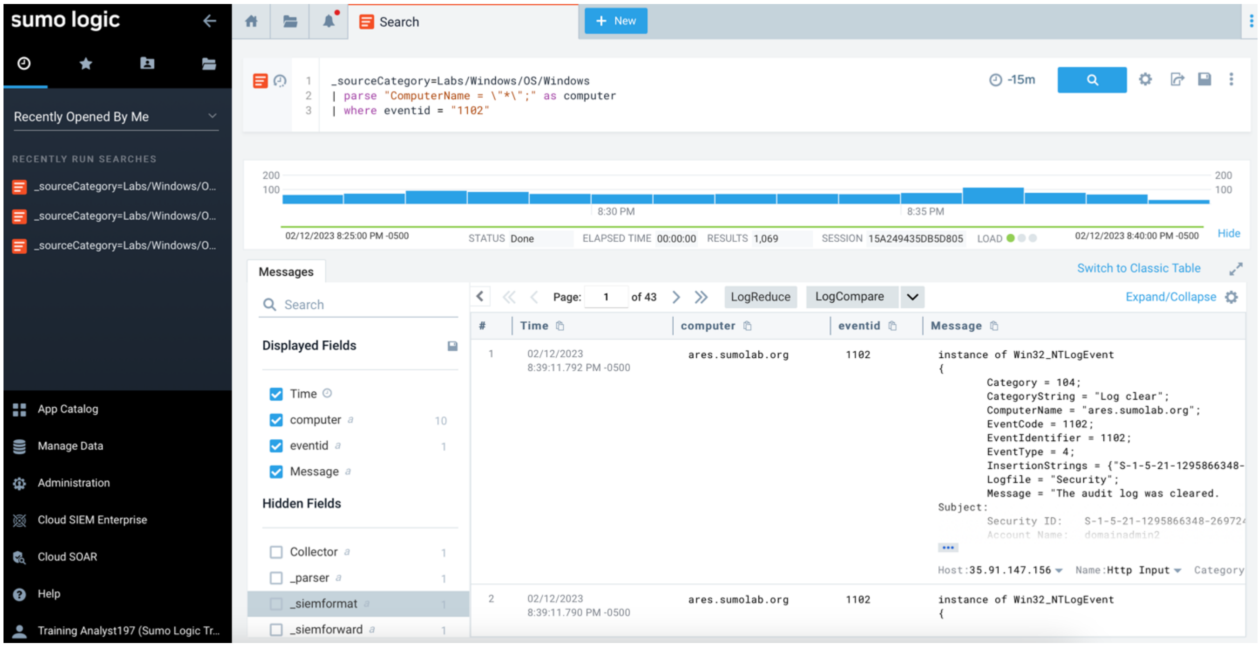
ENDPOINT SECURITY INVESTIGATION
STEPHEN MENSAH

Lab Screenshots

Windows Log cleared

Filtering logs with the event id 1102



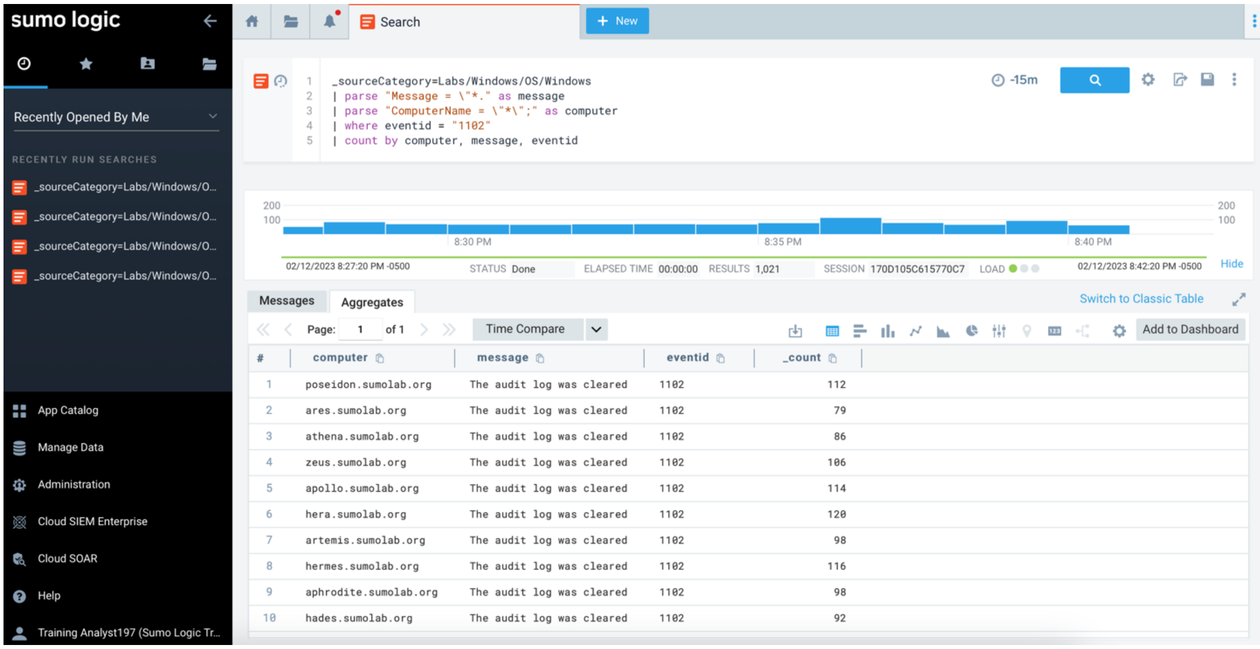
```
_sourceCategory=Labs/Windows/OS/Windows
| parse "ComputerName = \"*\";" as computer
| where eventid = "1102"
```

02/12/2023 8:25:00 PM -0500 STATUS Done ELAPSED TIME 00:00:00 RESULTS 1,069 SESSION 15A249435DB5D805 LOAD 02/12/2023 8:40:00 PM -0500

#	Time	computer	eventid	Message
1	02/12/2023 8:39:11.792 PM -0500	ares.sumolab.org	1102	instance of Win32_NTLogEvent
2	02/12/2023 8:39:11.790 PM -0500	ares.sumolab.org	1102	instance of Win32_NTLogEvent

```
instance of Win32_NTLogEvent
{
        Category = 104;
        CategoryString = "Log clear";
        ComputerName = "ares.sumolab.org";
        EventCode = 1102;
        EventIdentifier = 1102;
        EventType = 4;
        InsertionStrings = {"S-1-5-21-1295866348-
        Logfile = "Security";
        Message = "The audit log was cleared.
Subject:
        Security ID:    S-1-5-21-1295866348-26972
        Account Name:   domainadmin2
...
Host:35.91.147.156   Name:Http Input   Category
```

The aggregated query results



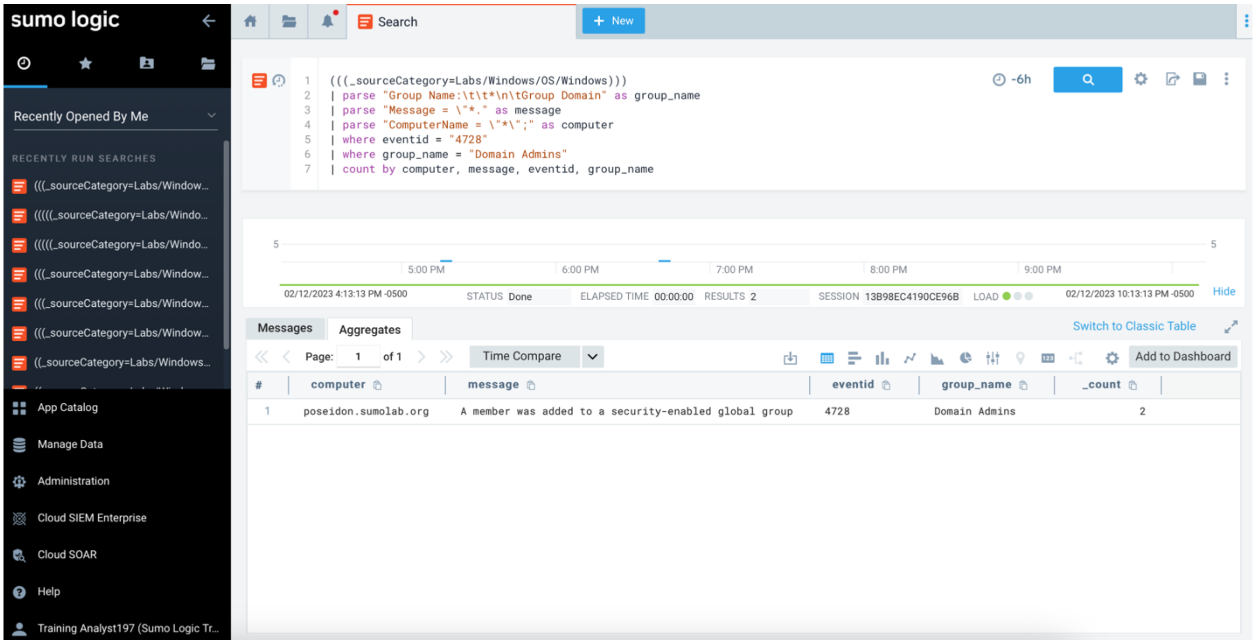
```
_sourceCategory=Labs/Windows/OS/Windows
| parse "Message = \"*." as message
| parse "ComputerName = \"*\";" as computer
| where eventid = "1102"
| count by computer, message, eventid
```

02/12/2023 8:27:20 PM -0500 STATUS Done ELAPSED TIME 00:00:00 RESULTS 1,021 SESSION 170D105C615770C7 LOAD 02/12/2023 8:42:20 PM -0500

#	computer	message	eventid	_count
1	poseidon.sumolab.org	The audit log was cleared	1102	112
2	ares.sumolab.org	The audit log was cleared	1102	79
3	athena.sumolab.org	The audit log was cleared	1102	86
4	zeus.sumolab.org	The audit log was cleared	1102	106
5	apollo.sumolab.org	The audit log was cleared	1102	114
6	hera.sumolab.org	The audit log was cleared	1102	120
7	artemis.sumolab.org	The audit log was cleared	1102	98
8	hermes.sumolab.org	The audit log was cleared	1102	116
9	aphrodite.sumolab.org	The audit log was cleared	1102	98
10	hades.sumolab.org	The audit log was cleared	1102	92

CHANGES TO DOMAIN ADMINS

Parsing user group names and filtering logs using event ID 4728 and group name “Domain Admins”

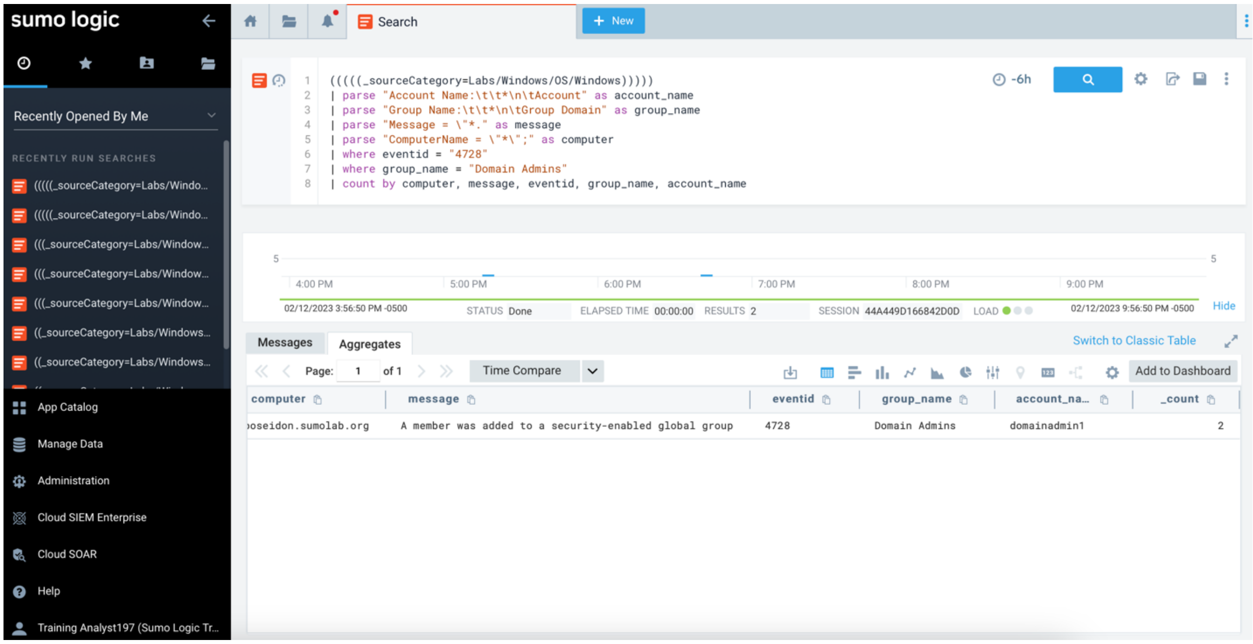

sumo logic
Search
New
Recently Opened By Me
RECENTLY RUN SEARCHES
(((_sourceCategory=Labs/Window...
(((((_sourceCategory=Labs/Windo...
(((((_sourceCategory=Labs/Windo...
(((_sourceCategory=Labs/Window...
(((_sourceCategory=Labs/Window...
(((_sourceCategory=Labs/Window...
((_sourceCategory=Labs/Windows...
App Catalog
Manage Data
Administration
Cloud SIEM Enterprise
Cloud SOAR
Help
Training Analyst197 (Sumo Logic Tr...
-6h
5
5:00 PM
6:00 PM
7:00 PM
8:00 PM
9:00 PM
Hide
Messages
Aggregates
Switch to Classic Table
Page: 1 of 1
Time Compare
Add to Dashboard

```
(((_sourceCategory=Labs/Windows/OS/Windows)))
| parse "Group Name:\t\t*\n\tGroup Domain" as group_name
| parse "Message = \"*." as message
| parse "ComputerName = \"*\";" as computer
| where eventid = "4728"
| where group_name = "Domain Admins"
| count by computer, message, eventid, group_name
```

02/12/2023 4:13:13 PM -0500 STATUS Done ELAPSED TIME 00:00:00 RESULTS 2 SESSION 13B98EC4190CE96B LOAD 02/12/2023 10:13:13 PM -0500

#	computer	message	eventid	group_name	_count
1	poseidon.sumolab.org	A member was added to a security-enabled global group	4728	Domain Admins	2

Parsing account names and aggregated query results

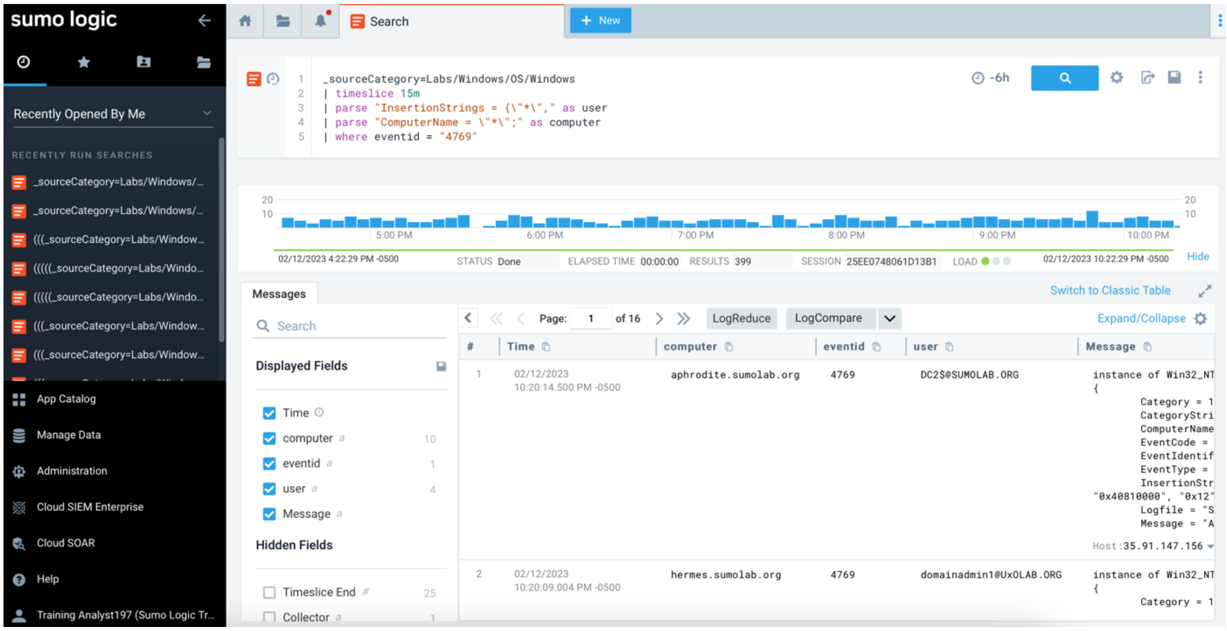

sumo logic
Search
New
Recently Opened By Me
RECENTLY RUN SEARCHES
(((((_sourceCategory=Labs/Windo...
(((((_sourceCategory=Labs/Windo...
(((_sourceCategory=Labs/Window...
(((_sourceCategory=Labs/Window...
(((_sourceCategory=Labs/Window...
((_sourceCategory=Labs/Windows...
((_sourceCategory=Labs/Windows...
App Catalog
Manage Data
Administration
Cloud SIEM Enterprise
Cloud SOAR
Help
Training Analyst197 (Sumo Logic Tr...
-6h
5
4:00 PM
5:00 PM
6:00 PM
7:00 PM
8:00 PM
9:00 PM
Hide
Messages
Aggregates
Switch to Classic Table
Page: 1 of 1
Time Compare
Add to Dashboard

```
(((((_sourceCategory=Labs/Windows/OS/Windows)))))
| parse "Account Name:\t\t*\n\tAccount" as account_name
| parse "Group Name:\t\t*\n\tGroup Domain" as group_name
| parse "Message = \"*." as message
| parse "ComputerName = \"*\";" as computer
| where eventid = "4728"
| where group_name = "Domain Admins"
| count by computer, message, eventid, group_name, account_name
```

02/12/2023 3:56:50 PM -0500 STATUS Done ELAPSED TIME 00:00:00 RESULTS 2 SESSION 44A449D166842D0D LOAD 02/12/2023 9:56:50 PM -0500

computer	message	eventid	group_name	account_na...	_count
oseidon.sumolab.org	A member was added to a security-enabled global group	4728	Domain Admins	domainadmin1	2

Detecting Compromised Accounts
Monitoring Events within every 15 minutes



```
_sourceCategory=Labs/Windows/OS/Windows
| timeslice 15m
| parse "InsertionStrings = {\"*\"," as user
| parse "ComputerName = \"*\";" as computer
| where eventid = "4769"
```

02/12/2023 4:22:29 PM -0500 STATUS Done ELAPSED TIME 00:00:00 RESULTS 399 SESSION 25EE0748061D13B1 LOAD 02/12/2023 10:22:29 PM -0500

Displayed Fields:

☑	Time	
☑	computer	10
☑	eventid	1
☑	user	4
☑	Message	

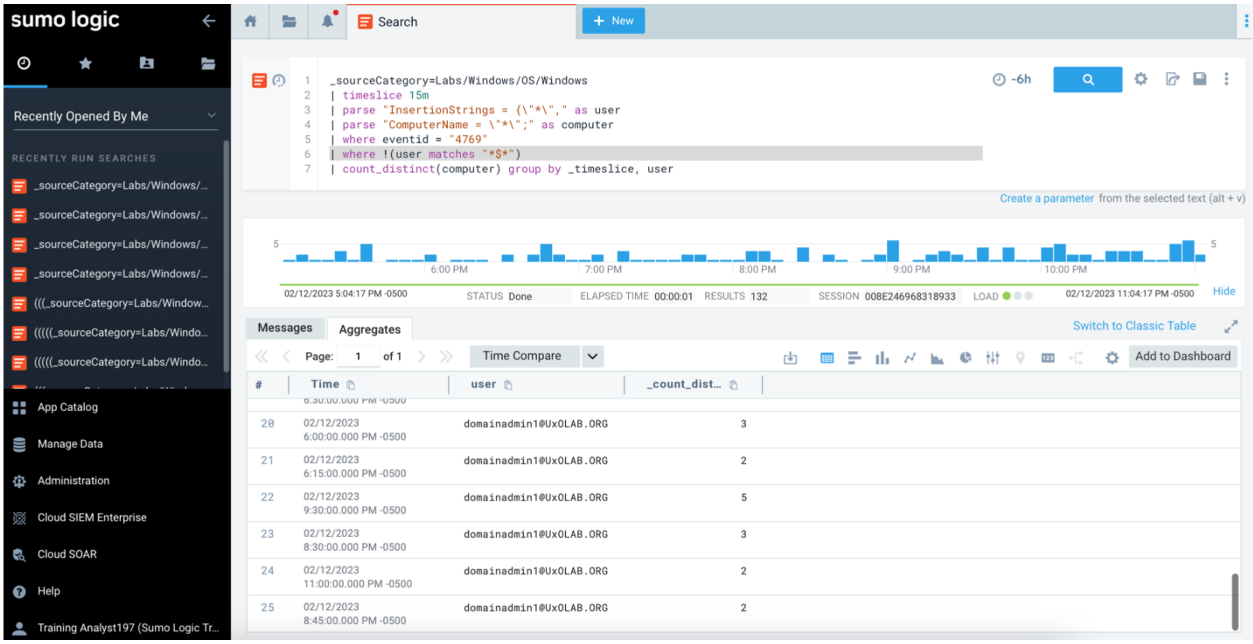
Hidden Fields:

□	Timeslice End	25
□	Collector	1

Page: 1 of 16

#	Time	computer	eventid	user	Message
1	02/12/2023 10:20:14.500 PM -0500	aphrodite.sumolab.org	4769	DC2$@SUMOLAB.ORG	instance of Win32_NT { Category = 1 CategoryStri ComputerName EventCode = EventIdentif EventType = InsertionStr "0x40810000", "0x12" Logfile = "S Message = "A Host:35.91.147.156
2	02/12/2023 10:20:09.004 PM -0500	hermes.sumolab.org	4769	domainadmin1@UxOLAB.ORG	instance of Win32_NT { Category = 1

Reviewing events associated with usernames with no "$" in them


sumo logic
Recently Opened By Me
RECENTLY RUN SEARCHES
_sourceCategory=Labs/Windows/...
_sourceCategory=Labs/Windows/...
_sourceCategory=Labs/Windows/...
_sourceCategory=Labs/Windows/...
(((_sourceCategory=Labs/Window...
((((_sourceCategory=Labs/Windo...
((((_sourceCategory=Labs/Windo...
App Catalog
Manage Data
Administration
Cloud SIEM Enterprise
Cloud SOAR
Help
Training Analyst197 (Sumo Logic Tr...
Search
New
-6h
Create a parameter from the selected text (alt + v)
5
6:00 PM
7:00 PM
8:00 PM
9:00 PM
10:00 PM
Hide
Messages
Aggregates
Switch to Classic Table
Time Compare
Add to Dashboard

```
_sourceCategory=Labs/Windows/OS/Windows
| timeslice 15m
| parse "InsertionStrings = {\"*\"," as user
| parse "ComputerName = \"*\";" as computer
| where eventid = "4769"
| where !(user matches "*$*")
| count_distinct(computer) group by _timeslice, user
```

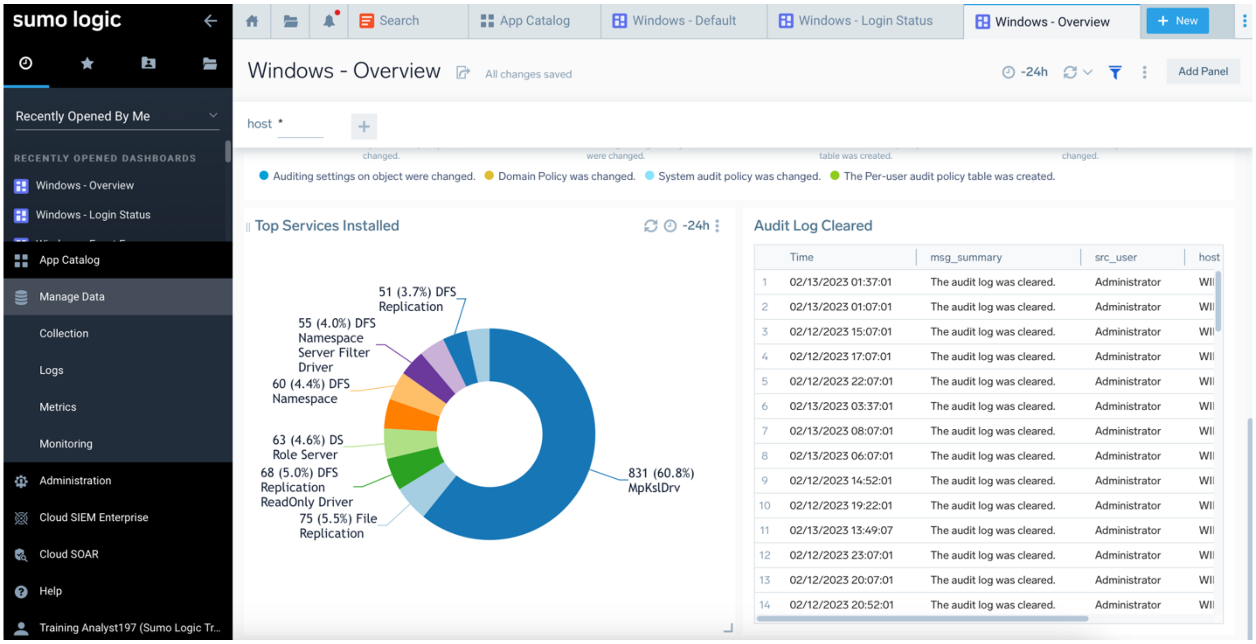
02/12/2023 5:04:17 PM -0500 STATUS Done ELAPSED TIME 00:00:01 RESULTS 132 SESSION 008E246968318933 LOAD 02/12/2023 11:04:17 PM -0500

Page: 1 of 1

#	Time	user	_count_dist...
	6:30:00.000 PM -0500		
20	02/12/2023 6:00:00.000 PM -0500	domainadmin1@UxOLAB.ORG	3
21	02/12/2023 6:15:00.000 PM -0500	domainadmin1@UxOLAB.ORG	2
22	02/12/2023 9:30:00.000 PM -0500	domainadmin1@UxOLAB.ORG	5
23	02/12/2023 8:30:00.000 PM -0500	domainadmin1@UxOLAB.ORG	3
24	02/12/2023 11:00:00.000 PM -0500	domainadmin1@UxOLAB.ORG	2
25	02/12/2023 8:45:00.000 PM -0500	domainadmin1@UxOLAB.ORG	2

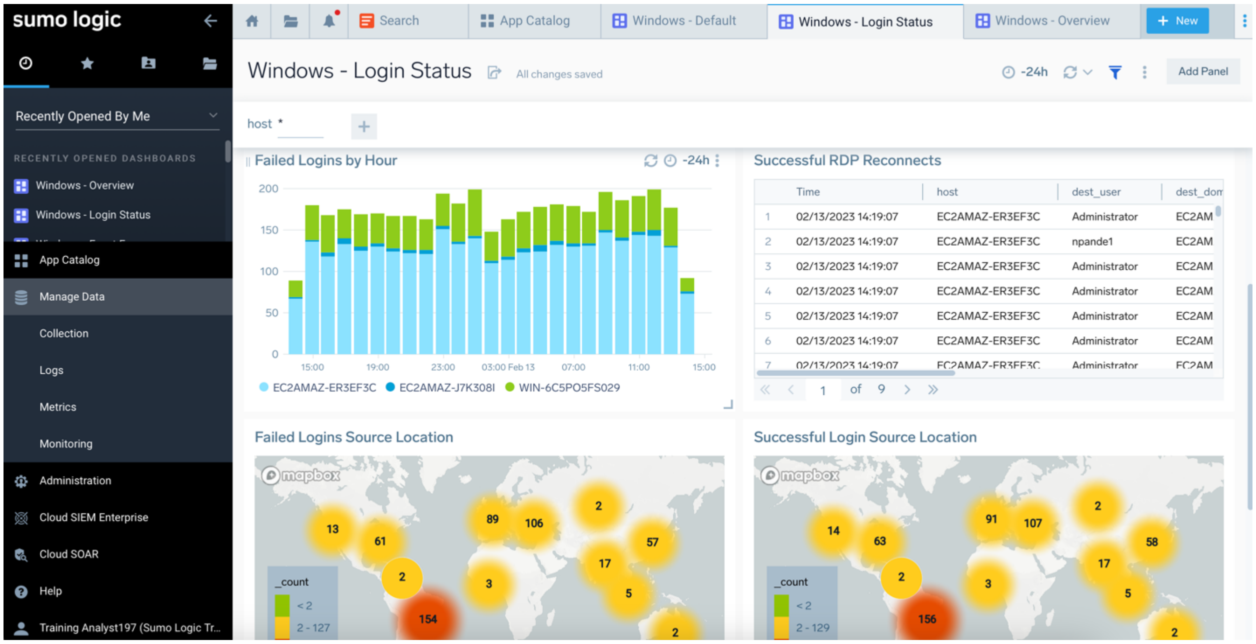
Dashboards

Windows Overview dashboard with details on audit log cleared and top installed services



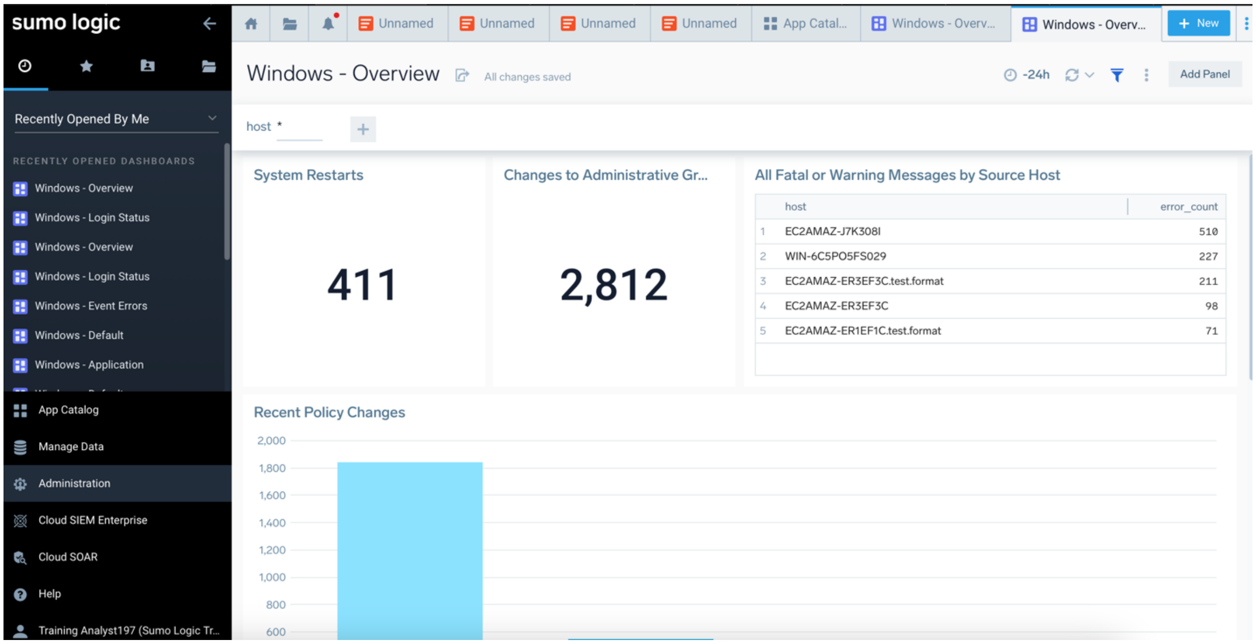
	Time	msg_summary	src_user	host
1	02/13/2023 01:37:01	The audit log was cleared.	Administrator	WII
2	02/13/2023 01:07:01	The audit log was cleared.	Administrator	WII
3	02/12/2023 15:07:01	The audit log was cleared.	Administrator	WII
4	02/12/2023 17:07:01	The audit log was cleared.	Administrator	WII
5	02/12/2023 22:07:01	The audit log was cleared.	Administrator	WII
6	02/13/2023 03:37:01	The audit log was cleared.	Administrator	WII
7	02/13/2023 08:07:01	The audit log was cleared.	Administrator	WII
8	02/13/2023 06:07:01	The audit log was cleared.	Administrator	WII
9	02/12/2023 14:52:01	The audit log was cleared.	Administrator	WII
10	02/12/2023 19:22:01	The audit log was cleared.	Administrator	WII
11	02/13/2023 13:49:07	The audit log was cleared.	Administrator	WII
12	02/12/2023 23:07:01	The audit log was cleared.	Administrator	WII
13	02/12/2023 20:07:01	The audit log was cleared.	Administrator	WII
14	02/12/2023 20:52:01	The audit log was cleared.	Administrator	WII

Windows Login Status Dashboard



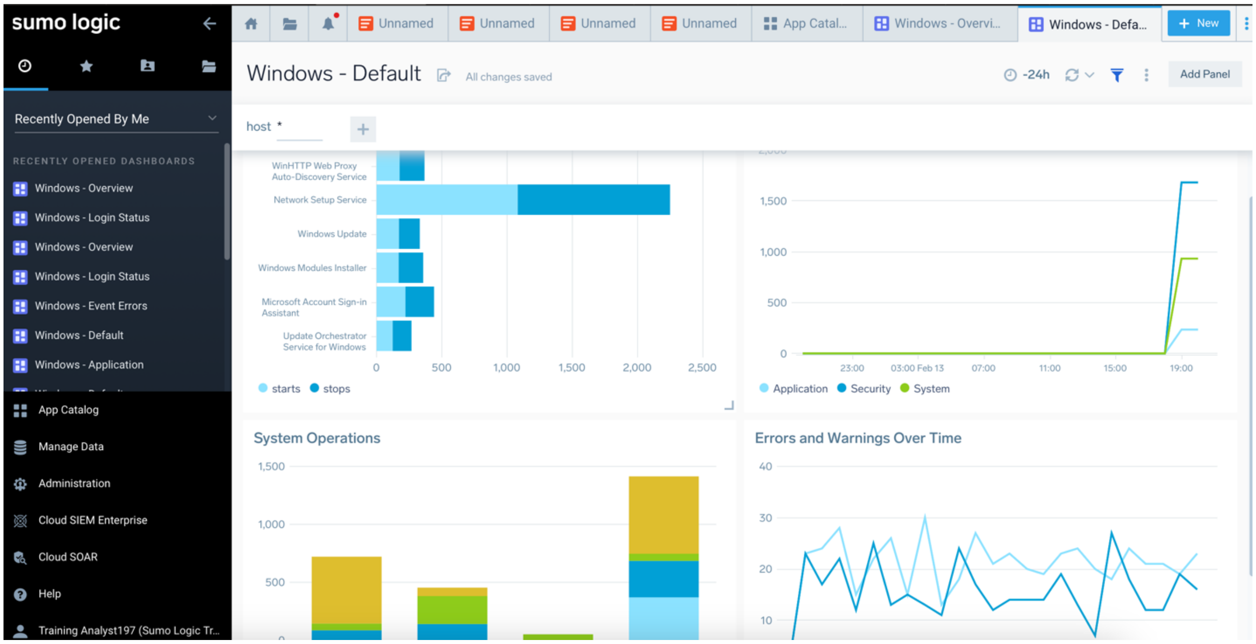
	Time	host	dest_user	dest_dom
1	02/13/2023 14:19:07	EC2AMAZ-ER3EF3C	Administrator	EC2AM
2	02/13/2023 14:19:07	EC2AMAZ-ER3EF3C	npande1	EC2AM
3	02/13/2023 14:19:07	EC2AMAZ-ER3EF3C	Administrator	EC2AM
4	02/13/2023 14:19:07	EC2AMAZ-ER3EF3C	Administrator	EC2AM
5	02/13/2023 14:19:07	EC2AMAZ-ER3EF3C	Administrator	EC2AM
6	02/13/2023 14:19:07	EC2AMAZ-ER3EF3C	Administrator	EC2AM
7	02/13/2023 14:19:07	EC2AMAZ-ER3EF3C	Administrator	EC2AM

Windows Overview Dashboard



	host	error_count
1	EC2AMAZ-J7K308I	510
2	WIN-6C5PO5FS029	227
3	EC2AMAZ-ER3EF3C.test.format	211
4	EC2AMAZ-ER3EF3C	98
5	EC2AMAZ-ER1EF1C.test.format	71

Windows Default Dashboard



Exercises

Audit Log cleared

1. Threat Simulation

To investigate such an event, it is essential that I customize alerts that will send notifications as soon as suspicious activity is detected. Clearing audit logs should not normally occur on a system. As such, could depict that suspicious activity has occurred. After receiving the alert, I will review all the logs within 12 hours (or to an extended time radius) from the time the alert was triggered. This will enable me to monitor all events that took place before the audit log was cleared and help me detect the activity that led to it and the user who cleared the logs. However, this will generate a massive number of logs that will be difficult and time-consuming to review. To this effect, I will use the "logreduce" button to summarize the logs. By using this function, sumo logic will build signatures for all the events that fall within the specified timeframe, reduce noises, and whilst it maintains the details of every event. It will also generate the number of times each signature occurs. This will help me find meaningful patterns and get to the root cause of the clearing of audit logs event. The windows review dashboard will be used to visualize the details of the event. I will assign a high criticality level. This is because clearing audit logs could be used to cover the tracks of a threat or malicious activity like malware. The incident will equally be documented.

2. Business Impacts

Short-term risks include the business will not be able to effectively troubleshoot unknown systems errors, track system damages, and security breaches. Generating digital evidence for legal issues will become a problem, the business can have issues with compliance with industry regulations, and millions of dollars could be lost to security breaches and non-compliance issues.

3. Remediation

Reduce auditing and security log management rights to only local system administrators, regularly install security patches, monitor events in real-time, and consistently check for changes in account roles and permissions.

Changes to Domain Admins

1. Threat simulation

To be able to attend to the situation in a timely fashion, I will first create an alert to send notifications to the security team the moment the event is logged. To focus on logs that are important to the event, I will limit my search to logs with event ID 4728 or 4729 and the group name "Domain Admins". This is because changes to the domain admin group could be in the form of adding a new member or removing an existing member from the group. To investigate the source of changes, I will set additional fields to collect the additional information such as the IP address and name of the host device used to make the changes, the name and ID of the domain admin who made the changes, and the details of the new member added to or removed from the group. By gathering this information, I will be able to determine the members who were legitimately added or removed and take the necessary action to address the event. I will use the windows overview dashboard to monitor domain admin changes to be able to determine the number of new members added and dropped at any given time. I will assign a high severity level to maliciously added members but a low severity level to an event where members were added by a legitimate administrator. An unauthorized change can lead to devastating consequences for the business.

2. Business Impacts

An unauthorized member added to the domain admin group can remove legitimate users and lock them out of the system. Such members can also steal sensitive information, shut down business systems, and privilege escalation to perform other malicious activities. Long-term risks include malware infections, financial loss from ransomware demands, and legal issues that result from unauthorized data access or exfiltration.

3. Remediation

Review and monitor all accounts in domain admin groups, install security patches in a timely fashion, and use Multi-Factor Authentication solutions.

Detecting Compromised User Accounts

1. Threat Simulation

Detecting compromised user accounts would require that I monitor the activities and details of each user account for patterns that could represent suspicious activities and send prompt notifications. To start with, I will monitor all logs within a particular time frame prior to and after the event. The logs prior to the alert will indicate actions that triggered the alert and the log after the event will provide insight on activities that were carried out by a compromised account. I will filter the logs using the event ID “4769”. This filter will however fetch the details of both compromised and uncompromised accounts. I will further filter my query results to detect user account names that deviate from how the windows operating system stores local system accounts. All the logs will be divided into time chunks to monitor unusual activities. After gathering all compromised accounts, I will use the “timecompare” function to trace the number of unique systems the compromised users have gained access to in the past. This will help me to trace their activities on such a system for potential security breaches or malicious activities. I will use the Windows login status dashboard and create a customized panel to track the systems the compromised accounts have a login to, the number of successful logins, the IP addresses, and the location from which they gained access. I will assign a high severity level. An incident response report will be written, and the threat intel will be updated.

2. Business Impacts

Short-term risks could be that highly privileged accounts can be used to steal sensitive business and user information, add new malicious members, or create a backdoor for future exploitations. The business can suffer from long-term risks such as financial loss from data exposure and ransomware, legal battles with compliance regulatory bodies, or loss of customers’ trust.

3. Remediation

Use multi-factor authentication to restrict access, block compromised accounts, encrypt business and client data with secure encryption algorithms, and train employees on security

References

Datadog (n.d). Audit Logging Overview. Retrieved February 10, 2023 from https://www.datadoghq.com/knowledge-center/audit-logging/

Macdonald, K. (2016, February 6). The security benefits of audit logging. Retrieved February 10, 2023 from https://www.digicert.com/blog/the-security-benefits-of-audit-logging

Metcalf, S (2016, January 1). Attack Methods for Gaining Domain Admin Rights in Active Directory. Retrieved February 12, 2023 from https://adsecurity.org/?p=2362

Microsoft (2022, December 21). Address compromised user accounts with automated investigation and response. Retrieved from February 10, 2023 from https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/address-compromised-users-quickly?view=o365-worldwide

Microsoft (2023, January 13). Manage auditing and security log. Retrieved February 12, 2023 from https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/manage-auditing-and-security-log