Cyber Security Task 2 – SOC Alert Monitoring & Incident Response

Overview

This task simulates the role of a Security Operations Center (SOC) analyst. The objective is to monitor security alerts, analyze suspicious activity, and document incident response actions using a SIEM platform.

Tools Used

- SIEM Tool Used
  - Splunk (Free Trial / Demo)
  - Website: https://www.splunk.com/

Both tools were used in combination to ensure accurate identification and validation of security issues.

1. Log Source

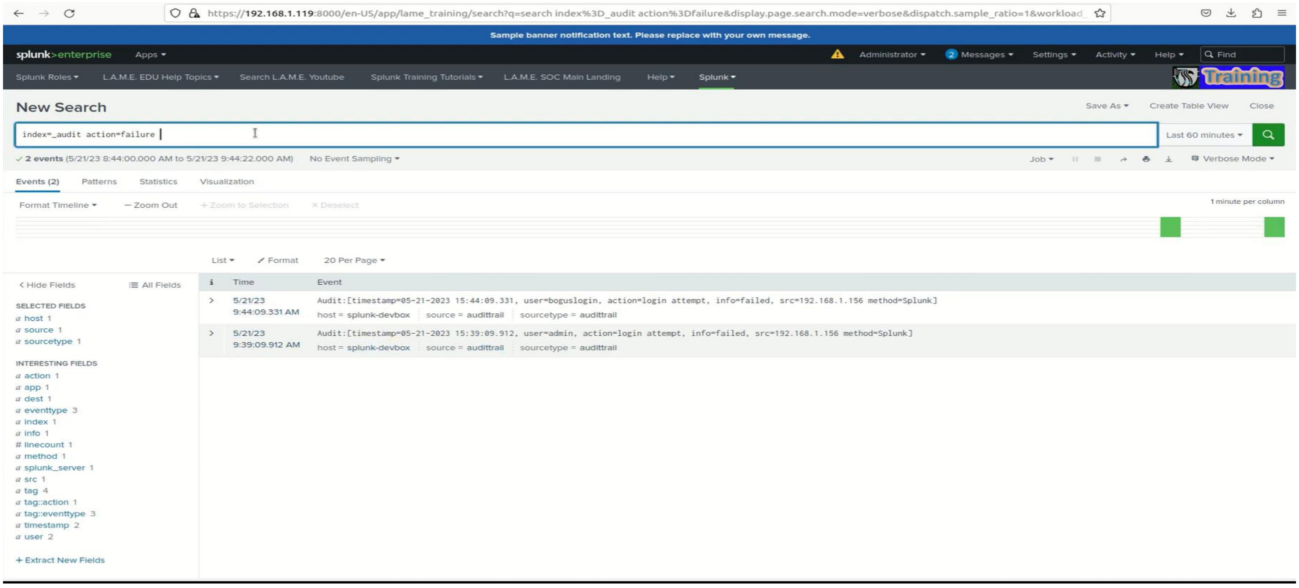
- Simulated SOC sample logs
- Authentication logs
- Network traffic logs
- Malware detection alerts

2. Identified Security Alerts

Alert 1: Multiple Failed Login Attempts

Severity: High

Description:Multiple failed login attempts were detected from an unknown IP address, indicating a possible brute-force attack.



https://192.168.1.119:8000/en-US/app/lame_training/search?q=search index%3D_audit action%3Dfailure&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload

Sample banner notification text. Please replace with your own message.

New Search

```
index=_audit action=failure
```

Last 60 minutes

✓ 2 events (5/21/23 8:44:00.000 AM to 5/21/23 9:44:22.000 AM) No Event Sampling

Verbose Mode

```
Time                     Event
5/21/23 9:44:09.331 AM   Audit:[timestamp=05-21-2023 15:44:09.331, user=boguslogin, action=login attempt, info=failed, src=192.168.1.156 method=Splunk]
                         host = splunk-devbox | source = audittrail | sourcetype = audittrail
5/21/23 9:39:09.912 AM   Audit:[timestamp=05-21-2023 15:39:09.912, user=admin, action=login attempt, info=failed, src=192.168.1.156 method=Splunk]
                         host = splunk-devbox | source = audittrail | sourcetype = audittrail
```

SELECTED FIELDS

```
a host 1
a source 1
a sourcetype 1
```

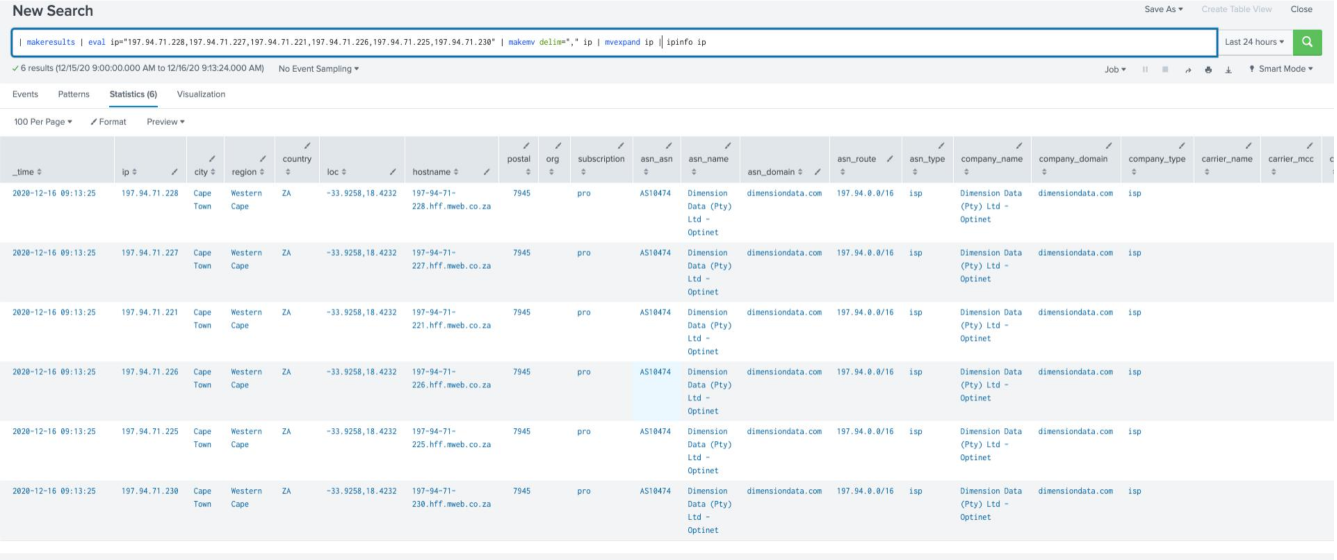
INTERESTING FIELDS

```
a action 1
a app 1
a dest 1
a eventtype 3
a index 1
a info 1
# linecount 1
a method 1
a splunk_server 1
a src 1
a tag 4
a tag::action 1
a tag::eventtype 3
a timestamp 2
a user 2
```

Alert 2: Login from Unusual IP Address

Severity: Medium

Description: A successful login was detected from an unfamiliar geographic location.



```
| makeresults | eval ip="197.94.71.228,197.94.71.227,197.94.71.221,197.94.71.226,197.94.71.225,197.94.71.230" | makemv delim="," ip | mvexpand ip | ipinfo ip
```

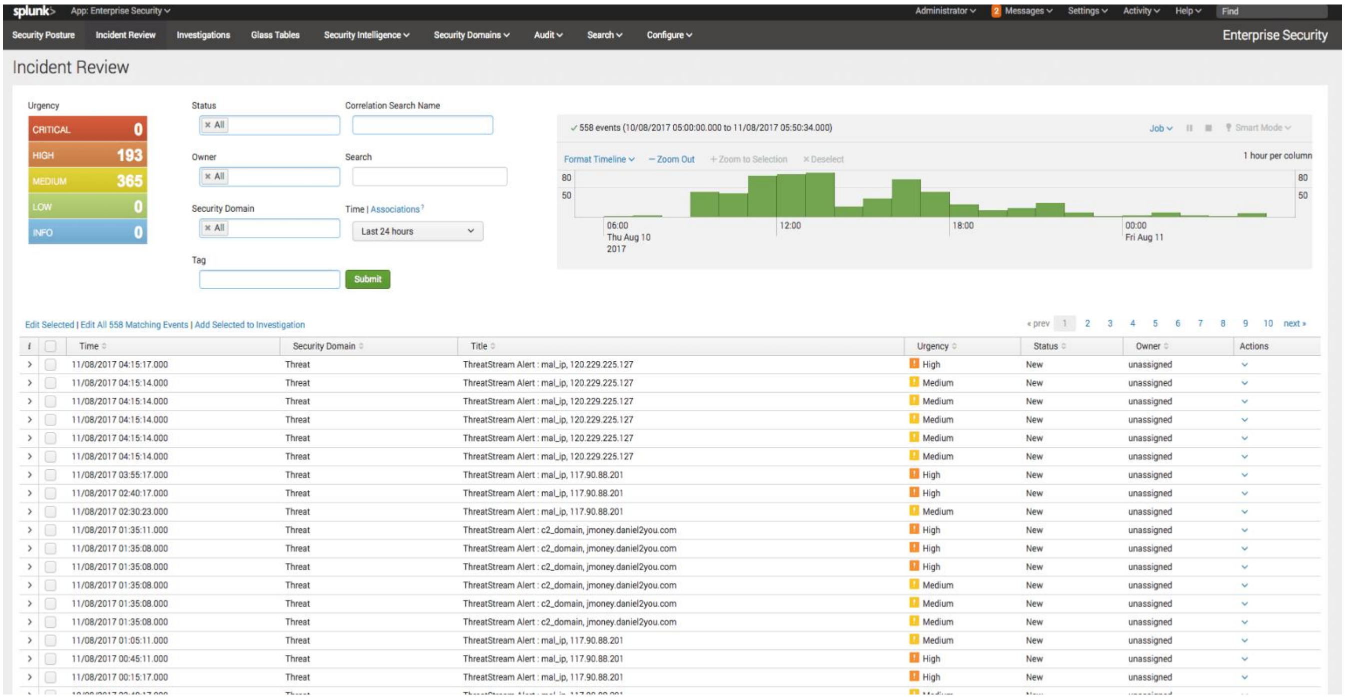
✓ 6 results (12/15/20 9:00:00.000 AM to 12/16/20 9:13:24.000 AM) No Event Sampling ▾

_time	ip	city	region	country	loc	hostname	postal	org	subscription	asn_asn	asn_name	asn_domain	asn_route	asn_type	company_name	company_domain	company_type	carrier_name	carrier_mcc
2020-12-16 09:13:25	197.94.71.228	Cape Town	Western Cape	ZA	-33.9258,18.4232	197-94-71-228.hff.mweb.co.za	7945		pro	AS10474	Dimension Data (Pty) Ltd - Optinet	dimensiondata.com	197.94.0.0/16	isp	Dimension Data (Pty) Ltd - Optinet	dimensiondata.com	isp		
2020-12-16 09:13:25	197.94.71.227	Cape Town	Western Cape	ZA	-33.9258,18.4232	197-94-71-227.hff.mweb.co.za	7945		pro	AS10474	Dimension Data (Pty) Ltd - Optinet	dimensiondata.com	197.94.0.0/16	isp	Dimension Data (Pty) Ltd - Optinet	dimensiondata.com	isp		
2020-12-16 09:13:25	197.94.71.221	Cape Town	Western Cape	ZA	-33.9258,18.4232	197-94-71-221.hff.mweb.co.za	7945		pro	AS10474	Dimension Data (Pty) Ltd - Optinet	dimensiondata.com	197.94.0.0/16	isp	Dimension Data (Pty) Ltd - Optinet	dimensiondata.com	isp		
2020-12-16 09:13:25	197.94.71.226	Cape Town	Western Cape	ZA	-33.9258,18.4232	197-94-71-226.hff.mweb.co.za	7945		pro	AS10474	Dimension Data (Pty) Ltd - Optinet	dimensiondata.com	197.94.0.0/16	isp	Dimension Data (Pty) Ltd - Optinet	dimensiondata.com	isp		
2020-12-16 09:13:25	197.94.71.225	Cape Town	Western Cape	ZA	-33.9258,18.4232	197-94-71-225.hff.mweb.co.za	7945		pro	AS10474	Dimension Data (Pty) Ltd - Optinet	dimensiondata.com	197.94.0.0/16	isp	Dimension Data (Pty) Ltd - Optinet	dimensiondata.com	isp		
2020-12-16 09:13:25	197.94.71.230	Cape Town	Western Cape	ZA	-33.9258,18.4232	197-94-71-230.hff.mweb.co.za	7945		pro	AS10474	Dimension Data (Pty) Ltd - Optinet	dimensiondata.com	197.94.0.0/16	isp	Dimension Data (Pty) Ltd - Optinet	dimensiondata.com	isp		

Alert 3: Malware Detection on Endpoint

Severity: High

Description: The SIEM tool detected a malware alert on a user endpoint.



Urgency	
CRITICAL	0
HIGH	193
MEDIUM	365
LOW	0
INFO	0

Status: × All

Correlation Search Name:

Owner: × All

Search:

Security Domain: × All

Time | Associations: Last 24 hours

Tag:

✓ 558 events (10/08/2017 05:00:00.000 to 11/08/2017 05:50:34.000)

i	□	Time	Security Domain	Title	Urgency	Status	Owner	Actions
›	□	11/08/2017 04:15:17.000	Threat	ThreatStream Alert : mal_ip, 120.229.225.127	High	New	unassigned	⌄
›	□	11/08/2017 04:15:14.000	Threat	ThreatStream Alert : mal_ip, 120.229.225.127	Medium	New	unassigned	⌄
›	□	11/08/2017 04:15:14.000	Threat	ThreatStream Alert : mal_ip, 120.229.225.127	Medium	New	unassigned	⌄
›	□	11/08/2017 04:15:14.000	Threat	ThreatStream Alert : mal_ip, 120.229.225.127	Medium	New	unassigned	⌄
›	□	11/08/2017 04:15:14.000	Threat	ThreatStream Alert : mal_ip, 120.229.225.127	Medium	New	unassigned	⌄
›	□	11/08/2017 04:15:14.000	Threat	ThreatStream Alert : mal_ip, 120.229.225.127	Medium	New	unassigned	⌄
›	□	11/08/2017 03:55:17.000	Threat	ThreatStream Alert : mal_ip, 117.90.88.201	High	New	unassigned	⌄
›	□	11/08/2017 02:40:17.000	Threat	ThreatStream Alert : mal_ip, 117.90.88.201	High	New	unassigned	⌄
›	□	11/08/2017 02:30:23.000	Threat	ThreatStream Alert : mal_ip, 117.90.88.201	Medium	New	unassigned	⌄
›	□	11/08/2017 01:35:11.000	Threat	ThreatStream Alert : c2_domain, jmoney.daniel2you.com	High	New	unassigned	⌄
›	□	11/08/2017 01:35:08.000	Threat	ThreatStream Alert : c2_domain, jmoney.daniel2you.com	High	New	unassigned	⌄
›	□	11/08/2017 01:35:08.000	Threat	ThreatStream Alert : c2_domain, jmoney.daniel2you.com	High	New	unassigned	⌄
›	□	11/08/2017 01:35:08.000	Threat	ThreatStream Alert : c2_domain, jmoney.daniel2you.com	Medium	New	unassigned	⌄
›	□	11/08/2017 01:35:08.000	Threat	ThreatStream Alert : c2_domain, jmoney.daniel2you.com	Medium	New	unassigned	⌄
›	□	11/08/2017 01:35:08.000	Threat	ThreatStream Alert : c2_domain, jmoney.daniel2you.com	Medium	New	unassigned	⌄
›	□	11/08/2017 01:05:11.000	Threat	ThreatStream Alert : mal_ip, 117.90.88.201	Medium	New	unassigned	⌄
›	□	11/08/2017 00:45:11.000	Threat	ThreatStream Alert : mal_ip, 117.90.88.201	High	New	unassigned	⌄
›	□	11/08/2017 00:15:17.000	Threat	ThreatStream Alert : mal_ip, 117.90.88.201	High	New	unassigned	⌄

3. Incident Response Actions

- Reviewed alerts using SIEM dashboards
- Analyzed source IP addresses and affected accounts
- Simulated blocking of malicious IPs
- Recommended password reset and endpoint malware scan.

5. Threat Classification

- Brute Force Authentication Attack
- Suspicious Network Activity
- Malware Infectionon

Conclusion

This project demonstrates basic SOC operations including alert monitoring, threat analysis, and incident response simulation using a SIEM platform.