

GRID-SIEM SD GROUP

29 SPRING '24

Trent Bickford
Westin Chamberlain
Ella Cook
Daniel Ocampo

Security Onion Work

- Launched a ping to see where the alert ends up in SOC
- Tools in the dashboard allow to see details like source, destination, message, and time

Count	rule.name	event.module	event.severity_label
104	ET INFO Observed Cloudflare DNS over HTTPS Domain (cloudflare-dns .com in TLS SNI)	suricata	low
8	GPL ICMP_INFO PING *NIX	suricata	low

Rows per page: 50 1-2 of 2

2024-02-21 09:54:51.672 +00:00	192.168.1.111	47326	172.64.41.4	443	ET INFO Observed Cloudflare DNS over HTTPS Domain (cloudflare-dns .com in TLS SNI)	Misc activity
@timestamp	2024-02-21T09:54:51.672Z					
@version	1					
data_stream.dataset	suricata					
data_stream.namespace	so					
data_stream.type	logs					
destination.geo.continent_name	North America					
destination.geo.country_iso_code	US					
destination.geo.country_name	United States					
destination.geo.ip	172.64.41.4					
destination.geo.location.lat	37.751					
destination.geo.location.lon	-97.822					
destination.geo.timezone	America/Chicago					
destination.ip	172.64.41.4					
destination.port	443					
destination_geo.asn	13335					

Security Onion Work

- Looking at the dashboard, the source for the files look like a docker
- Checked the dockers and that may be where the logs are being stored

soc_type	
soc_timestamp	2024-02-21T09:45:10.486Z
soc_source	ubuntu-vm-master-120:.ds-logs-zeek-so-2024.02.14-000004

ghcr.io/security-onion-solutions/so-zeek	2.4.20	5131d05b4e17	4 months ago	1.66GB
ubuntu-vm-master-120:5000/security-onion-solutions/so-zeek	2.4.20	5131d05b4e17	4 months ago	1.66GB
ghcr.io/security-onion-solutions/so-influxdb	2.4.20	bb1b78726766	4 months ago	474MB
ubuntu-vm-master-120:5000/security-onion-solutions/so-influxdb	2.4.20	bb1b78726766	4 months ago	474MB
ghcr.io/security-onion-solutions/so-strelka-backend	2.4.20	6111e543c635	4 months ago	2.63GB
ubuntu-vm-master-120:5000/security-onion-solutions/so-strelka-backend	2.4.20	6111e543c635	4 months ago	2.63GB
ghcr.io/security-onion-solutions/so-suricata	2.4.20	726c778cda2d	4 months ago	845MB
ubuntu-vm-master-120:5000/security-onion-solutions/so-suricata	2.4.20	726c778cda2d	4 months ago	845MB
ghcr.io/security-onion-solutions/so-elastic-fleet-package-registry	2.4.20	20a389014777	4 months ago	600MB

ML Updates

- Got script to run with help from Westin
 - Yesterday
- Next Steps
 - Need to work on accuracy of the script and running the proper conn.logs through it
 - Need to focus on getting multiple logs to run through and then analyze since it is currently running based on the specific path to a single particular log
 - Need to add functionality to ingest zipped logs since it required unzipping the logs before ingestion

```
/home/ubuntu/Desktop/impzeek1/logssensor1/logs/2024-02-17
Random Forest Results:
      precision    recall  f1-score   support

     0       1.00      1.00      1.00         7
     1       1.00      1.00      1.00         3
     2       1.00      1.00      1.00         3
     3       1.00      1.00      1.00        30

 accuracy          1.00          1.00          1.00          43
 macro avg          1.00          1.00          1.00          43
weighted avg          1.00          1.00          1.00          43

Accuracy: 1.0

Isolation Forest Results:
/home/ubuntu/anaconda3/lib/python3.10/site-packages/sklearn/metrics/_
_warn_prf(average, modifier, f"{metric.capitalize()} is", len(result
/home/ubuntu/anaconda3/lib/python3.10/site-packages/sklearn/metrics/_
_warn_prf(average, modifier, f"{metric.capitalize()} is", len(result
/home/ubuntu/anaconda3/lib/python3.10/site-packages/sklearn/metrics/_
_warn_prf(average, modifier, f"{metric.capitalize()} is", len(result
      precision    recall  f1-score   support

     0       0.17      1.00      0.29         7
     1       0.00      0.00      0.00         3
     2       0.00      0.00      0.00         3
     3       0.00      0.00      0.00        30

 accuracy          0.16          0.25          0.05          43
 macro avg          0.04          0.25          0.07          43
weighted avg          0.03          0.16          0.05          43

Accuracy: 0.16279069767441862
(base) ubuntu@ubuntu-vm-master-120:~/Desktop$
```

Attacking updates

Format for running a task

- \$action = New-ScheduledTaskAction -Execute 'Powershell.exe' -Argument '-ExecutionPolicy Bypass -File "C:\path\to\your\script\MyScript.ps1"'
- \$trigger = New-ScheduledTaskTrigger -Daily -At 3am
- \$settings = New-ScheduledTaskSettingsSet -Hidden -StartWhenAvailable
- Register-ScheduledTask -TaskName "MyScheduledTask" -Action \$action -Trigger \$trigger -Settings \$settings -Description "This task runs MyScript.ps1 daily at 3am"

With this I could run automatic attacks from the internal machines

Powershell script would look like

- Start-Process -FilePath "C:\path\to\file.exe" -NoNewWindow

Attacking Questions

- What should I aim for when developing future attacks?
 - Less stuff with establishing permanence on internal systems?
 - More stuff from the kali box?
- What attacks would you recommend attempting?
- Any updates on caldera?
- Still cant ping or attack substation 2