

Group Members :-

Muhammad Izham Bin Norhamadi , B032020039 , S2G1

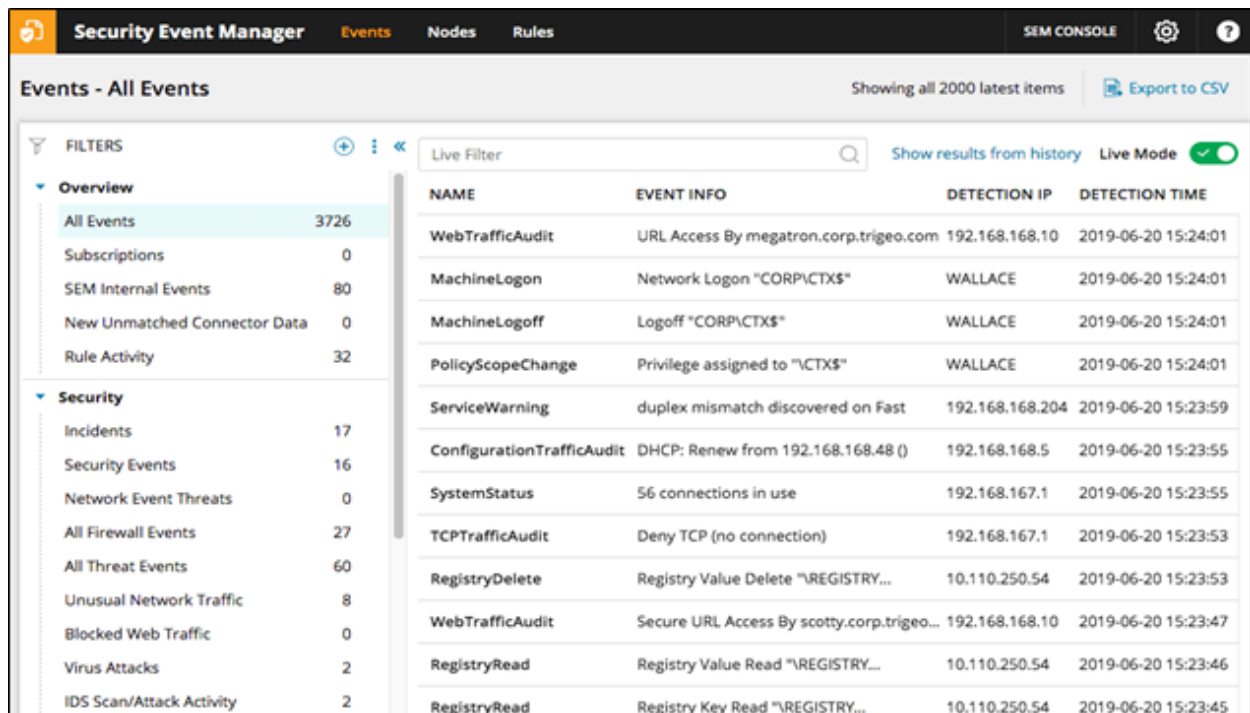
Ahmad Sha Herizam Bin Tahir, B032020009, S2G1

Muhammad Zahid Bin Saiful Adlan, B032010363, S2G1

Muhammad Haikal Bin Rosli, B032010336, S2G1

5.0 Lab Exercise Log

A log is an automatic computer-generated file that contains the time-stamped record of events obtained from various system in the network 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 have its own log file. The event log monitors the important event and analyze logs in the identification and for forensic investigation process. Figure 1 illustrates the security event management (SEM) from a console.



The screenshot displays the Security Event Manager interface. The top navigation bar includes 'Events', 'Nodes', and 'Rules'. The main header shows 'Events - All Events' with a count of 3726. A sidebar on the left lists various event categories under 'Overview' and 'Security'. The main table lists individual events with columns for NAME, EVENT INFO, DETECTION IP, and DETECTION TIME.

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

Figure 1: Event Log Management

Questions :

1. Explain the reason on machine logon and machine logoff by the WALLACE?

The reason is because authentication may take place on a different computer than the one into which you are logging. A logon session has a beginning and end.

2. What is the meaning of Deny TCP (no connection)?

An expected behavior when the packet faces asymmetric routing or different firewall context.

3. Is the event log has been normalized? (yes / no)?

Yes, event normalization makes it easy to process important and relevant data such as threat events

4. Why did WALLACE change his policy to privilege?

In an organization, it is to give an employee as much power as they need to do their job. Log and Event Manager can report on the actual usage of privileges to justify granting elevated permissions and audit against the abuse of these privileges.

5. List items of log categorization as shown as in Figure 1.

- The event log is listed by name, event info, detection ip and detection date.
- The Security log are listed by Incidents, Security Events, Network Event Threats, Firewall Events, Threat Events, Unusual Network Traffic, Blocked Web Traffic, Virus Attacks, and IDS Scan

6. What is the impact of incoming event WebTrafficAudit towards the safety of the URL?

A Web Traffic Audit identifies vulnerabilities to security breaches and prevents sensitive information from being compromised.

7. Explain the purpose of event log collection in SEM.

Record any event or activity occur in any system to take fully precaution on any source of breach or attack toward the system. When the log procedure captures any suspicious activity, it will automatically alert the administrator to take any swift action on that particular activity.

Other than that, by using the event log collection, system can identify user who is interacting with the system in a certain point of time. This is really useful when any suspicious activity happened, system can pinpoint the user at the time of the event. This will help if investigation is needed to investigate the event.

8. Explain the system status in the Figure 1.

There's 56 connections being connected to the system. Every activity occurring in the system will be recorded by the system in this Event Log.