GRID-SIEM SD GROUP 29 SPRING '24

Trent Bickford

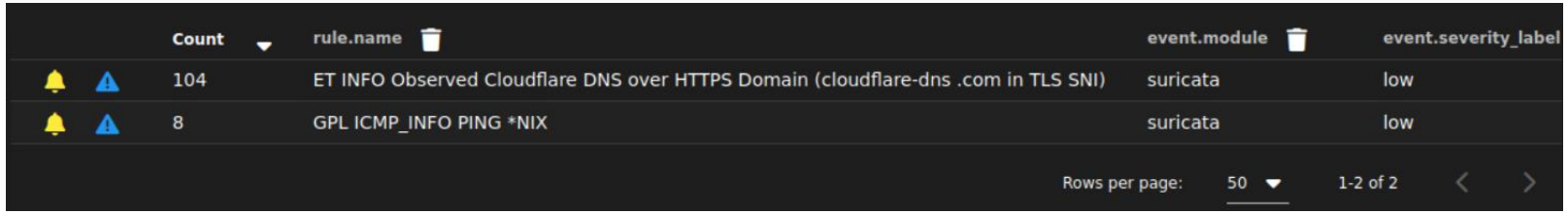
Westin Chamberlain

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

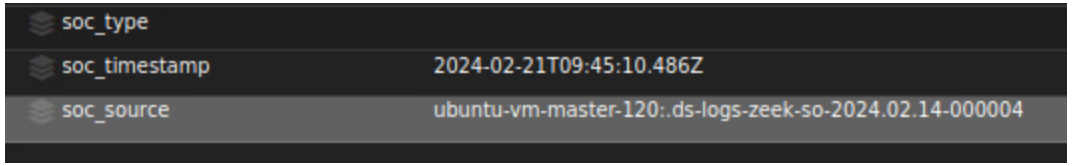
Rows per page: 50 1-2 of 2

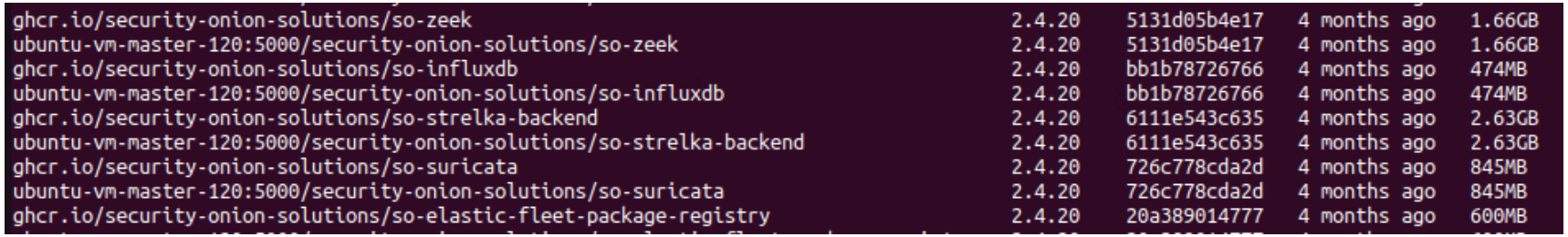
2024-02-21 09:54:51.672 +00:00 192.168.1.111 47326 172.64.41.4 443 ET INFO Observed Cloudflare DNS over HTTPS Domain (cloudflare-dns .com in TLS SNI) Misc activity

@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

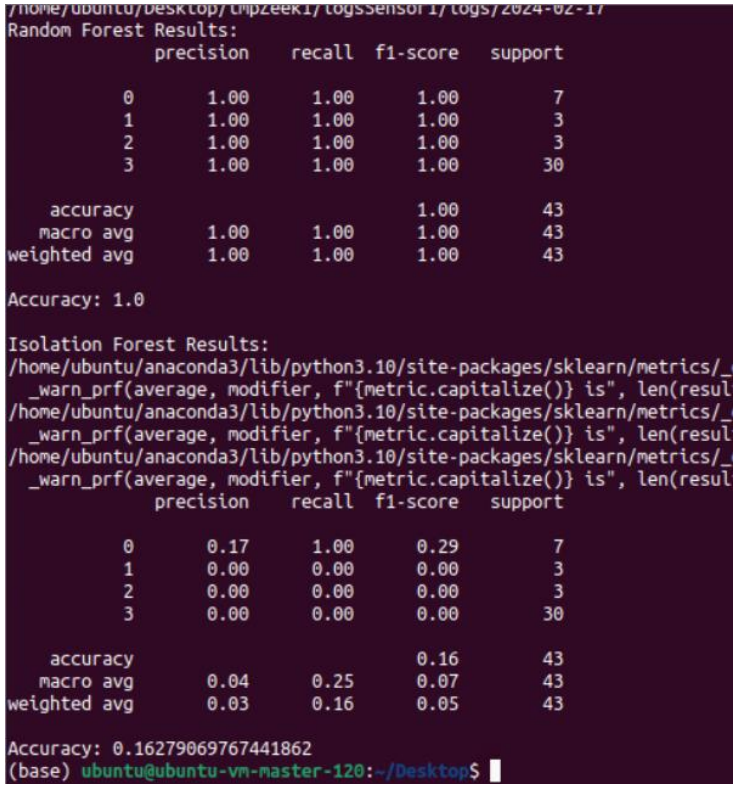




ML Updates

- 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



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