UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Chapter 5

Always A Pioneer, Always Ahead

Physical Security Log Collection

Dr. Zaheera Zainal Abidin
zaheera@utem.edu.my

MyUTeM

By the end of the lesson, the student will be able to:

a. understand the idea of log collection
b. understand the log normalization, log severity, log time correction and log category
c. Understand how to transport the syslog to the syslog server

CONTENT

- Introduction
- Standards in Log Collection
- Log Normalization
- Log Severity
- Log Time Correction
- Log Categorization
- What…..When……How….to Transport the Log ?

INTRODUCTION

WHAT IS A LOG, EVENT LOG, SYSLOG???

- A **log** is **an automatic computer-generated file that contains the time-stamped record of events** obtained **from various system** in the infrastructure.
- Meanwhile, **event log** is **a file consists of vital information about operations and usage of an application, device or operating system**. Each operation and application has its own log file. When there is an incident detected in the network, the event log monitors the importance event and analyse logs in the investigation and identification process.
- Besides, the **syslog means (system logging protocol)**, which is a **standard protocol used to send log or event message to a syslog server to collect various device logs from different machines for monitoring and review. Syslog is useful for network audits trails.**

INTRODUCTION

- What Does Syslog Do?
- Syslog provides a way for network devices to send messages and log events. Syslog has a standard format for all applications and devices to be used. A syslog message contains the following elements:
  - Header
  - Structured data
  - Message

INTRODUCTION

- The **header** includes information about the version, time stamp, host name, priority, application, process ID, and message ID. The **structured data** comprises data blocks in a specific format, which is followed by the log message.
- Log **messages** should be encoded using the **8-bit Unicode Transformation Format** (UTF-8), but apart from that, the messages can be configured based on individual needs. The flexibility of the message content is part of what makes syslog so popular and effective.
- The severity levels for syslog messages range from 0, which signals an emergency, to 5, which constitutes a warning. There are additional options for informational messages (level 6) and debugging (level 7).
- Syslog only supports sending messages to a defined location when certain events happen.

INTRODUCTION

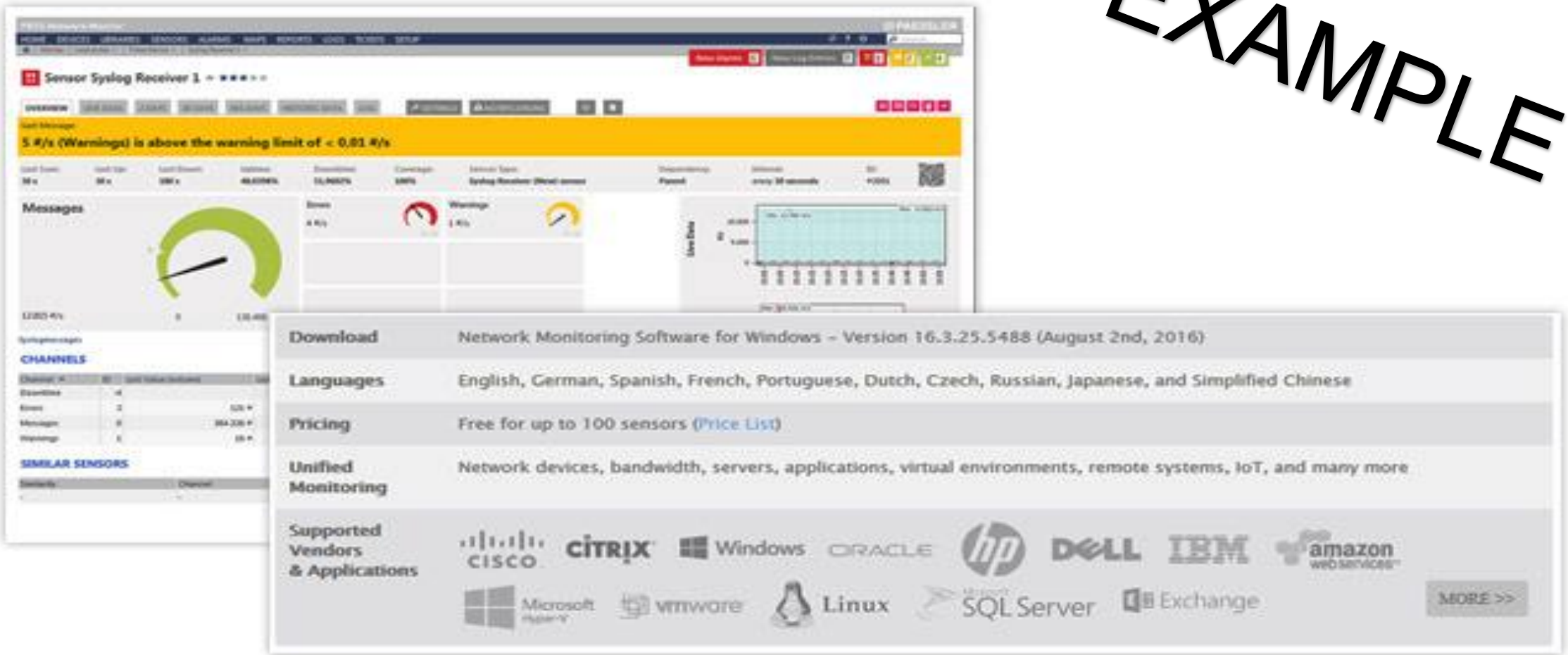
- Syslog is generated based on the source, type of logs or rate.
- Syslog are sent directly from point devices to ESM manager.
- A log collection mechanism needs to be scalable, extensible and flexible.
- Syslog has three layers as part of the standard definition:
  - Syslog content: The information in the event message
  - Syslog application: The layer that generates, routes, interprets, and stores the message
  - Syslog transport: The layer that transmits the message

What Is Syslog Server?

- Syslog servers are used to collect syslog messages in a single location. A syslog server might be a physical server, a standalone virtual machine, cloud- based SEM or a software-based service.
- To make it possible for syslog servers to receive, interpret, and store the messages, they usually have a couple of common components:
  - Syslog Listener: This allows the server to receive messages by gathering Syslog data.
  - Database: This is important for larger networks to be able to store syslog data for easy reference.
  - A good syslog server allows you to both collect the syslog messages and view and filter them from one location. This should include syslog messages from all devices and operating systems, with the ability to log in from any location through a secure portal.

PRTG Syslog Server

EXAMPLE



What Is Syslog Server?

- Automation is important. With the right syslog server, you configure alerts to notify you problems coming through syslog. You may set up other types of responses to messages, such as running scripts, forwarding messages, and logging to a file.
- Another way to view information is with reports. Syslog servers may allow you to schedule reports to run at certain times and be delivered to your email, so you can easily review graphs of statistics.
- Advanced functionality may also support:
  - Filtering messages based on priority, host IP address, host name, or time
  - Buffering messages, so your system or inbox doesn't get overwhelmed during heavy loads
  - While you won't want to keep all logs active for long periods, compliance frameworks have specific requirements for log retention. A good syslog server will support archiving log data to comply with HIPAA, SOX, and more.

LIMITATIONS OF SYSLOG

- Syslog has a few weak spots. The flexibility of the message component is useful, but **not having a standard format** can sometimes be challenging.
- Syslog also **employs User Datagram Protocol (UDP)** to transport information, which **means log messages could be lost if there's network congestion.**
- Finally, syslog does **not include any authentication** processes to prevent a machine from impersonating another.

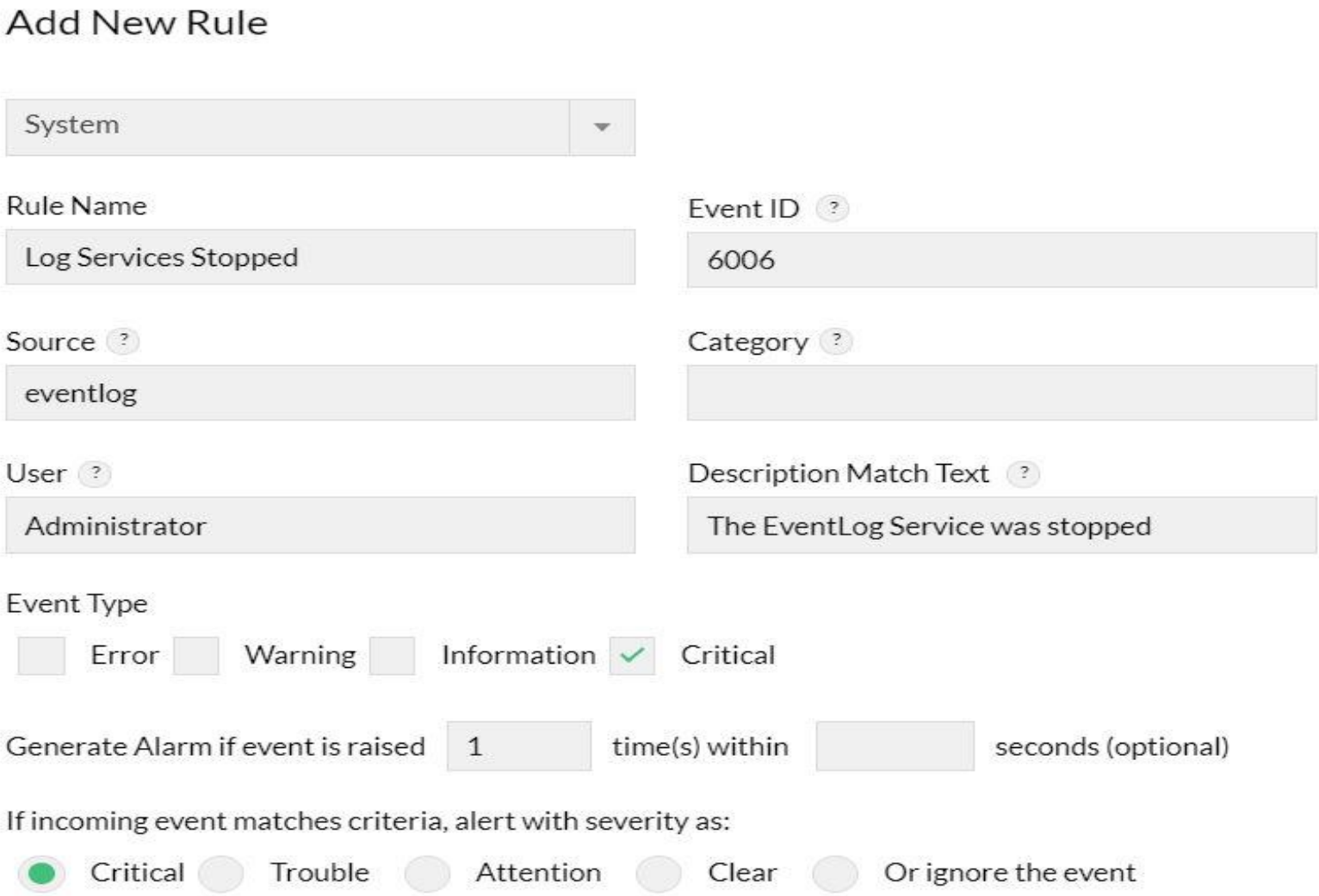
EVENT LOG

- An event log is a more basic resource that stores different types of information based on specific events. These events include:
  - Failed password attempts
  - Locked accounts
  - Network login sessions
  - Application errors
  - Unexpected application closures

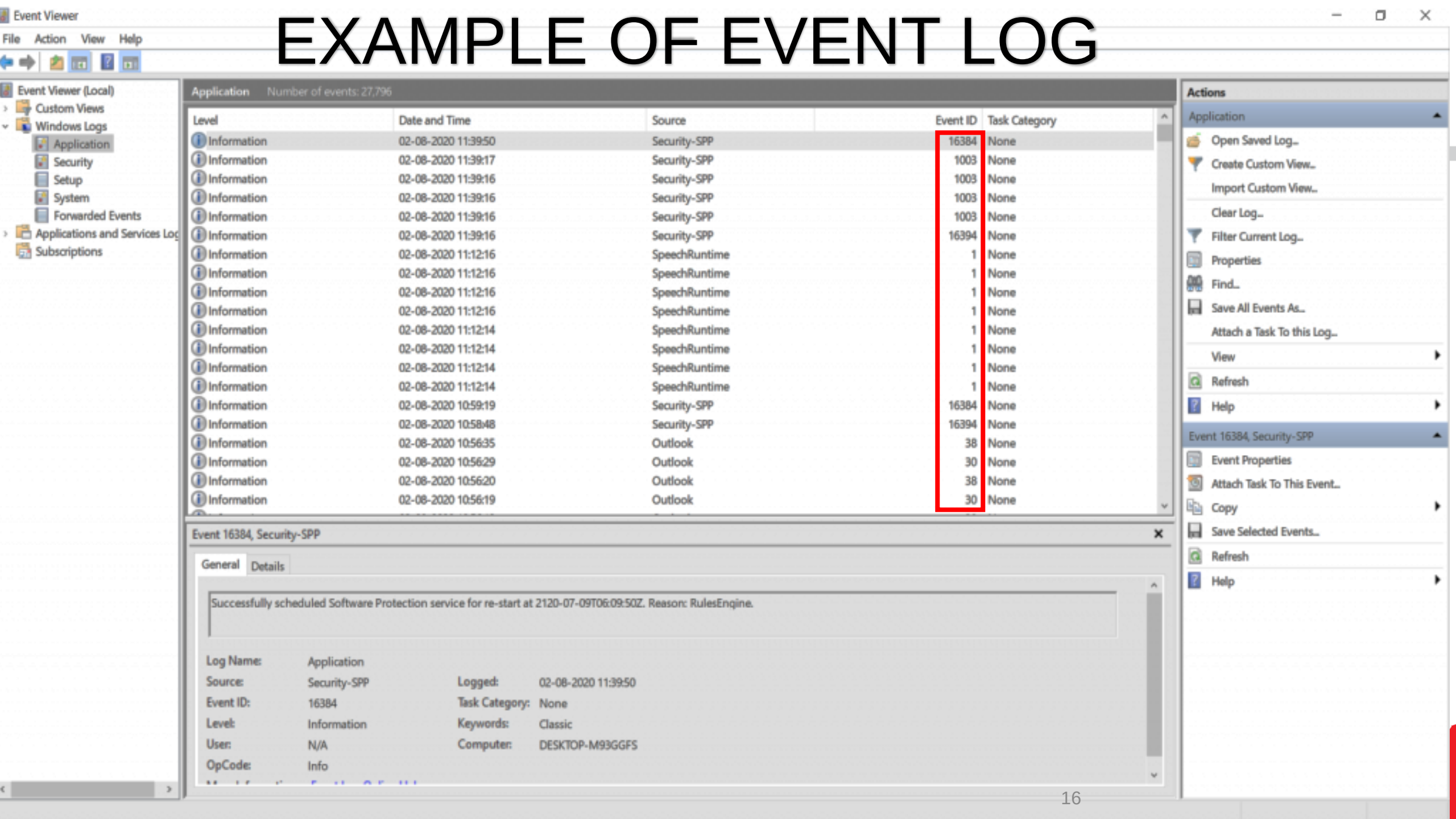
EVENT LOG

- Event logs used to troubleshoot problems with security management, application installations, and more. The Windows event log includes the following information for each entry:
  - Date: Date when the event occurred
  - Time: Time when the event occurred
  - User: User logged in when the event occurred
  - Computer: Name of the computer used
  - Event ID: An identification number from Windows indicating the event type
  - Source: Component or program that caused the event
  - Type: Type of event
  - When thinking about syslog vs. event log, it helps to remember an event log is a subset of what might be tracked in syslog. Syslog servers capture information from multiple logs and store it in a central location.

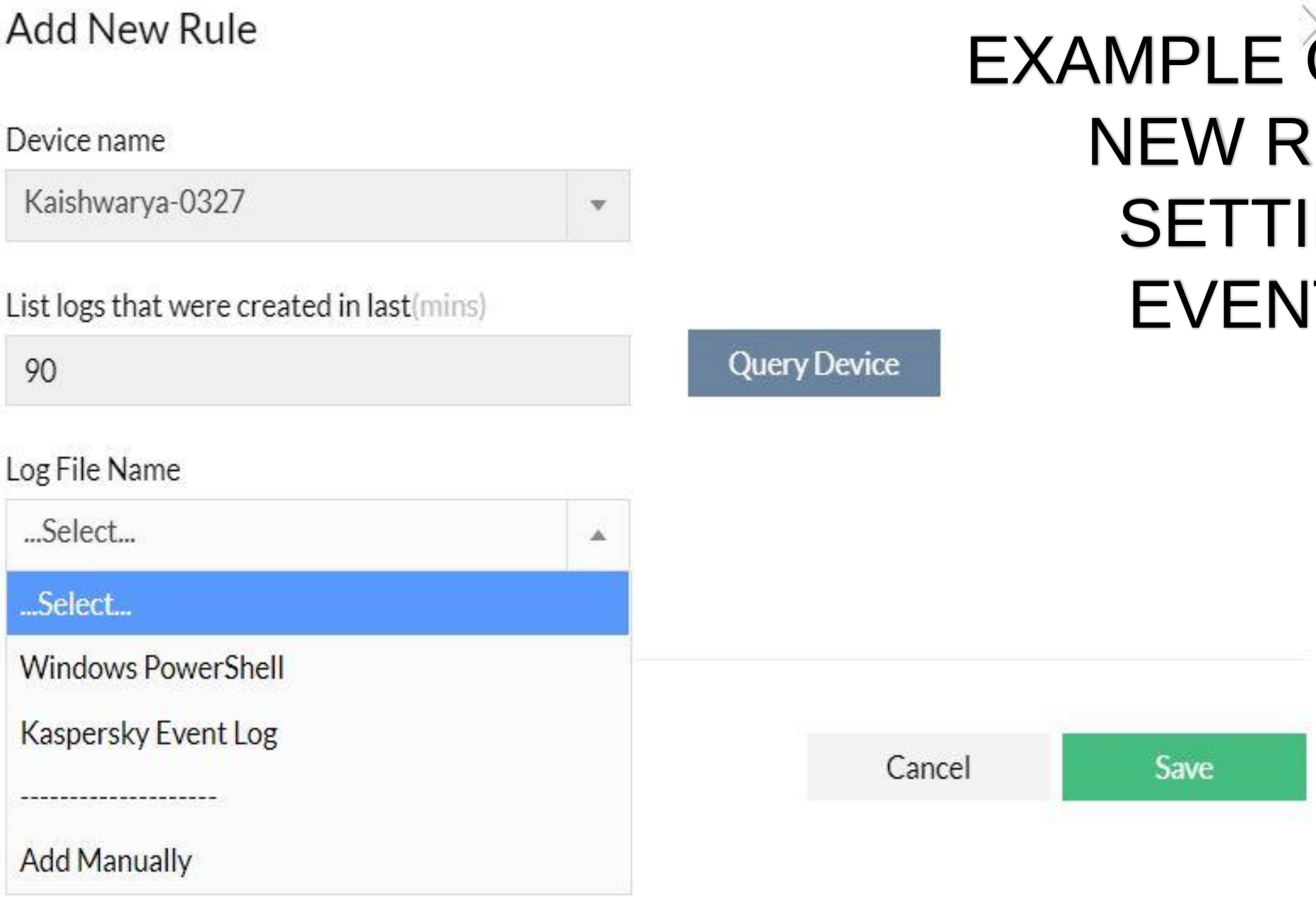
SETTING UP EVENT LOG - EXAMPLE



EXAMPLE OF EVENT LOG



EXAMPLE OF ADDING NEW RULE TO SETTING UP EVENT LOG



STANDARD IN LOG COLLECTION

STANDARD IN LOG COLLECTION

- National Institute of Standards and Technology (**NIST**) Special Publication 800-92 (International)
- **ISO/IEC 27001:2013** –Information Technologies –Security Techniques –Information Security Management Systems–Requirement (Department of Standards Malaysia, Ministry of Science, Technology and Innovation (MOSTI))

NIST 800-92

- Delivering guidance and standards for information security.
- Some general guidelines:
  - Prioritize log management
  - Establish policies and procedures for log management
  - Create and maintain a secure log management infrastructure

ISO/IEC 27001: 2013

- Establish Information Security Management Systems (ISMS) based on the process approach, implementation and improvement.
- Define and plan your systems by :
  - Defining scope and boundaries of ISMS
  - Defining your organization's ISMS policy
  - Defining your approach on assessing risk
  - Identifying the security risks by identifying the asset involved, the threats to those asset, the vulnerabilities exploited by the threats and impact of the risk incidents on the assets
  - Analyze and evaluate your organization's security risks.

ISO/IEC 27001: 2013

- Identify and evaluate risk options and actions for treatment
- Select control objectives and controls to treat risks to meet the requirements identified by the risk assessment and risk treatment process
- Ensure that management approves the residual risks (the remaining risk that are still available after risk assessment has been implemented)
- Obtain management approval to implement and operate your organization's ISMS
- Prepare a Statement of Applicability (SoA) that lists your organization's specific control objectives and controls as listed in Annex A of the standard.

- Implement and operate ISMS
- Develop and implement a risk treatment plan to manage your organization's information security risks

ISO/IEC 27001: 2013

- Implement your organization's security controls and define how to measure the effectiveness of the security control
- Implement training and awareness programs
- Manage and operate your organization's ISMS
- Manage ISMS resources
- Establish procedures on identifying security events and response to security incident
- Monitor and review the ISMS by :
- Implement monitoring and reviewing procedure to detect errors, identify attempted and successful security breaches and incidents, enable management to determine that the security activities and performing as expected, prevent security events and ensure effectiveness of actions taken to breach of security
- Perform regular reviews of your ISMS and measure the effectiveness of the controls

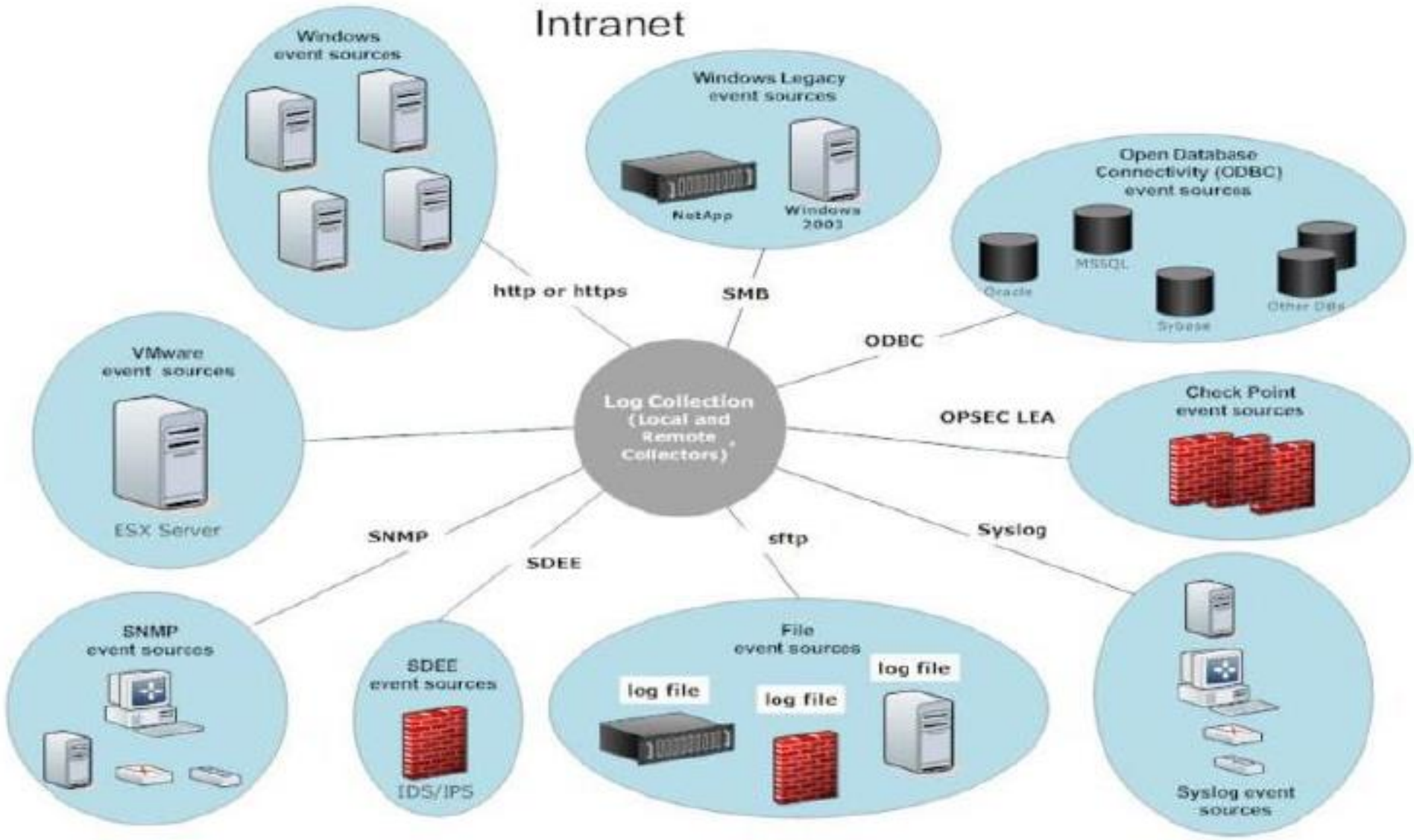
ISO/IEC 27001: 2013

- Review your risk assessments, residual risks and acceptable levels of risk on a regular basis
  - Conduct internal audits of your ISMS
  - Conduct management reviews of your ISMS and update your information security plans
  - Maintain a record of ISMS events and actions
- Maintain and improve ISMS
  - Implement identified improvement for your systems
  - Perform suitable corrective and preventive actions and learn from the breach and incidents
  - Communicate action and improvement and ensure the improvement applied achieved its intended objectives

ISO/IEC 27001: 2013

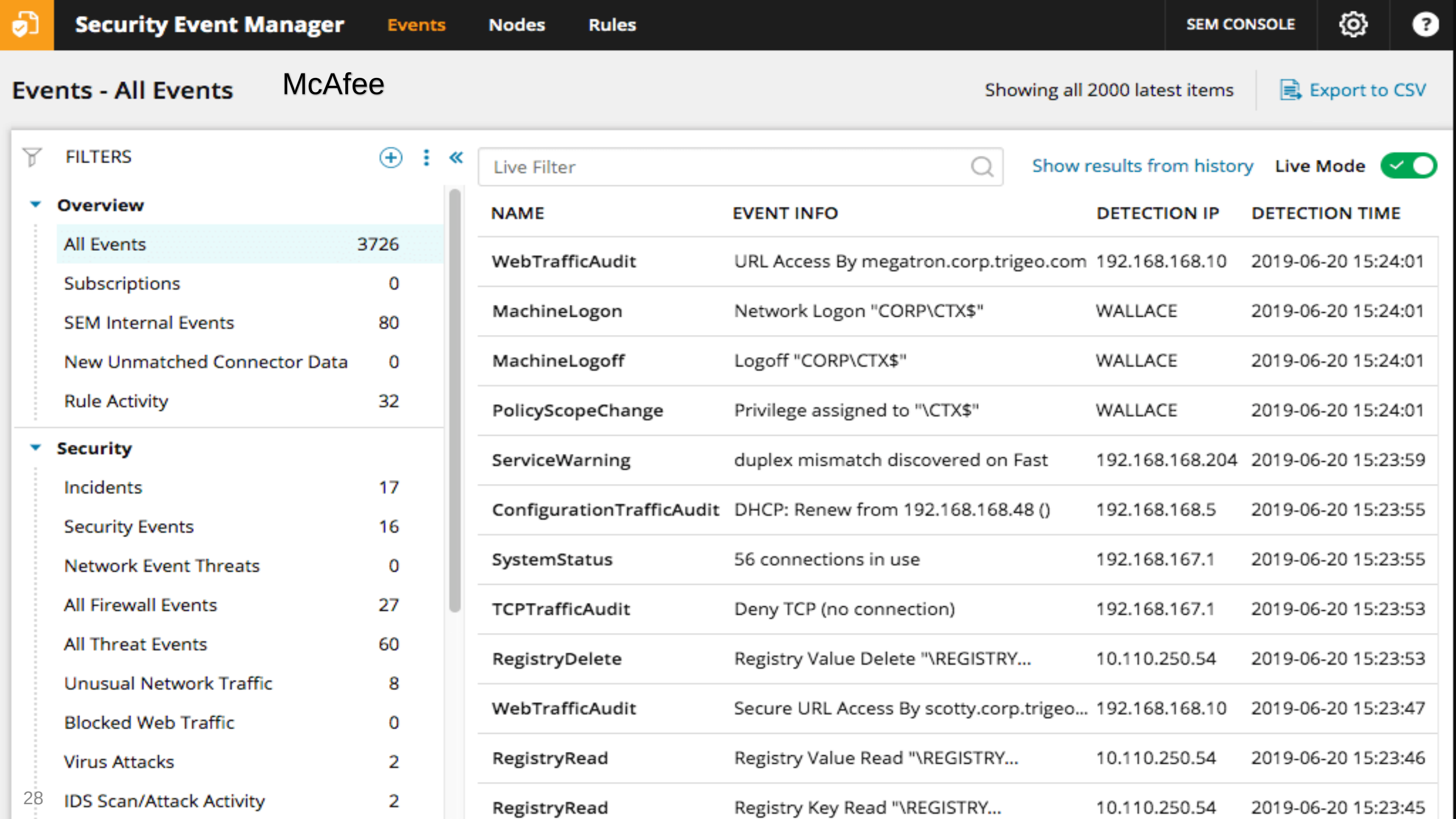
- Document your systems and explain how it works in your organization through manual, procedures, work instructions etc. and must include statement of ISMS policy, procedures and controls required by the ISMS, risk methodology, risk assessment report and risk treatment plan
- Document Control Procedure to control documents used for ISMS
- Record Control Procedure to control records that are used for ISMS

COMPONENTS IN EVENT LOG COLLECTION



EVENT COLLECTION SOURCE

- The syslog protocol is used as a way to transport messages from network devices to a logging server, typically known as a syslog server.
- Event sources are the assets on the network, such as servers, switches, routers, storage arrays, operating systems, and firewalls.
- In most cases, your Information Technology (IT) team configures event sources to send their logs to the Log Collector and the Security Analytics administrator configures the Log Collector to poll event sources and retrieve their logs.
- As a result, the Log Collector receives all logs in their original form, without filtering or normalization.


Security Event Manager
Events
Nodes
Rules
SEM CONSOLE
Events - All Events
McAfee
Showing all 2000 latest items
Export to CSV
FILTERS
Live Filter
Show results from history
Live Mode
Overview
All Events 3726
Subscriptions 0
SEM Internal Events 80
New Unmatched Connector Data 0
Rule Activity 32
Security
Incidents 17
Security Events 16
Network Event Threats 0
All Firewall Events 27
All Threat Events 60
Unusual Network Traffic 8
Blocked Web Traffic 0
Virus Attacks 2
IDS Scan/Attack Activity 2
NAME
EVENT INFO
DETECTION IP
DETECTION TIME
WebTrafficAudit URL Access By megatron.corp.trigeo.com 192.168.168.10 2019-06-20 15:24:01
MachineLogon Network Logon "CORP\CTX$" WALLACE 2019-06-20 15:24:01
MachineLogoff Logoff "CORP\CTX$" WALLACE 2019-06-20 15:24:01
PolicyScopeChange Privilege assigned to "\CTX$" WALLACE 2019-06-20 15:24:01
ServiceWarning duplex mismatch discovered on Fast 192.168.168.204 2019-06-20 15:23:59
ConfigurationTrafficAudit DHCP: Renew from 192.168.168.48 () 192.168.168.5 2019-06-20 15:23:55
SystemStatus 56 connections in use 192.168.167.1 2019-06-20 15:23:55
TCPTrafficAudit Deny TCP (no connection) 192.168.167.1 2019-06-20 15:23:53
RegistryDelete Registry Value Delete "\REGISTRY... 10.110.250.54 2019-06-20 15:23:53
WebTrafficAudit Secure URL Access By scotty.corp.trigeo... 192.168.168.10 2019-06-20 15:23:47
RegistryRead Registry Value Read "\REGISTRY... 10.110.250.54 2019-06-20 15:23:46
RegistryRead Registry Key Read "\REGISTRY... 10.110.250.54 2019-06-20 15:23:45

EVENT COLLECTION SOURCE

- **Check Point** -The Log Collector service collects events from Check Point event sources using OPSEC LEA. OPSEC LEA is the Check Point Operations Security Log Export API that facilitates the extraction of logs (see Check Point Event Source).
- **File**- The Log Collector service collects events from log files. Event sources generate log files that are transferred using a secure file transfer method to the Log Decoder appliance running the Log Collector service (see File Event Source).
- **ODBC**- The Log Collector service collects events from event sources that store audit data in a database using the Open Database Connectivity (ODBC) software interface (see ODBC Event Source).

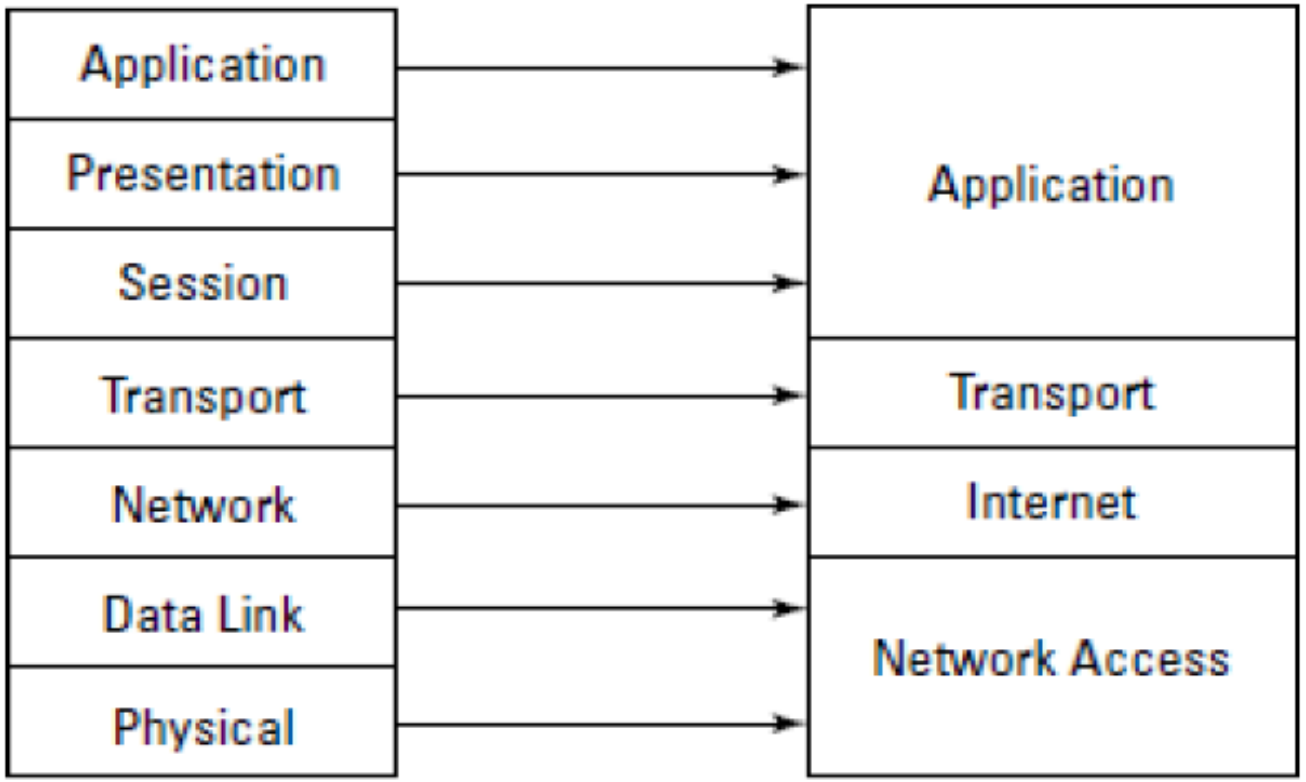
EVENT COLLECTION SOURCE

- **SDEE**-The Log Collector service collects Intrusion Detection System (IDS) and Intrusion Prevention Service (IPS) messages (view SDEE Event Source).
- **SNMP**-The Log Collector service collects SNMP traps (see SNMP Event Source).
- **Syslog** –The Log Collector service collects messages from event sources that issue syslog messages (see Syslog Event Source).
- **VMware** –The Log Collector service collects events from a VMware virtual infrastructure (see VMware Event Source)

EVENT COLLECTION SOURCE

- Windows - The Log Collector service collects events from Windows machines that support the Microsoft Windows model. Windows 6.0 is an event logging and tracing framework included in the operating system beginning with Microsoft Windows Vista and Windows Server 2008 (see Windows Event Source).
- Windows Legacy -The Log Collector service collects events from:
  - Older Windows versions such as Windows 2000 and Window 2003 and collects from Windows event sources that are already configured for envision collection without having to reconfigure them.
  - NetApp ONTAP appliance event source so that you can now collect and parse NetApp evt files.

EVENT LOG COLLECTION – TCP/IP



Events

Bound to: Event Summary

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
9780	TCP_NC_MISS - The object returned from the ori	489	69.20.2.87	194.63.247.30	n/a	01/02/2013 21:08:33	alert
40	TCP_MISS - The requested object was not in the	2	69.20.2.87	208.111.128.7	n/a	01/02/2013 20:04:55	alert
15160	TCP_HIT - A valid copy of the requested object w	758	69.20.2.87	208.19.38.8	n/a	01/02/2013 16:30:50	alert
1820	TCP_HIT - A valid copy of the requested object w	91	69.20.10.202	202.127.169.21	n/a	01/02/2013 16:07:37	alert
19	User Login	1	208.69.158.11	69.20.171.253	n/a	01/02/2013 14:18:38	success
306488	ET TROJAN Hiloti/Mufanom Downloader Checkin	3368	69.20.1.9	88.85.72.75	tcp	01/02/2013 14:17:28	critical
390	Connection opened	39	69.20.160.150	69.20.128.98	udp	01/02/2013 14:17:28	alert
4475	F5_Firepass Dialing Network Access	179	69.20.56.79	::	n/a	01/02/2013 14:17:28	start
0	Unknown_0	19250	69.20.1.237	::	n/a	01/02/2013 14:17:27	alert
75	LTM_NEDS Client Connection Started	3	69.20.113.202	69.20.113.202	tcp	01/02/2013 14:17:27	start

Details | Advanced Details | Geolocation | Description | Notes | Packet | Custom Types | ELM Archive

Retrieve ELM Archive:

Find text:

```
<191>snort: [1:2010071:2] ET TROJAN Bredolab Infection - checkin [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 69.20.1.9:1034 -> 88.85.72.75:80
<191>snort: [1:2010071:2] ET TROJAN Bredolab Infection - checkin [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 69.20.1.9:4602 -> 88.85.72.75:80
<191>snort: [1:2010071:2] ET TROJAN Bredolab Infection - checkin [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 69.20.1.9:3706 -> 88.85.72.75:80
<191>snort: [1:2010071:2] ET TROJAN Bredolab Infection - checkin [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 69.20.1.9:1714 -> 88.85.72.75:80
<191>snort: [1:2010071:2] ET TROJAN Bredolab Infection - checkin [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 69.20.1.9:4148 -> 88.85.72.75:80
<191>snort: [1:2010071:2] ET TROJAN Bredolab Infection - checkin [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 69.20.1.9:4295 -> 88.85.72.75:80
<191>snort: [1:2010071:2] ET TROJAN Bredolab Infection - checkin [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 69.20.1.9:4970 -> 88.85.72.75:80
<191>snort: [1:2010071:2] ET TROJAN Bredolab Infection - checkin [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 69.20.1.9:2363 -> 88.85.72.75:80
<191>snort: [1:2010071:2] ET TROJAN Bredolab Infection - checkin [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 69.20.1.9:1263 -> 88.85.72.75:80
<191>snort: [1:2010071:2] ET TROJAN Bredolab Infection - checkin [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 69.20.1.9:3687 -> 88.85.72.75:80
<191>snort: [1:2010071:2] ET TROJAN Bredolab Infection - checkin [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 69.20.1.9:2028 -> 88.85.72.75:80
<191>snort: [1:2010071:2] ET TROJAN Bredolab Infection - checkin [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 69.20.1.9:3077 -> 88.85.72.75:80
<191>snort: [1:2010071:2] ET TROJAN Bredolab Infection - checkin [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 69.20.1.9:2260 -> 88.85.72.75:80
```


Page 1

All events

LOG NORMALIZATION

- Normalization –to determine an acceptable standard for log format.
- In log normalization, each log data field is converted to a particular data representation and categorized consistently.
- In security logs –have multiple standards and multiple formats
- Either to store log time in 12-hour format (2:34) or 24-hour format (14:34)
- Normalizing makes log analysis and documentation much easier especially when multiple log formats are used.

LOG SEVERITY

- Severity means degree of defect that effects the functionality of the component.
- Log severity means a set of threshold value for the security event log. Each log source may have a unique severity level assigned to it.
- Vendor specific: grade log severity on scale of 1 to 10, 1 to 1,000 and some use letters (grade A, grade B or grade C).
- Connector severity is the translation of device severity into normalized value.
- Eg: Snort uses a device severity scale of 1 to 10, whereas check point uses a scale of High, Medium and Low.

LOG TIME CORRECTION

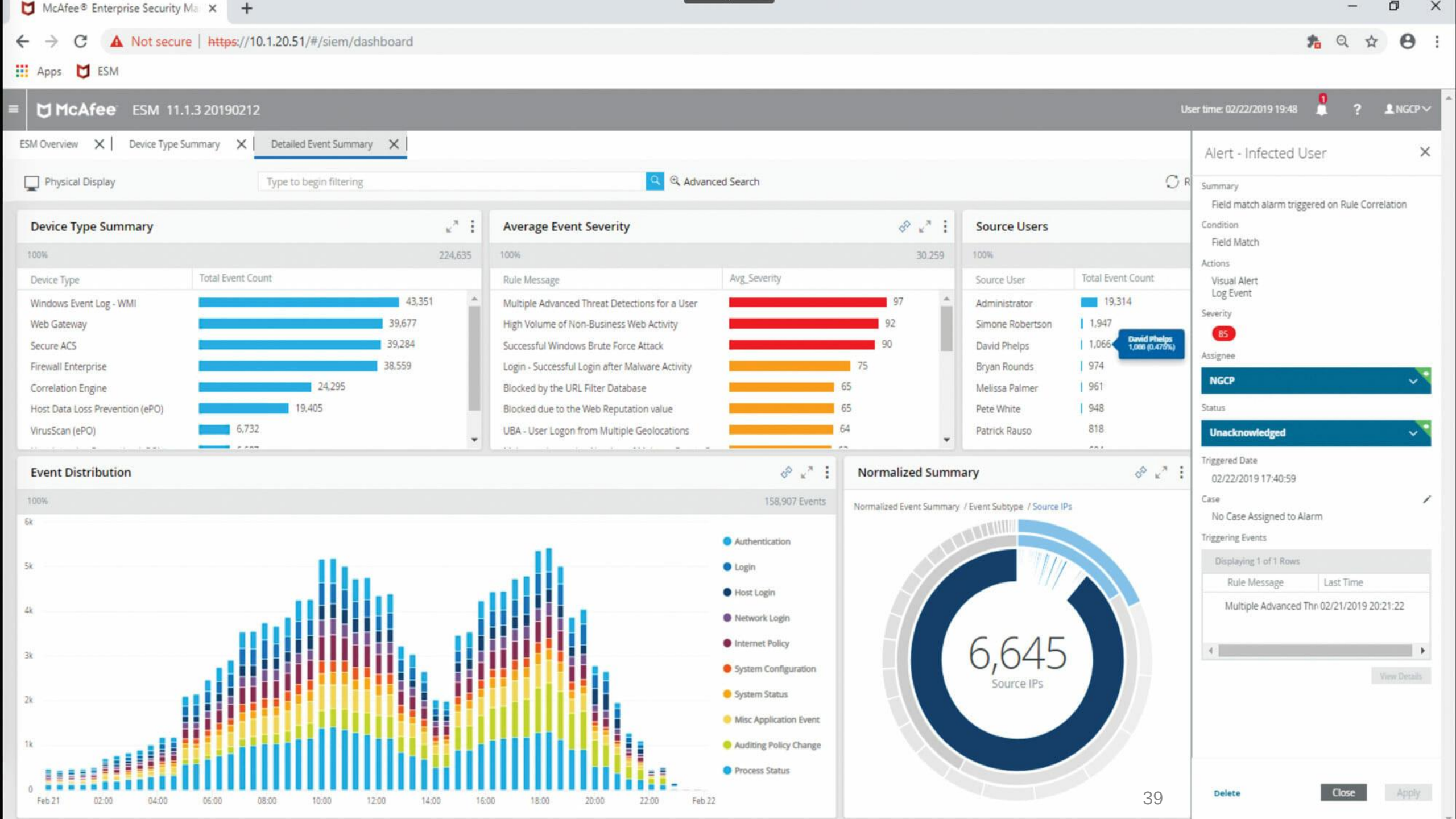
- The important factor to consider for log analysis is the time to agree upon time zone, such as Greenwich Mean Time (GMT)
- Using Network Time Protocol (NTP) for time synchronization
- The connector is always report the actual time.

LOG CATEGORIZATION

- A methodology for describing logs enables analysts to understand the significance of a particular log as reported from different devices
- Correlation on categorized logs in the form of log categories
- Eg: include detailing log's behavior, techniques it uses, its outcome.

THEREFORE…

- At this point,
  - The logs have been normalized
  - The severity levels based on disparate devices have commonality
  - The time has accurate
  - The logs have been fully categorized to become more usable


McAfee® Enterprise Security Ma
Not secure | https://10.1.20.51/#/siem/dashboard
Apps
ESM
McAfee ESM 11.1.3 20190212
User time: 02/22/2019 19:48
NGCP
ESM Overview
Device Type Summary
Detailed Event Summary
Physical Display
Type to begin filtering
Advanced Search
Device Type Summary
100%
224,635
Device Type
Total Event Count
Windows Event Log - WMI 43,351
Web Gateway 39,677
Secure ACS 39,284
Firewall Enterprise 38,559
Correlation Engine 24,295
Host Data Loss Prevention (ePO) 19,405
VirusScan (ePO) 6,732
Average Event Severity
100%
30,259
Rule Message
Avg_Severity
Multiple Advanced Threat Detections for a User 97
High Volume of Non-Business Web Activity 92
Successful Windows Brute Force Attack 90
Login - Successful Login after Malware Activity 75
Blocked by the URL Filter Database 65
Blocked due to the Web Reputation value 65
UBA - User Logon from Multiple Geolocations 64
Source Users
100%
Source User
Total Event Count
Administrator 19,314
Simone Robertson 1,947
David Phelps 1,066
Bryan Rounds 974
Melissa Palmer 961
Pete White 948
Patrick Rauso 818
David Phelps 1,066 (0.475%)
Event Distribution
100%
158,907 Events
6k
5k
4k
3k
2k
1k
0
Feb 21
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
Feb 22
Authentication
Login
Host Login
Network Login
Internet Policy
System Configuration
System Status
Misc Application Event
Auditing Policy Change
Process Status
Normalized Summary
Normalized Event Summary / Event Subtype / Source IPs
6,645
Source IPs
Alert - Infected User
Summary
Field match alarm triggered on Rule Correlation
Condition
Field Match
Actions
Visual Alert
Log Event
Severity
85
Assignee
NGCP
Status
Unacknowledged
Triggered Date
02/22/2019 17:40:59
Case
No Case Assigned to Alarm
Triggering Events
Displaying 1 of 1 Rows
Rule Message
Last Time
Multiple Advanced Thr
02/21/2019 20:21:22
View Details
Delete
Close
Apply
39

WHAT TO TRANSPORT?

- The data captured or monitored must be at the highest prioritize and have recommendations from other authority. Data should be logged and analysed if time and resources permit them.
- So, anything that is mission-critical to environment should be logged.
- Mission critical assets are more commonly critical applications, OS, databases, physical security safeguards–asks discovery recovery team.

WHEN TO TRANSPORT?

- Two primary log transport capabilities: real-time and batch-mode.
  - In **real time-logs** generated by the source device, collected by the log connectors and automatically sent to ESM for processing.
  - **Batch-mode–**allow the log flow to be more predictable and controlled. This help to ensure the most time-sensitive security data is relied and processed.

HOW TO TRANSPORT

- Transport mechanism –TCP or UDP?
- Reduce load applied to the network, the log data is compressed
- Encrypt logs using Secure Socket Layer (SSL)
- Thus, the combination of TCP, high availability architectures, compression and encryption provides a solid foundation for log transmission
- It facilitates reliable, highly available, efficient and secure transmission of every logs

TOOLS FOR EVENT LOG COLLECTION

- The open source log management tools are:
- **Nagios**
- **Windows Event Collector**
- **OSSEC** (ossec.net) an open source tool for analysis of real-time log data from Unix systems, Windows servers and network devices. It includes as et of useful default alerting rules as well as a web-based graphical user interface. This is THE tool to use, if you are starting up your log review program.
- **Snare** agent (intersectalliance.com/projects/index.html) and **Project Lasso** remote collector (sourceforge.net/projects/lassolog) are used to convert Windows **Event Logs in** to **syslog**, a key component of any log management infrastructure today (at least until Visa / W7 log aggregation tools become mainstream).

TOOLS FOR EVENT LOG COLLECTION

- The open source log management tools are:
- **syslog-ng** (balabit.com/network-security/syslog-ng/) is a replacement and improvement of classic syslog service -it also has a Windows version that can be used the same way as Snare
- **rsyslog**(rsyslog.com) is another notable replacement and improvement of syslog service that uses traditional (rather than ng-style) format for syslog.conf configuration files. No Windows version, but it has an associated front-end called phpLogCon.
- Among the somewhat dated tools, **Logwatch** (logwatch.org) and Lire (logreport.org).

TOOLS FOR EVENT LOG COLLECTION

- The open source log management tools are:
- **LogSurfer**(crypt.gen.nz/logsurfer) can all be used to summarize logs into readable reports.
- **sec** (simple-evcorr.sourceforge.net) can be used for correlating logs, even though most people will likely find OSSEC correlation a bit easier to use.
- **LogHound**(ristov.users.sourceforge.net/loghound) and slct(ristov.users.sourceforge.net/slct) are more "research-grade" tools, that are still very useful for going thru a large pool of barely-structured log data.
- **Log2timeline** (log2timeline.net/) is a useful tool for investigative review of logs; it can create a timeline view out of raw log data.
- **LogZilla**(aka php-syslog-ng) (code.google.com/p/php-syslog-ng) is a simple PHP-based visual front-end for a syslog server to do searches, reports, etc.


McAfee
McAfee ESM
Summary
Source ips
Destination IPs
79
Distribution
Source Ports
Widget Title
842,408
Refresh
Configuration
Drilldown
Actions
Export
Delete
Help
32%
172.16.0.1
20%
From Baseline
View Details

EXAMPLE OF LOG DATA - DEVICE

ID	DATE	USER	PC	ACTIVITY
{Y6O4-A7KC67IN-0899AOZK}	01/04/2019 0:10	DTAA/KEE0997	PC-1914	Logon
{O5Y6-O7CJ02JC-6704RWBS}	01/04/2019 0:52	DTAA/KEE0997	PC-1914	Logoff
{D2D1-C6EB14QJ-2100RSZO}	01/04/2019 1:17	DTAA/KEE0997	PC-3363	Logon
{H9W1-X0MC70BT-6065RPAT}	01/04/2019 1:28	DTAA/KEE0997	PC-3363	Logoff
{H3H4-S5AZ00AZ-9560IYHC}	01/04/2019 1:57	DTAA/BJM0992	PC-3058	Logon

Thank You

MyUTeM

www.utem.edu.my