alert
3	system daemons	15	clock daemon
4	**security/authorization messages	16	local use 0 (local0)
5	messages generated internally by Syslog	17	local use 1 (local1)
6	line printer subsystem	18	local use 2 (local2)
7	network news subsystem	19	local use 3 (local3)
8	UUCP subsystem	20	local use 4 (local4)
9	clock daemon	21	local use 5 (local5)
10	security/authorization messages	22	local use 6 (local6)
11	FTP daemon	23	local use 7 (local7)

End Device Logs

Syslog (Contd.)

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

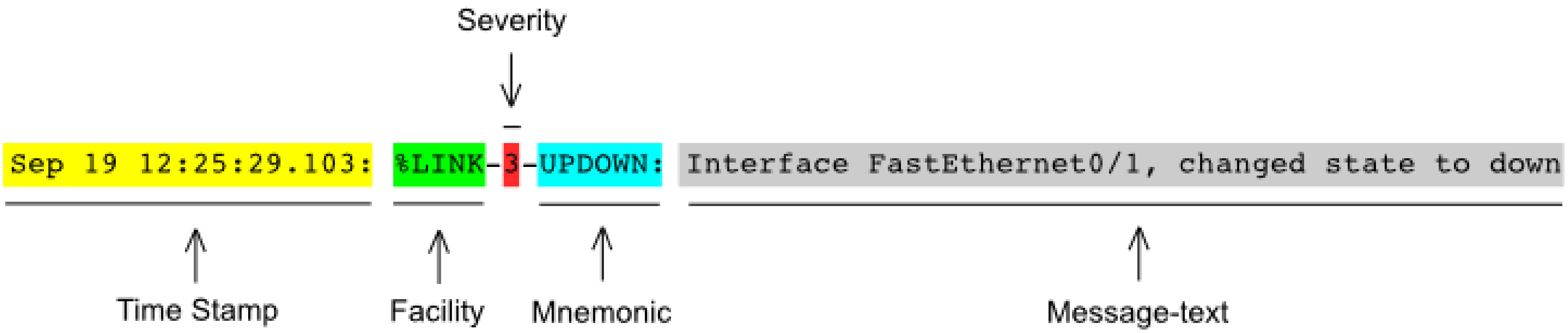
Priority = (Facility * 8) + Severity

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

The following is a list of RFCs that define the Syslog protocol:

- RFC 3195 *Reliable Delivery for Syslog*
- RFC 5424 *The Syslog Protocol*
- RFC 5425 *TLS Transport Mapping for Syslog*
- RFC 5426 *Transmission of Syslog Messages over UDP*
- RFC 5427 *Textual Conventions for Syslog Management*
- RFC 5848 *Signed Syslog Messages*
- RFC 6012 Datagram Transport Layer Security (DTLS) *Transport Mapping for Syslog*

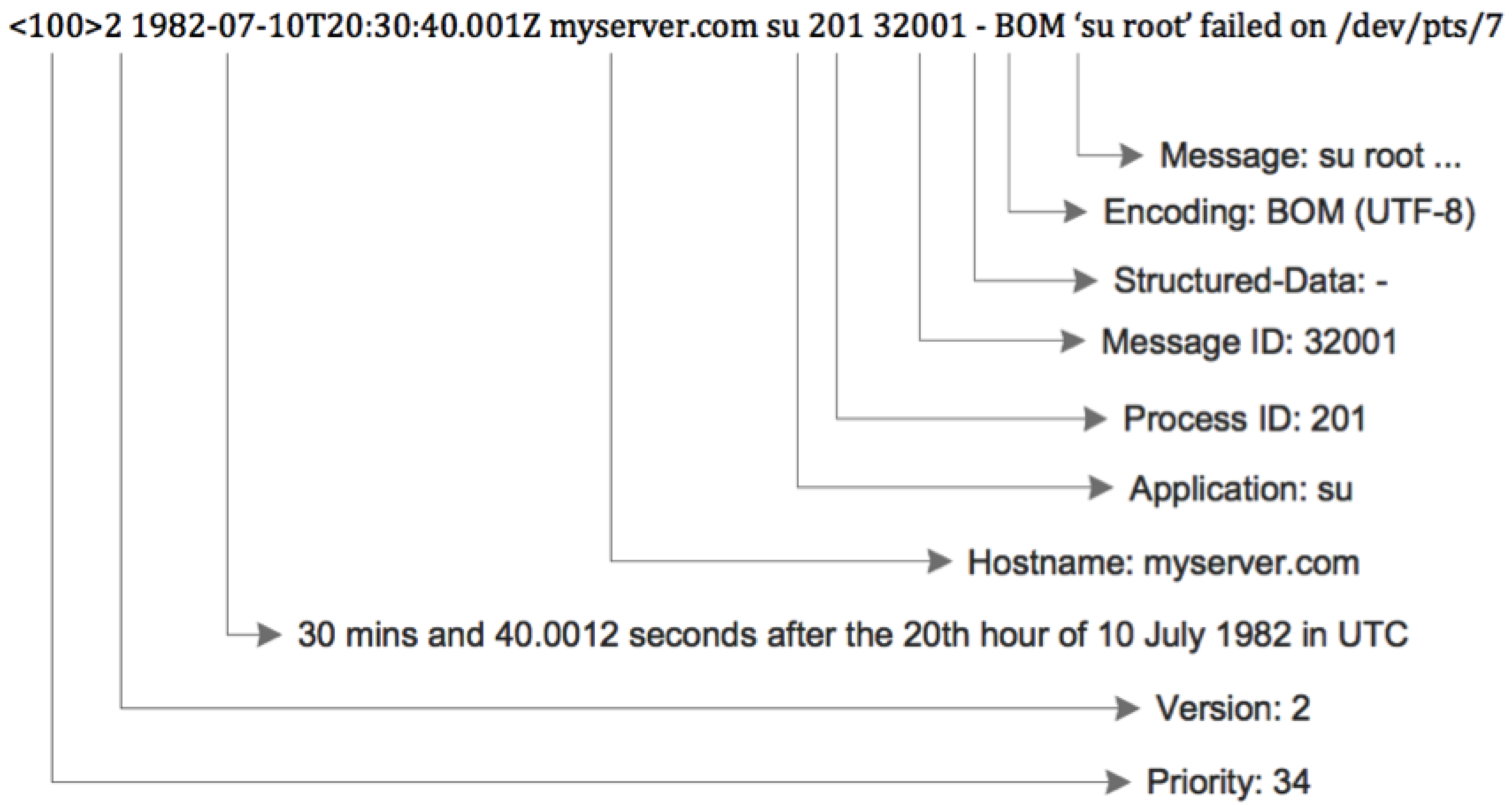
Syslog



```
Sep 19 12:25:29.103: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
```

Cisco IOS syslog message

Rapid7 syslog message



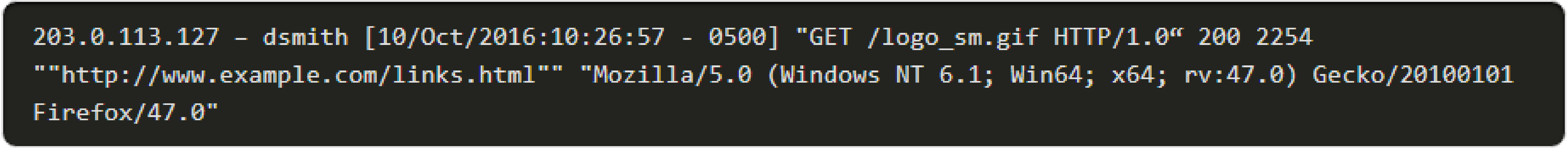
```
<100>2 1982-07-10T20:30:40.001Z myserver.com su 201 32001 - BOM ‘su root’ failed on /dev/pts/7
```

End Device Logs

Server Logs

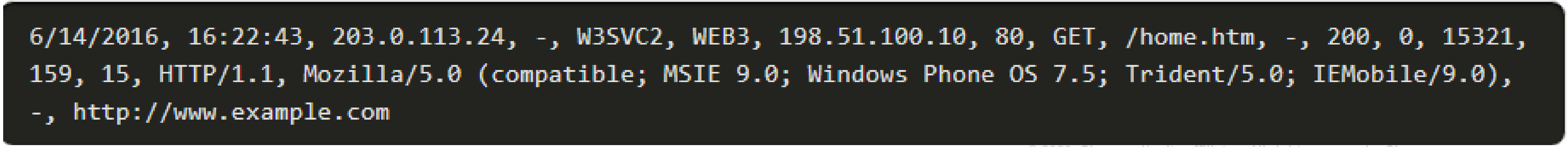
- essential source of data for NSM
- **DNS proxy server logs** which document all the DNS queries and responses that occur on the network are especially important.
- Two important log files are **Apache webserver access logs** and **Microsoft Internet Information Server (IIS) access logs**.

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

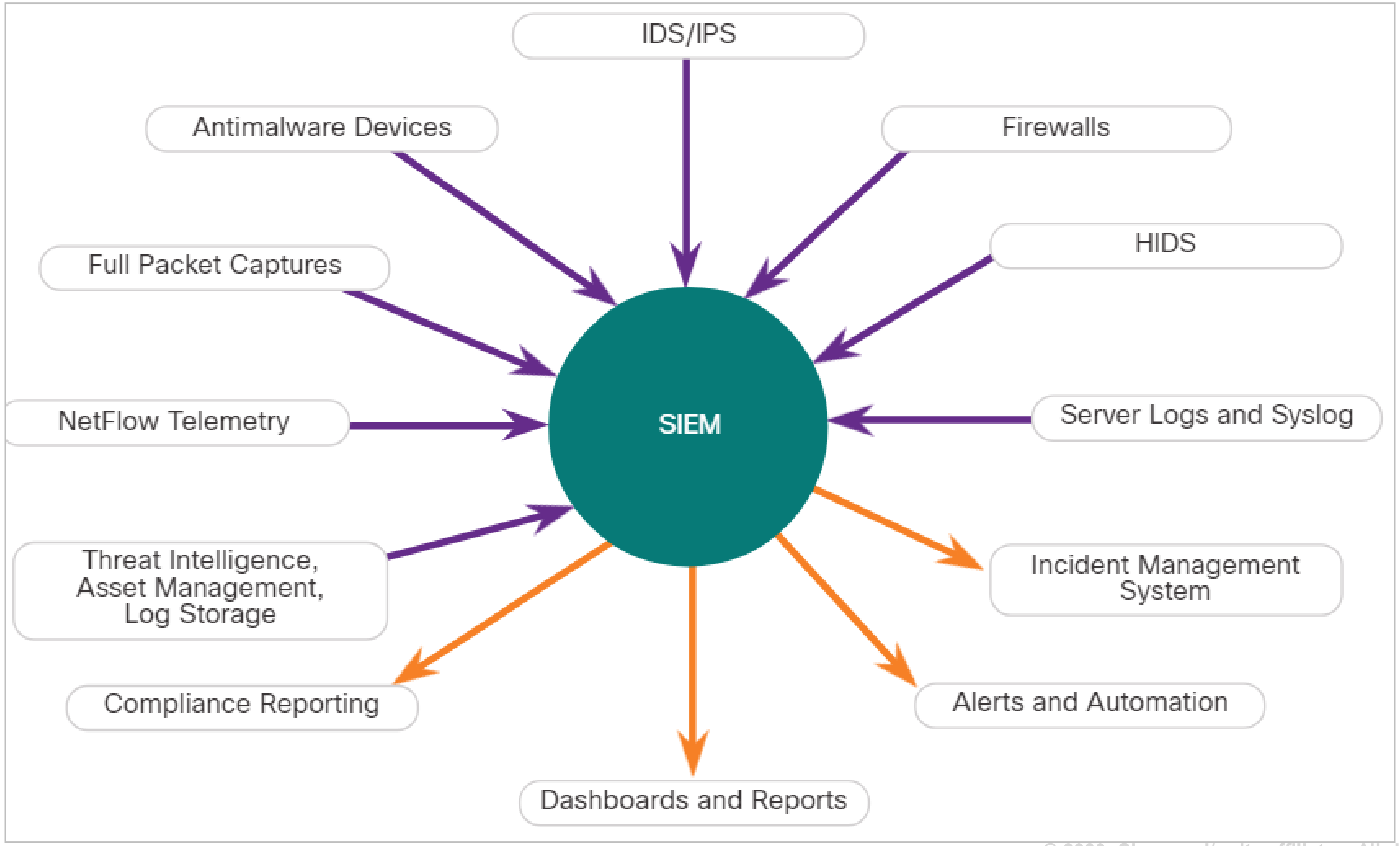


```
6/14/2016, 16:22:43, 203.0.113.24, -, W3SVC2, WEB3, 198.51.100.10, 80, GET, /home.htm, -, 200, 0, 15321,
159, 15, HTTP/1.1, Mozilla/5.0 (compatible; MSIE 9.0; Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0),
-, http://www.example.com
```

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:

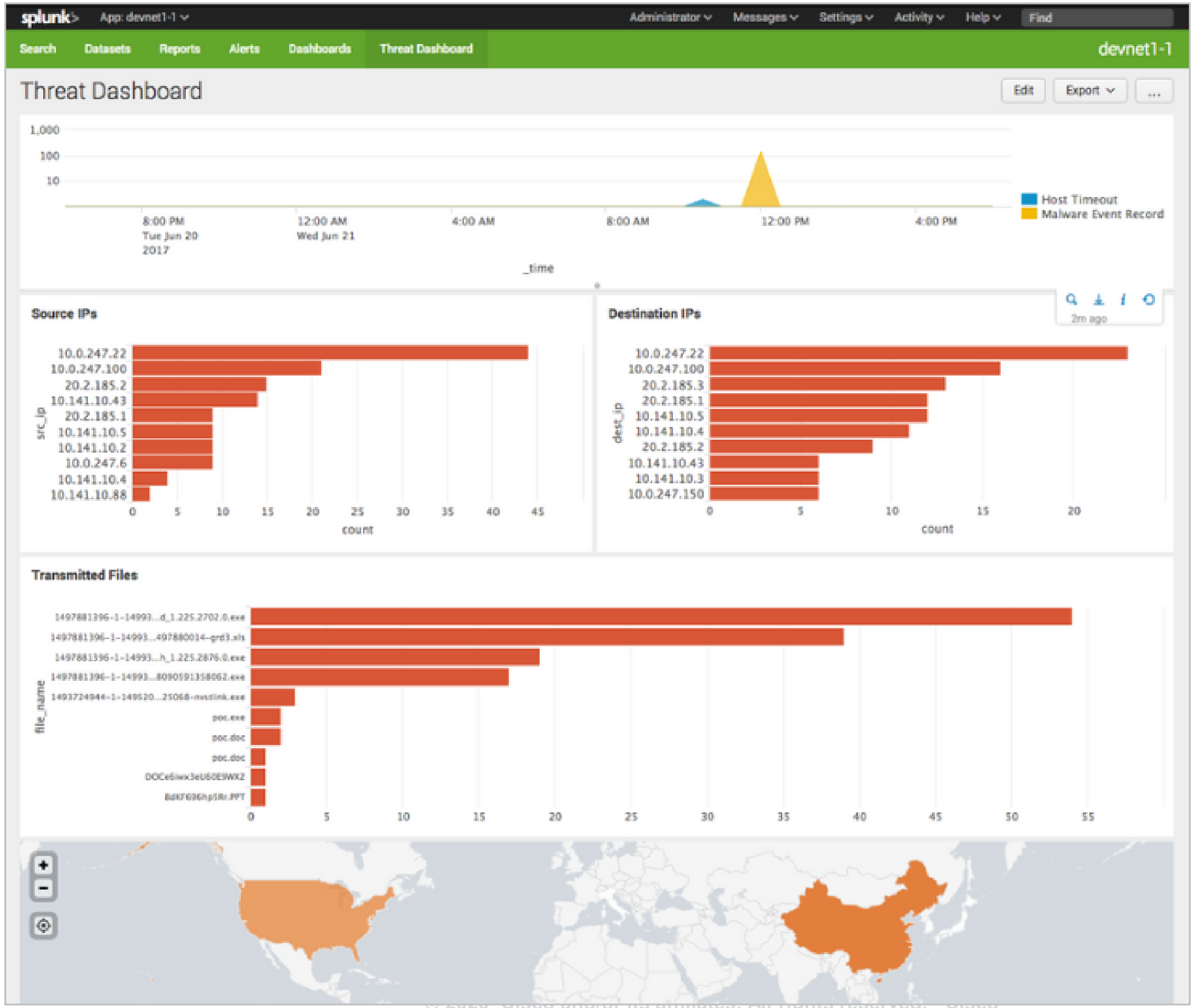
- **Log collection** – Event records from sources throughout the organization provide important forensic information and help to address compliance reporting requirements.
- **Normalization** – This maps log messages from different systems into a common data model, enabling the organization to connect and analyze related events, even if they are initially logged in different source formats.
- **Correlation** – This links logs and events from disparate *(rozdielne)* 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.
- 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** <u>can be integrated into a single platform</u>.
- Integrated security platforms go **<u>beyond</u> SIEM and SOAR** to unify multiple security technologies into a unified team.

Splunk Threat Dashboard



25.3 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.

Network Logs

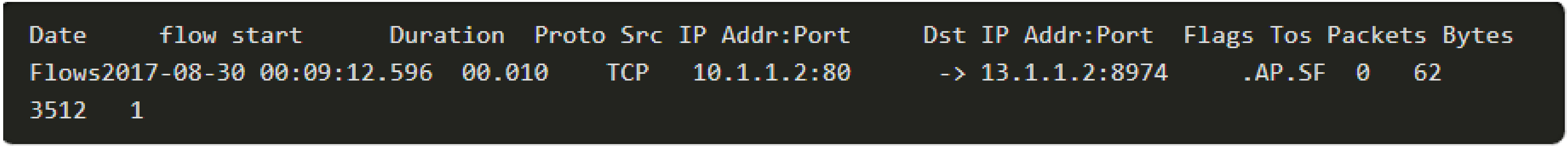
NetFlow

- 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.
  - 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.

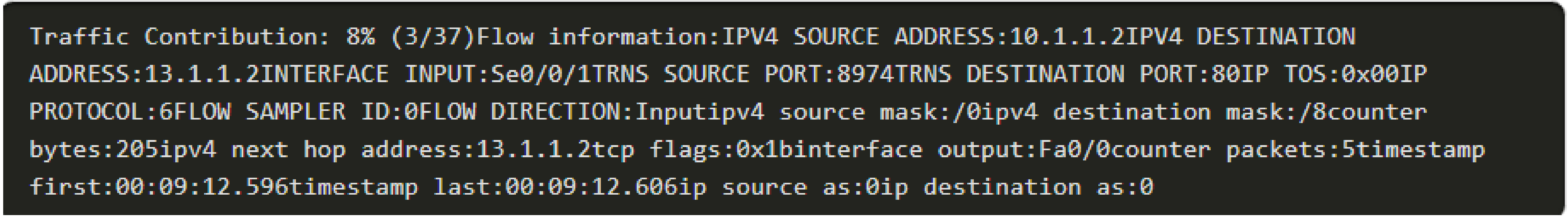
Network Logs

NetFlow (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 (AVC)

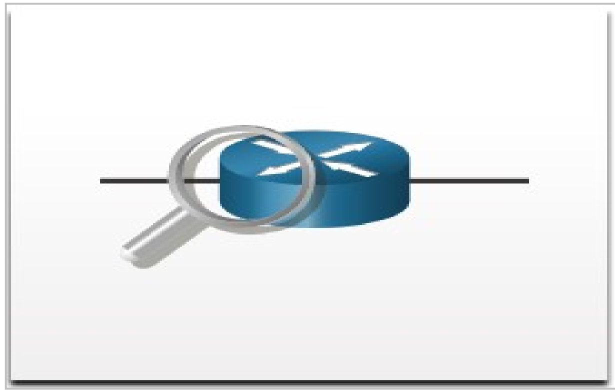
- combines multiple technologies:
  - to recognize
  - analyze
  - and control

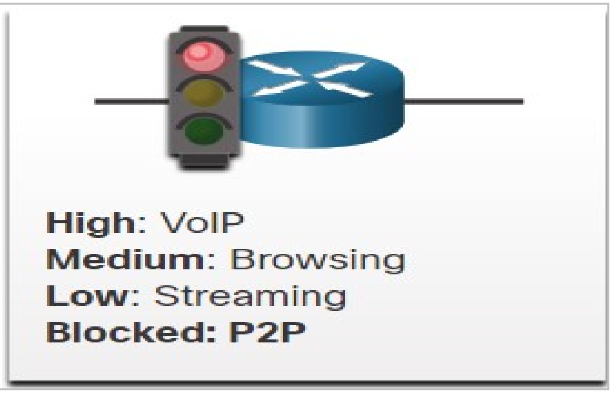
  over 1000 applications.

  - 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.

Network Logs

Application Visibility and Control (Contd.)





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

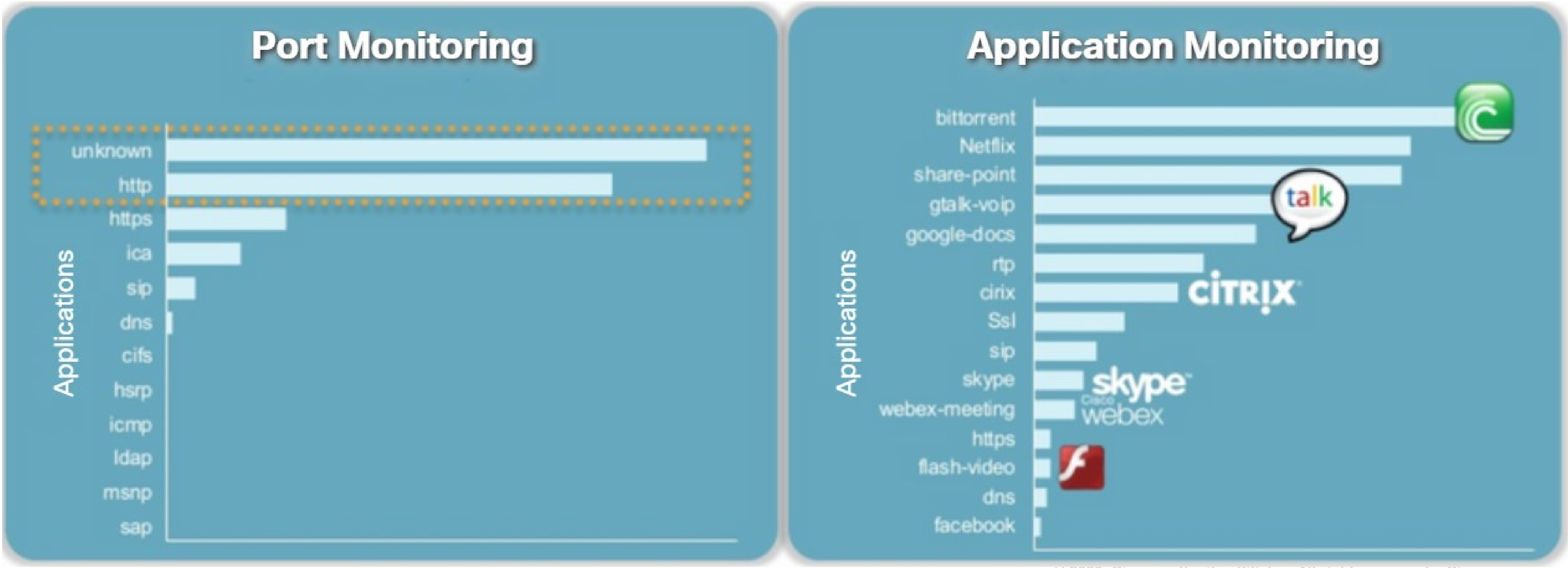
- Application prioritizarion
- Application bandwidth enforcement *(Vynútenie šírky pásma aplikácie)*

QoS

Application Visibility and Control (Contd.)

Port Monitoring vs. Application Monitoring

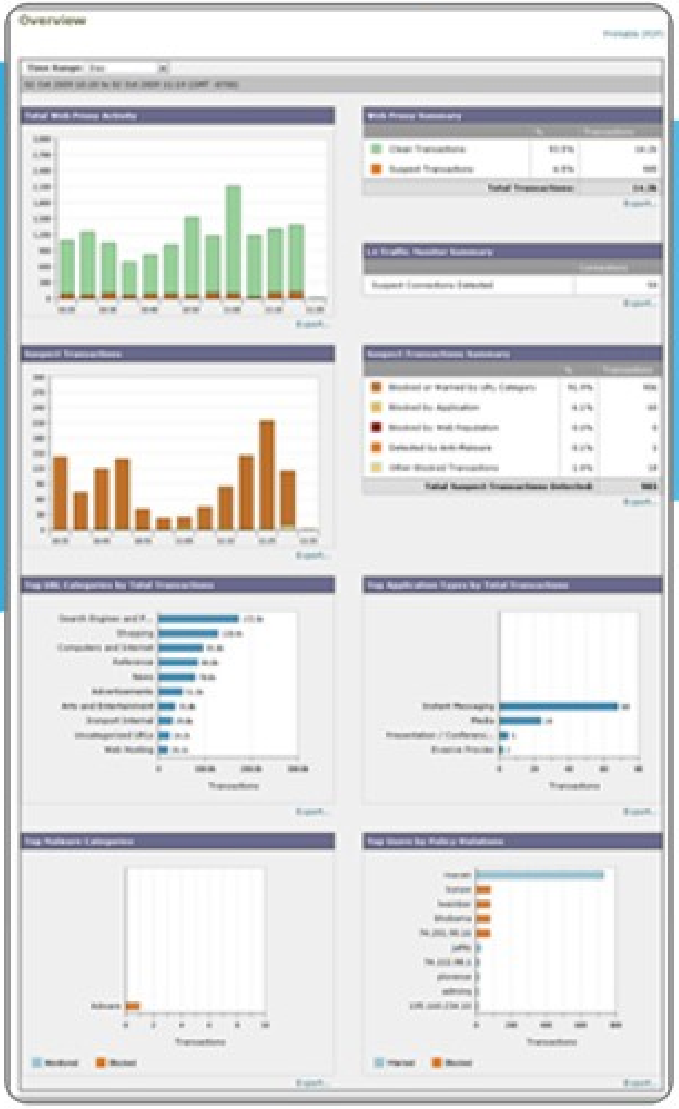
A management and reporting system analyzes and presents the application analysis data into dashboard reports for use by network monitoring personnel. Application usage can also be controlled through quality of service classification and policies based on the AVC information.



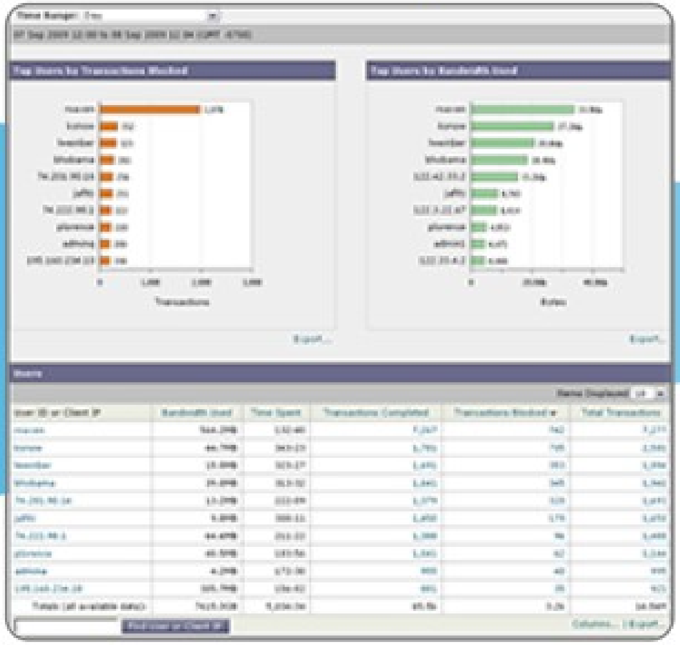
Network Logs

Content Filter Logs

“Overview” Reports



“Detailed” Reports

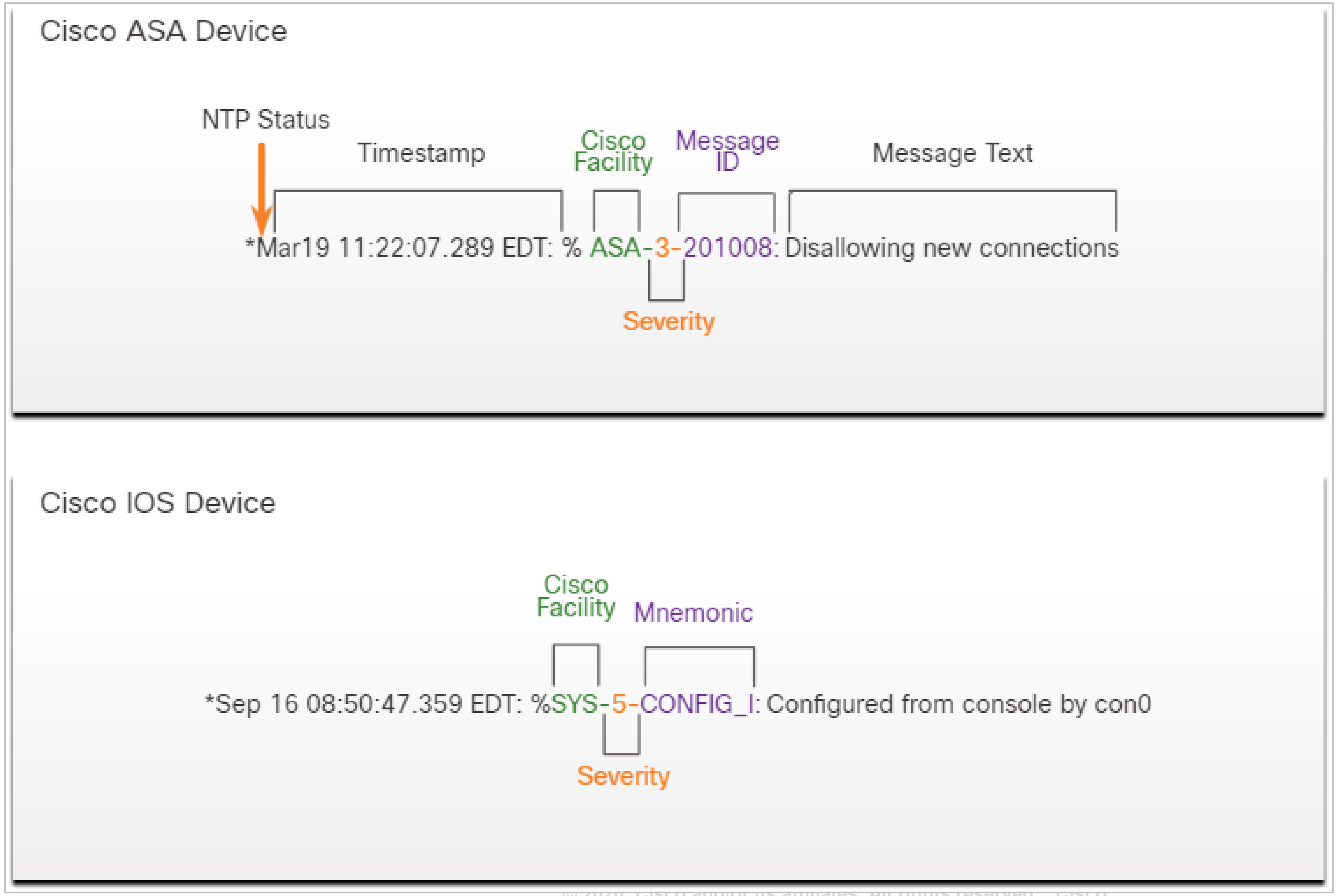


Targeted Search

- 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.

Logging from Cisco Devices

- Cisco security devices can be configured to submit events and alerts to security management platforms using SNMP or syslog.
- The figure shows a syslog message generated by a Cisco ASA device and a syslog message generated by a Cisco IOS device.
- There are two meanings used for the term facility in Cisco syslog messages.
- The first is the standard set of Facility values that were established by the syslog standards.
- **The other Facility value is assigned by Cisco and occurs <u>in the MSG part</u> of the syslog message.**



```
*Mar19 11:22:07.289 EDT: % ASA-3-201008: Disallowing new connections
```

```
*Sep 16 08:50:47.359 EDT: %SYS-5-CONFIG_I: Configured from console by con0
```

Network Logs

Proxy Logs

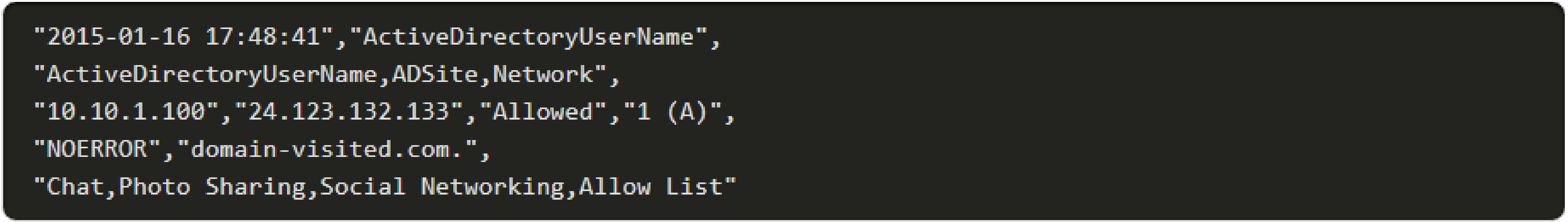
- Proxy servers, such as those used **for web and DNS requests,** contain valuable logs that are a primary source of data for NSM.
- The proxy server requests the resources and returns them to the client and generates logs of all requests and responses.
- These logs can then be analyzed to determine 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.

Proxy Logs (Contd.)

Cisco Umbrella (suite of security products)

- formerly OpenDNS
- offers a hosted DNS service
- that extends the capability of DNS to include security enhancements.
- applies many more resources to managing DNS than most organizations can afford.
    - functions in part as a DNS super proxy in this regard.
- 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"
```

Next-Generation Firewalls

- extend network security beyond IP addresses and Layer 4 port numbers
  - to the **application layer and beyond**.
- 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.
- Cisco NGFW use **Firepower** Services
  - consolidate multiple security layers into a single platform.
  - include application visibility and control
  - Firepower Next-Generation IPS (NGIPS)
  - reputation and category-based URL filtering
  - Advanced Malware Protection (AMP).

Next-Generation Firewalls (Contd.)

Common NGFW events include:

- Connection Event
- Intrusion Event *(prienik)*
- 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

25.4 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.

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.

Chapter 26
Evaualting Alerts (in Security Onion)

Module Objective: Explain the process of evaluating alerts

Topic Title	Topic Objective
Source of Alerts	Identify the structure of alerts.
Overview of Alert Evaluation	Explain how alerts are classified.

26.1 Sources of Alerts

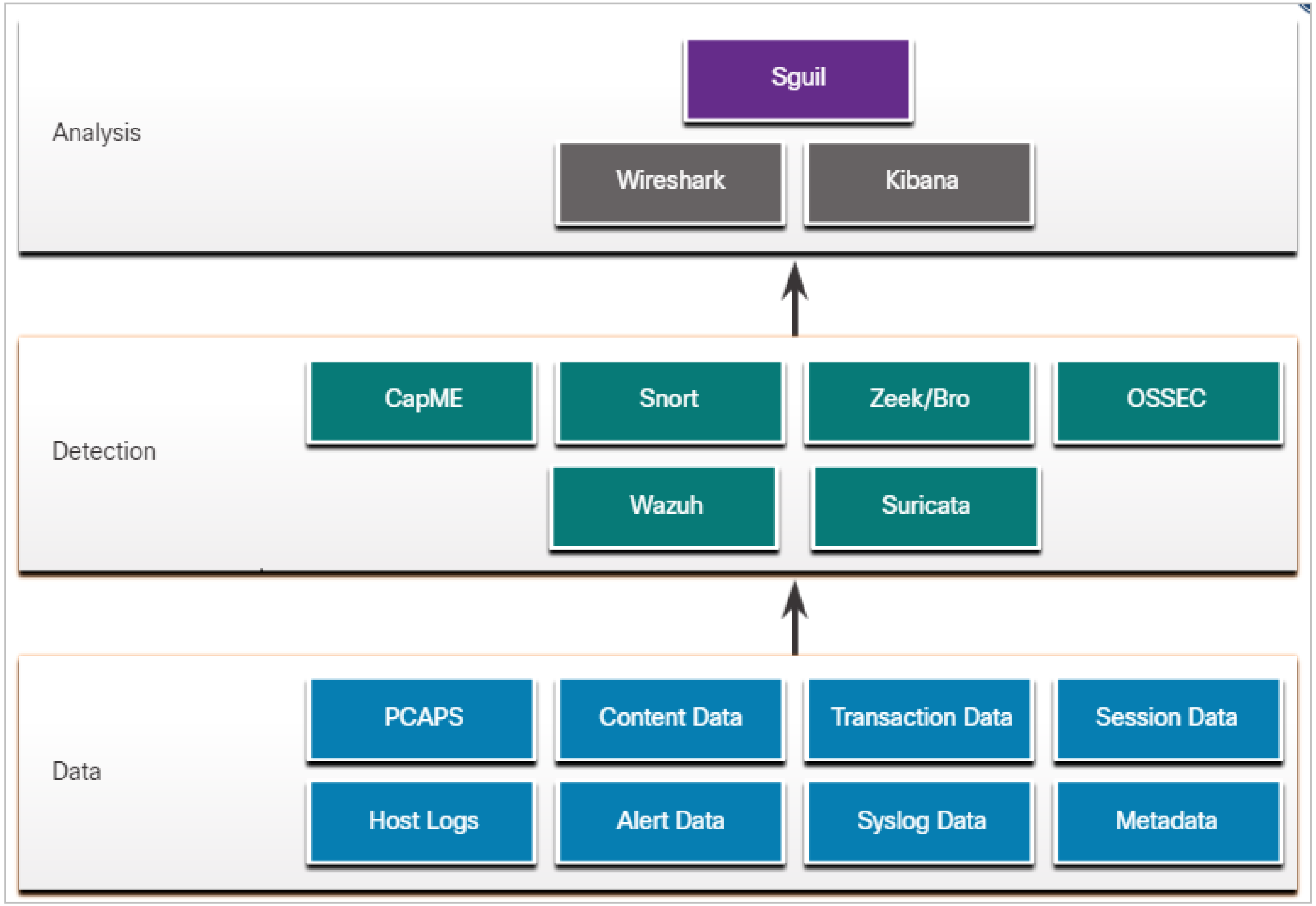
Evaluating Alerts

Security Onion

- open-source suite of NSM tools that run on an Ubuntu **Linux** distribution.
- provides **three core func**tions for the cybersecurity analyst such as:
    - RAW: full packet capture and data types
    - NIDS, HIDS: network-based and host-based intrusion detection systems
    - ALERTS: alert analyst tools.
- Security Onion can be installed as
    - **standalone** installation
    - or as a **sensor** and **server** platform.
- Some components of Security Onion are owned and maintained by corporations, such as Cisco and Riverbed Technologies, but are made available as **open source**.

Detection Tools for Collecting Alert Data

- Security Onion contains many components. It is an integrated environment which is designed to simplify the deployment of a comprehensive NSM solution.
- The figure illustrates the way in which components of the Security Onion work together.



A Security Onion Architecture

Detection Tools for Collecting Alert Data (Contd.)

The following table lists the detection tools of the Security Onion:

Components	Description
CapME	This is a web application that allows viewing of pcap transcripts rendered *(vykreslený)* with the tcpflow or Zeek tools.
Snort	This is a Network Intrusion Detection System (NIDS). It is an important source of **alert data** that is **indexed** in the Sguil analysis tool.
Zeek	Formerly known as Bro. This is a NIDS that uses more of a behavior-based approach to intrusion detection.
OSSEC	This is a host-based intrusion detection system (HIDS) that is integrated into Security Onion.
Wazuh	It is a full-featured solution that provides a broad spectrum of endpoint protection mechanisms including **host logfile analysis**, **file integrity monitoring**, **vulnerability detection**, **configuration assessment**, and **incident response**.
Suricata	This is a NIDS that uses a signature-based approach. It can also be used for inline intrusion prevention.

Analysis Tools

Security Onion integrates these various types of data and Intrusion Detection System (IDS) logs into a single platform through the following tools:

- **Sguil:** This provides a high-level **console for investigating security alerts** from a wide variety of sources. Sguil serves as a starting point in the investigation of security alerts. Many data sources are available by pivoting directly from Sguil to other tools.
- **Kibana:** It is an interactive dashboard **interface to Elasticsearch data**. It allows querying of NSM data and provides flexible visualizations of that data. It is possible to **pivot from Sguil directly** into Kibana to see contextualized displays.
- **Wireshark:** It is a packet capture application that is integrated into the Security Onion suit. It **can be opened directly from other tools** and display full packet captures relevant to an analysis.
- **Zeek:** This is a network traffic analyzer that serves as a security monitor. It inspects all traffic on a network segment and enables in-depth analysis of that data**. Pivoting from Sguil into Zeek** provides access to very accurate **transaction logs**, **file content**, and **customized out**put.

Alert Generation

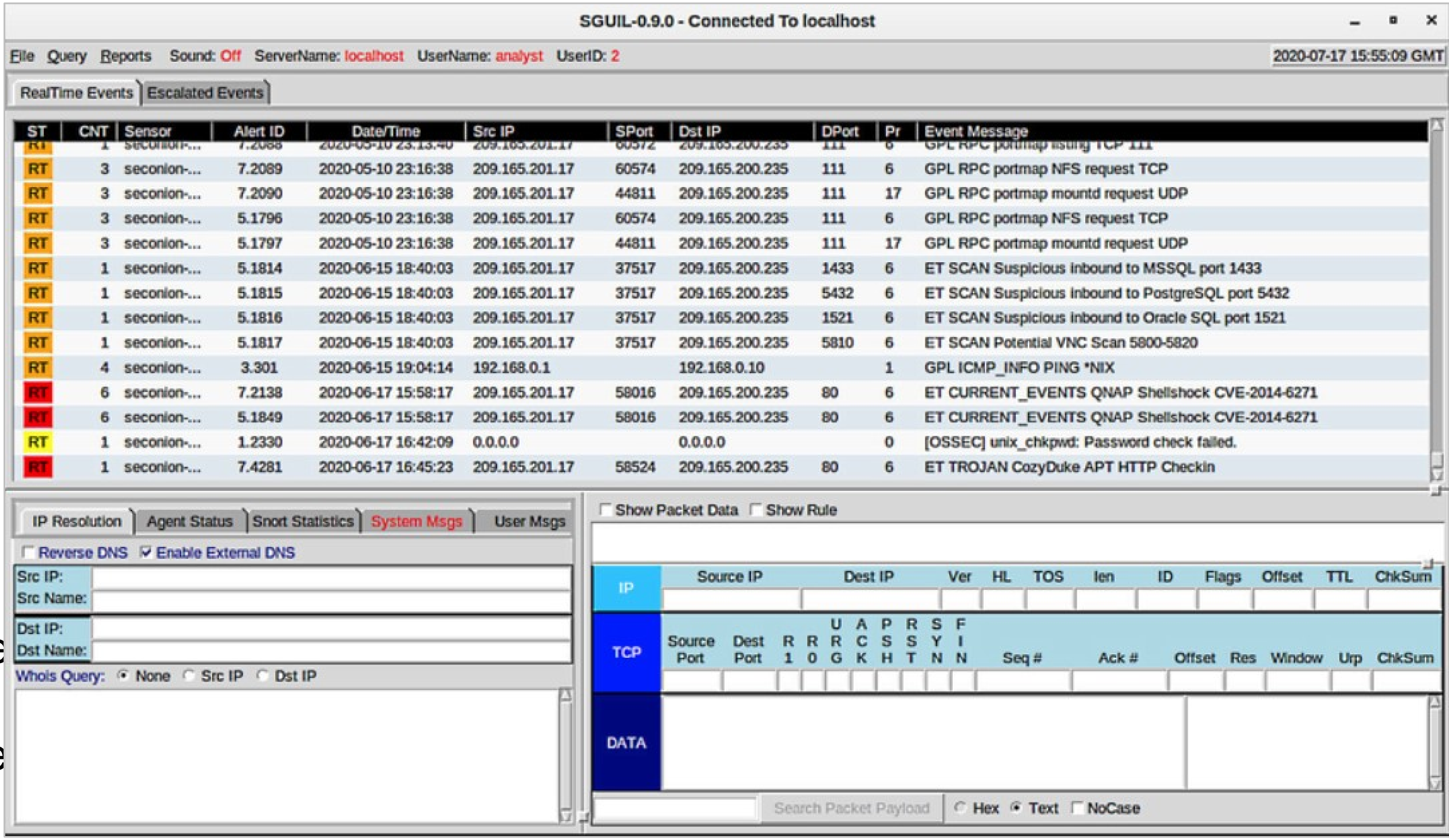
- Security alerts are notification messages that are generated by NSM tools, systems, and security devices. Alerts can come in many forms depending on the source.
- In Security Onion, Sguil provides a console that integrates alerts from multiple sources into a timestamped queue.
- A cybersecurity analyst works through the **security queue** investigating, classifying, escalating (T1, T2, T3, T4), or retiring *(rušiť)* alerts.
- Alerts will generally include five-tuples information, as well as timestamps and information identifying which device or system generated the alert.
  - **SrcIP** - the source IP address for the event.
  - **SPort** - the source (local) Layer 4 port for the event.
  - **DstIP** - the destination IP for the event.
  - **DPort** - the destination Layer 4 port for the event.
  - **Pr** - the IP protocol number for the event.

Evaluating Alerts

Alert Generation (Contd.)

The figure shows the Sguil application window with the queue of alerts that are waiting to be investigated in the top portion of the interface. The fields available for the real-time events are as follows:

- **ST** - This is the **status** of the event. The event is color-coded by priority based on the category of the alert. There are four priority levels: very low, low, medium, and high and the colors range from light yellow to red as the priority increases.
- **CNT** - This is the count for the number of times this event has been detected for the same source and destination IP address. The system has determined that this set of events is correlated.
- **Sensor** - This is the agent reporting the event. The available sensors and their identifying numbers can be found in the Agent Status tab of the pane which appears below the events window on the left.



SGUIL-0.9.0 - Connected To localhost

Sound: Off ServerName: localhost UserName: analyst UserID: 2

2020-07-17 15:55:09 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion-...	7.2088	2020-05-10 23:13:40	209.165.201.17	60572	209.165.200.235	111	6	GPL RPC portmap listing TCP 111
RT	3	seconion-...	7.2089	2020-05-10 23:16:38	209.165.201.17	60574	209.165.200.235	111	6	GPL RPC portmap NFS request TCP
RT	3	seconion-...	7.2090	2020-05-10 23:16:38	209.165.201.17	44811	209.165.200.235	111	17	GPL RPC portmap mountd request UDP
RT	3	seconion-...	5.1796	2020-05-10 23:16:38	209.165.201.17	60574	209.165.200.235	111	6	GPL RPC portmap NFS request TCP
RT	3	seconion-...	5.1797	2020-05-10 23:16:38	209.165.201.17	44811	209.165.200.235	111	17	GPL RPC portmap mountd request UDP
RT	1	seconion-...	5.1814	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	1433	6	ET SCAN Suspicious inbound to MSSQL port 1433
RT	1	seconion-...	5.1815	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	5432	6	ET SCAN Suspicious inbound to PostgreSQL port 5432
RT	1	seconion-...	5.1816	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	1521	6	ET SCAN Suspicious inbound to Oracle SQL port 1521
RT	1	seconion-...	5.1817	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	5810	6	ET SCAN Potential VNC Scan 5800-5820
RT	4	seconion-...	3.301	2020-06-15 19:04:14	192.168.0.1		192.168.0.10		1	GPL ICMP_INFO PING *NIX
RT	6	seconion-...	7.2138	2020-06-17 15:58:17	209.165.201.17	58016	209.165.200.235	80	6	ET CURRENT_EVENTS QNAP Shellshock CVE-2014-6271
RT	6	seconion-...	5.1849	2020-06-17 15:58:17	209.165.201.17	58016	209.165.200.235	80	6	ET CURRENT_EVENTS QNAP Shellshock CVE-2014-6271
RT	1	seconion-...	1.2330	2020-06-17 16:42:09	0.0.0.0		0.0.0.0		0	[OSSEC] unix_chkpwd: Password check failed.
RT	1	seconion-...	7.4281	2020-06-17 16:45:23	209.165.201.17	58524	209.165.200.235	80	6	ET TROJAN CozyDuke APT HTTP Checkin

□ Reverse DNS ☑ Enable External DNS

Whois Query: ● None ○ Src IP ○ Dst IP

□ Show Packet Data □ Show Rule

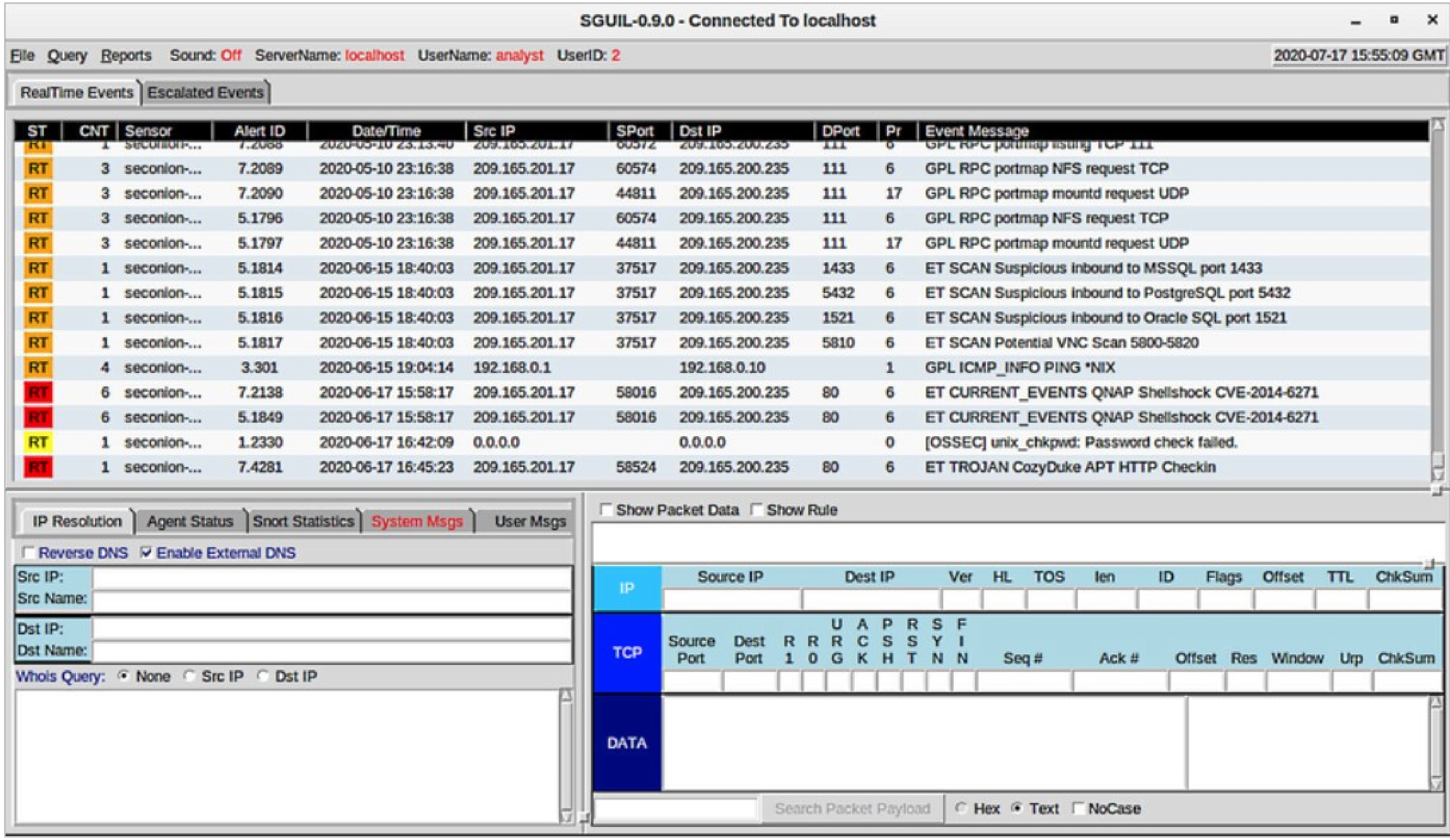
○ Hex ● Text □ NoCase

Sguil Window

Evaluating Alerts

Alert Generation (Contd.)

- **Alert ID** - This two-part number represents the sensor that has reported the problem and the event number for that sensor.
- **Date/Time** - This is the timestamp for the event. In the case of correlated events, it is the timestamp for the first event.
- **Event Message** - This is the identifying text for the event. This is configured in the rule that triggered the alert. The associated rule can be viewed in the right-hand pane, just above the packet data. To display the rule, the **Show Rule** checkbox must be selected.



SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2 2020-07-17 15:55:09 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion-...	7.2088	2020-05-10 23:13:40	209.165.201.17	60572	209.165.200.235	111	6	GPL RPC portmap listing TCP 111
RT	3	seconion-...	7.2089	2020-05-10 23:16:38	209.165.201.17	60574	209.165.200.235	111	6	GPL RPC portmap NFS request TCP
RT	3	seconion-...	7.2090	2020-05-10 23:16:38	209.165.201.17	44811	209.165.200.235	111	17	GPL RPC portmap mountd request UDP
RT	3	seconion-...	5.1796	2020-05-10 23:16:38	209.165.201.17	60574	209.165.200.235	111	6	GPL RPC portmap NFS request TCP
RT	3	seconion-...	5.1797	2020-05-10 23:16:38	209.165.201.17	44811	209.165.200.235	111	17	GPL RPC portmap mountd request UDP
RT	1	seconion-...	5.1814	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	1433	6	ET SCAN Suspicious inbound to MSSQL port 1433
RT	1	seconion-...	5.1815	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	5432	6	ET SCAN Suspicious inbound to PostgreSQL port 5432
RT	1	seconion-...	5.1816	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	1521	6	ET SCAN Suspicious inbound to Oracle SQL port 1521
RT	1	seconion-...	5.1817	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	5810	6	ET SCAN Potential VNC Scan 5800-5820
RT	4	seconion-...	3.301	2020-06-15 19:04:14	192.168.0.1		192.168.0.10		1	GPL ICMP_INFO PING *NIX
RT	6	seconion-...	7.2138	2020-06-17 15:58:17	209.165.201.17	58016	209.165.200.235	80	6	ET CURRENT_EVENTS QNAP Shellshock CVE-2014-6271
RT	6	seconion-...	5.1849	2020-06-17 15:58:17	209.165.201.17	58016	209.165.200.235	80	6	ET CURRENT_EVENTS QNAP Shellshock CVE-2014-6271
RT	1	seconion-...	1.2330	2020-06-17 16:42:09	0.0.0.0		0.0.0.0		0	[OSSEC] unix_chkpwd: Password check failed.
RT	1	seconion-...	7.4281	2020-06-17 16:45:23	209.165.201.17	58524	209.165.200.235	80	6	ET TROJAN CozyDuke APT HTTP Checkin

☐ Reverse DNS ☑ Enable External DNS

Whois Query: ● None ○ Src IP ○ Dst IP

☐ Show Packet Data ☐ Show Rule

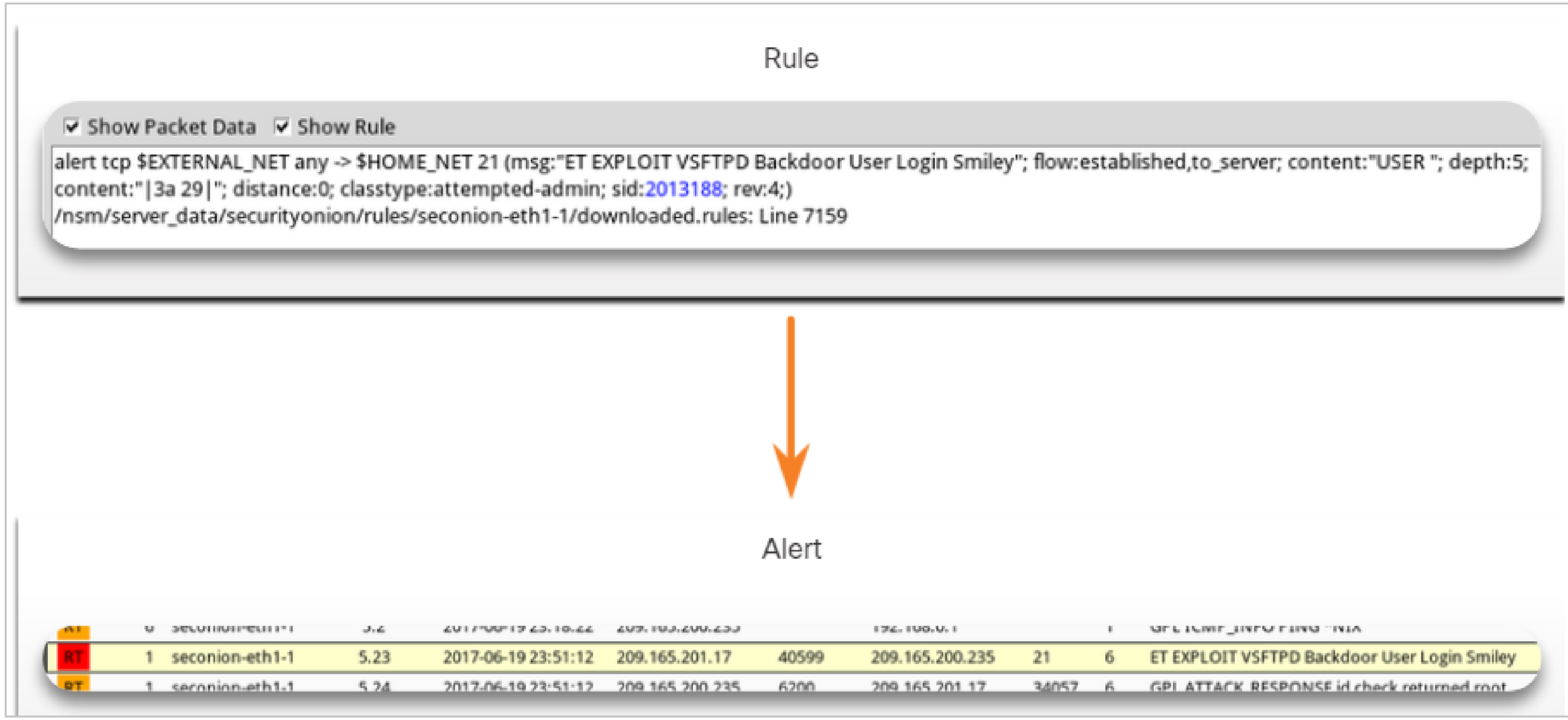
○ Hex ● Text ☐ NoCase

Sguil Window

Evaluating Alerts

Rules and Alerts

- Alerts can come from a number of sources:
  - **NIDS** - Snort, Zeek, and Suricata
  - **HIDS** - OSSEC, Wazuh
  - **Asset management and monitoring** - Passive Asset Detection System (PADS)
  - **HTTP, DNS, and TCP transactions** - Recorded by Zeek and pcaps
  - **Syslog messages** - Multiple sources



```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET EXPLOIT VSFTPD Backdoor User Login Smiley"; flow:established,to_server; content:"USER "; depth:5;
content:"|3a 29|"; distance:0; classtype:attempted-admin; sid:2013188; rev:4;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules: Line 7159
```

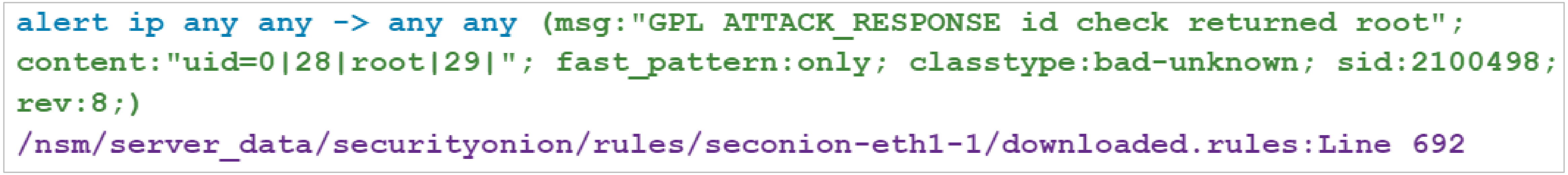
```
RT   0  seconion-eth1-1  5.2   2017-06-19 23:18:22  209.165.200.235          192.168.0.1            1  GPL ICMP_INFO PING *NIX
RT   1  seconion-eth1-1  5.23  2017-06-19 23:51:12  209.165.201.17   40599  209.165.200.235  21     6  ET EXPLOIT VSFTPD Backdoor User Login Smiley
RT   1  seconion-eth1-1  5.24  2017-06-19 23:51:12  209.165.200.235  6200   209.165.201.17   34057  6  GPL ATTACK_RESPONSE id check returned root
```

- The information found in the alerts that are displayed in Sguil will differ in message format because they come from different sources.
- The Sguil alert in the figure was triggered by a rule that was configured in Snort.

Evaluating Alerts

Snort Rule Structure

Snort rules consist of two sections, as shown in the figure: the rule header and the rule options. Rule Location is sometimes added by Sguil.



```
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;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

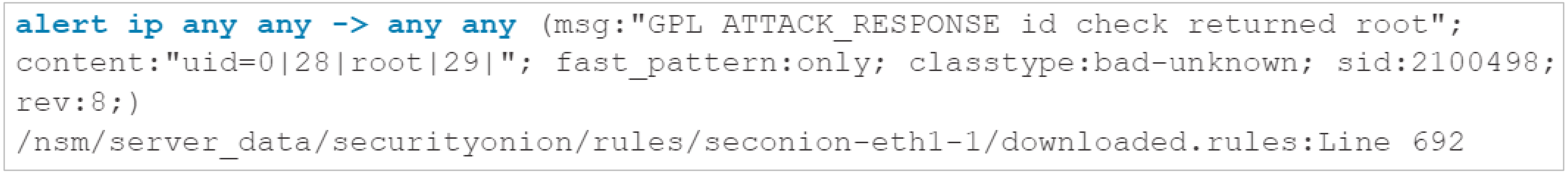
Component	Example (shortened…)	Explanation
rule header	alert ip any any -> any any	Contains the action to be taken, source and destination addresses and port, and the direction of traffic flow
rule options	(msg:"GPL ATTACK_RESPONSE ID CHECK RETURNED ROOT";…)	Includes the message to be displayed, details of packet content, alert type, source ID, and additional details, such as a reference for the rule or vulnerability
rule location	/nsm/server_data/securityonion/rules/…	Added by Sguil to indicate the location of the rule in the Security Onion file structure and in the specified rule file

Evaluating Alerts

Snort Rule Structure (Contd.)

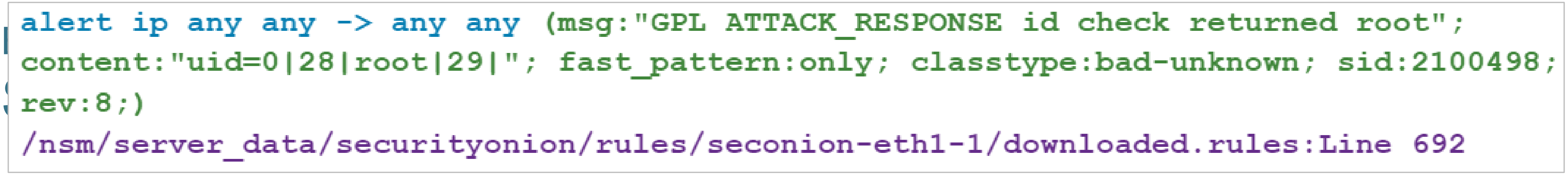
The Rule Header

The rule header contains the action, protocol, addressing, and port information, as shown in the figure. The structure of the header portion is consistent between Snort alert rule. Snort can be configured to use variables to represent internal and external IP addresses.



```
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;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

Component	Explanation
alert	the action to be taken is to issue an alert, other actions are log and pass
ip	the protocol
any any	the specified source is any IP address and any Layer 4 port
->	the direction of flow is from the source to the destination
any any	the specified destination is any IP address and any Layer 4 port



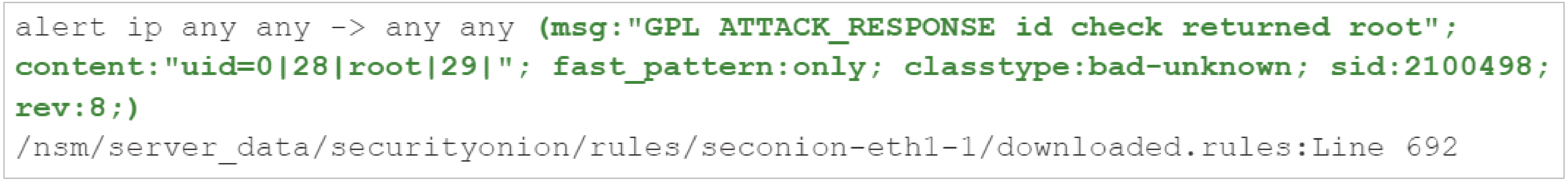
```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;
rev:8;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

Snort Rule Options

- The structure of the options section of the rule is variable. It is the portion of the rule that is enclosed in parenthesis, as shown in the figure. It contains the text message that identifies the alert. It also contains metadata about the alert, such as a URL.
- Snort rule messages may include the source of the rule. Three common sources for Snort rules are:
  - **GPL** - Older Snort rules that were created by Sourcefire and distributed under a GPLv2. The GPL ruleset is not Cisco Talos certified. The GPL ruleset can be downloaded from the Snort website, and it is included in Security Onion.
  - **ET** - Snort rules from Emerging Threats which is a collection point for Snort rules from multiple sources. The ET ruleset contains rules from multiple categories. A set of ET rules is included with Security Onion. Emerging Threats is a division of Proofpoint, Inc.
  - **VRT** - These rules are immediately available to subscribers and are released to registered users 30 days after they were created, with some limitations. They are now created and maintained by Cisco Talos.

Evaluating Alerts

Snort Rule Structure (Contd.)



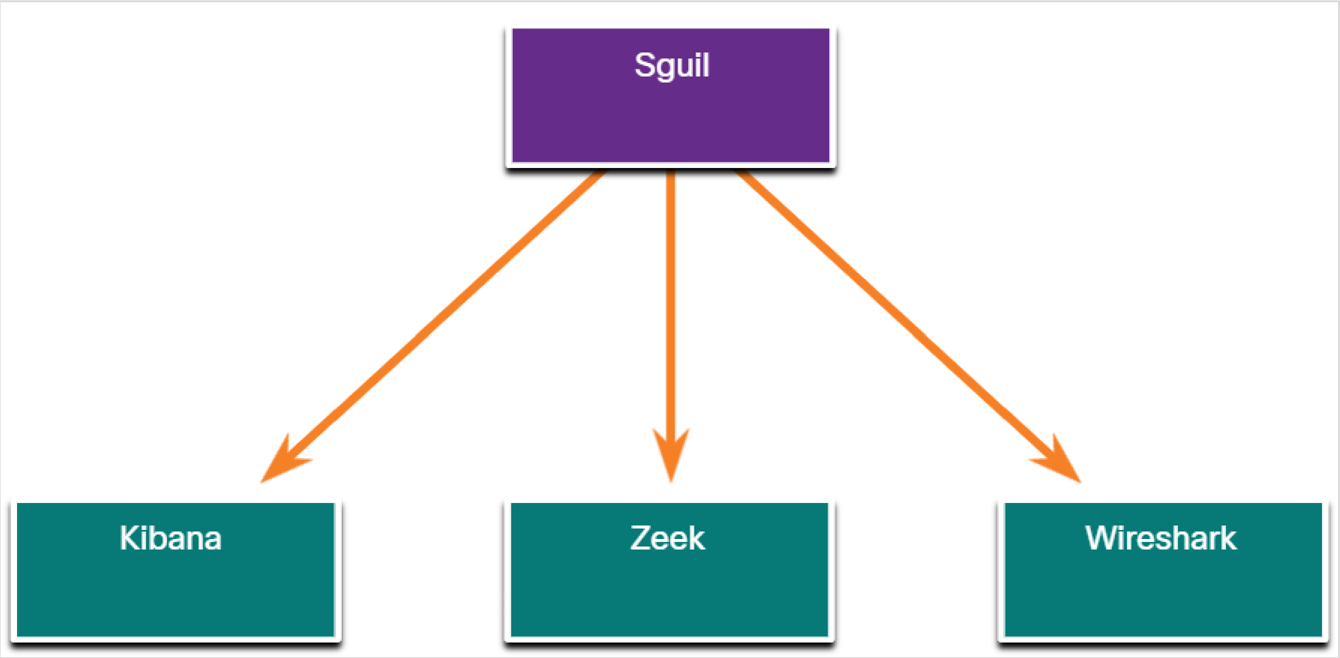
```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;
rev:8;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

Component	Explanation
msg:	Text that describes the alert.
content:	Refers to content of the packet. In this case, an alert will be sent if the literal text “uid=0(root)” appears anywhere in the packet data. Values specifying the location of the text can be provided.
reference:	This is not shown in the figure. It is often a link to a URL that provides more information on the rule. In this case, the sid is hyperlinked to the source of the rule on the internet.
classtype:	A category for the attack. Snort includes a set of default categories that have one of four priority values.
sid:	A unique numeric identifier for the rule.
rev:	The revision of the rule that is represented by the sid.

26.2 Overview of Alert Evaluation

The Need for Alert Evaluation

- The threat landscape is constantly changing as new vulnerabilities and threats are discovered. As user and organizational needs change, so also does the attack surface.
- Threat actors have learned how to quickly vary features of their exploits in order to evade detection.
- It is better to have alerts that are sometimes generated by innocent *(nevinná)* traffic, than it is to have rules that miss malicious traffic.
- It is necessary to have skilled cybersecurity analysts investigate alerts to determine if an exploit has actually occurred.
- Tier 1 cybersecurity analysts will work through queues of alerts in a tool like Sguil, pivoting to tools like Zeek, Wireshark, and Kibana to verify that an alert represents an actual exploit.



Primary Tools for the Tier 1 Cybersecurity Analyst

Evaluating Alerts

- Security incidents are classified **using a scheme** borrowed from medical diagnostics. This classification scheme is used to guide actions and to evaluate diagnostic procedures. The concern is that either **diagnosis** can be accurate, or true, or inaccurate, or false.
- In network security analysis, the cybersecurity analyst **is presented with an alert**. The cybersecurity analyst needs to **determine if this diagnosis is true**.
- Alerts can be classified as follows:
  - **True Positive**: The alert has been verified to be an actual security incident.
  - **False Positive**: The alert does not indicate an actual security incident. Benign activity that results in a false positive is sometimes referred to as **a benign trigger**.
- An alternative situation is that an alert was not generated. The absence of an alert can be classified as:
  - **True Negative**: No security incident has occurred. The activity is benign.
  - **False Negative**: An undetected incident has occurred.

Evaluating Alerts (Contd.)

When an alert is issued, it will receive one of four possible classifications:

	True	False
Positive (Alert exists)	Incident occurred	No incident occurred
Negative (No alert exists)	No incident occurred	Incident occurred

- **True positives** are the desired type of alert. They mean that the rules that generate alerts have worked correctly.
- **False positives** are not desirable. Although they do not indicate that an undetected exploit has occurred, they are costly because cybersecurity analysts must investigate false alarms.
- **True negatives** are desirable. They indicate that benign normal traffic is correctly ignored, and erroneous *(chybné)* alerts are not being issued.
- **False negatives** are dangerous. They indicate that exploits are not being detected by the security systems that are in place.

Note: *"True" events are desirable. "False" events are undesirable and potentially dangerous.*

Evaluating Alerts (Contd.)

- Benign events are those that should not trigger alerts. Excess benign events indicate that some **rules or other detectors** need to be improved or eliminated.
- When **true positives** are suspected, a cybersecurity analyst is required to escalate the alert to a higher level for investigation. The investigator will move forward with the investigation in order to confirm the incident and identify any potential damage that may have been caused.
- A cybersecurity analyst may also be responsible for informing security personnel that **false positives** are occurring to the extent that the cybersecurity analyst's time is seriously impacted.
- **False negatives** may be discovered well after an exploit has occurred. This can happen through retrospective security analysis (RSA). RSA can occur when **newly obtained rules** or other threat intelligence is applied **to archived network security data**.
- For this reason, it is important to monitor threat intelligence to learn of new vulnerabilities and exploits and to evaluate the likelihood that the network was vulnerable to them at some time in the past.

Overview of Alert Evaluation

Deterministic Analysis and Probabilistic Analysis

- Deterministic analysis evaluates risk based on what is known about a vulnerability. This type of risk analysis can only describe the worst case.
- Probabilistic analysis estimates the potential success of an exploit by estimating the likelihood that if one step in an exploit has successfully been completed that the next step will also be successful.
- In a **deterministic** analysis, all of the information to accomplish an exploit is assumed to be known.
- In **probabilistic** analysis, it is assumed that the port numbers that will be used can only be predicted with some degree of confidence.
- The two approaches are summarized below.
  - **Deterministic Analysis** - For an exploit to be successful, all prior steps in the exploit must also be successful. The cybersecurity analyst knows the steps for a successful exploit.
  - **Probabilistic Analysis** - Statistical techniques are used to determine the probability that a successful exploit will occur based on the likelihood that each step in the exploit will succeed.

26.3 Evaluating Alerts Summary

What Did I Learn in this Module?

- Security Onion is an open-source suite of Network Security Monitoring (NSM) tools that run on an Ubuntu Linux distribution.
- Security Onion tools provide three core functions for the cybersecurity analyst: full packet capture and data types, network-based and host-based intrusion detection systems, and alert analyst tools.
- Security Onion integrates the data and IDS logs into a single platform through the following tools:
  - Sguil - serves as a starting point in the investigation of security alerts.
  - Kibana - It is an interactive dashboard interface to Elasticsearch data.
  - The Wireshark packet capture application is integrated into the Security Onion suite.
  - Zeek is a network traffic analyzer that serves as a security monitor.

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

- Snort is a Network Intrusion Detection System (NIDS). It is an important source of the alert data that is indexed in the Sguil analysis tool.
- Alerts can be classified as True Positive (The alert has been verified to be an actual security incident) or False Positive (The alert does not indicate an actual security incident).
- An alternative situation is that an alert was not generated. The absence of an alert can be classified as: True Negative (No security incident has occurred. The activity is benign.) and False Negative (An undetected incident has occurred).
- Deterministic analysis evaluates risk based on what is known about a vulnerability.
- Probabilistic analysis estimates the potential success of an exploit by estimating the likelihood that if one step in an exploit has successfully been completed that the next step will also be successful.

UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

Ďakujem za pozornosť

Obsahom boli moduly:

Chapter 25 Network Security Data

Chapter 26 Evaualting Alerts (in Security Onion)

Vyjadrite spätnú väzbu na prednášku a/alebo cvičenie v anonymnej ankete cez google form: link

Vytvorené v rámci projektu KEGA 026TUKE-4/2021.