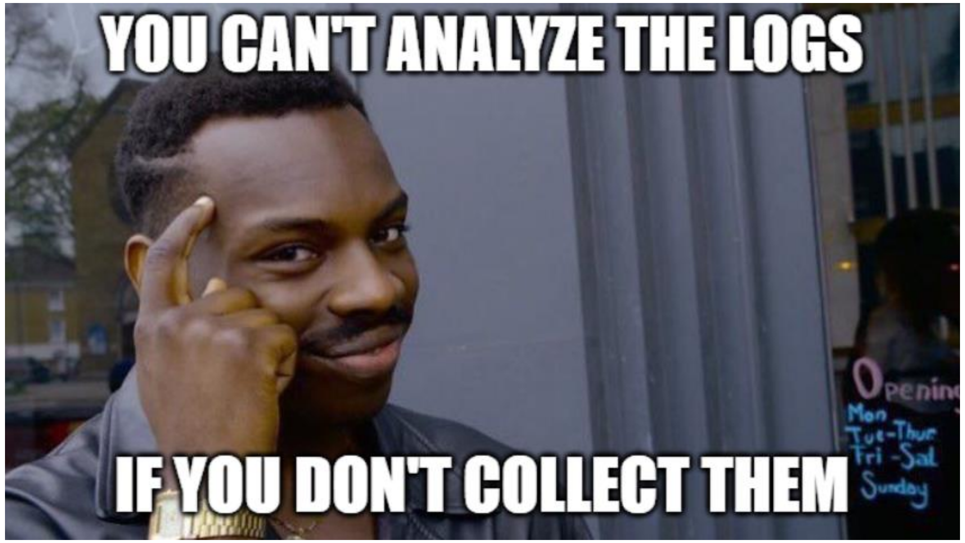
Building a better SIEM

Without paying for it

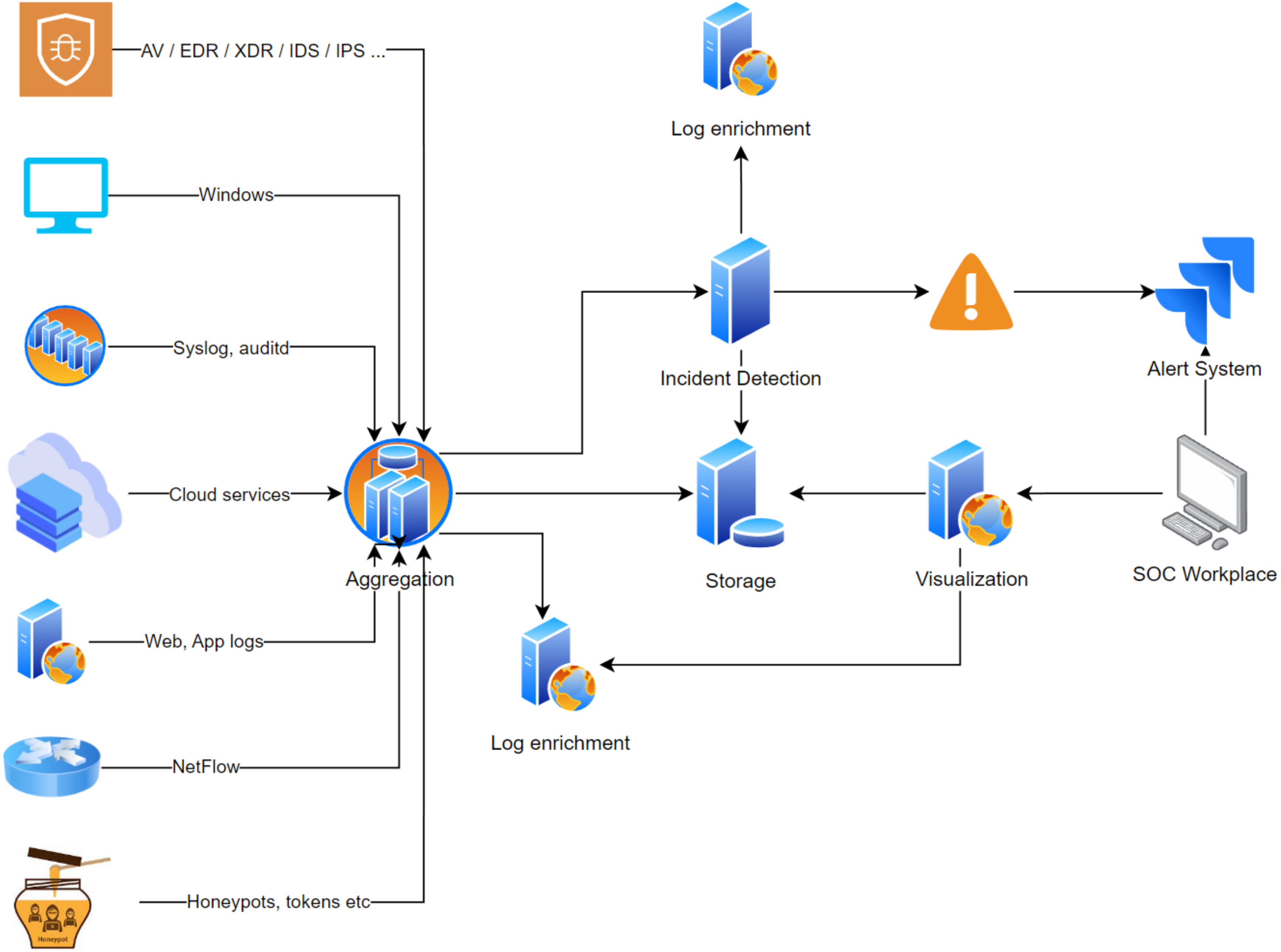
Sergey Egorov

Why SIEM?

- Log collection and central storage location
- Incident detection through malicious log patterns and log corelation
- Alert aggregation
- Incident investigation
- Compliance
- Non-threat related data analysis and management



What SIEM?



Sergey Egorov

Community SIEM offerings

Elastic Stack

graylog

wazuh.

OSSEC

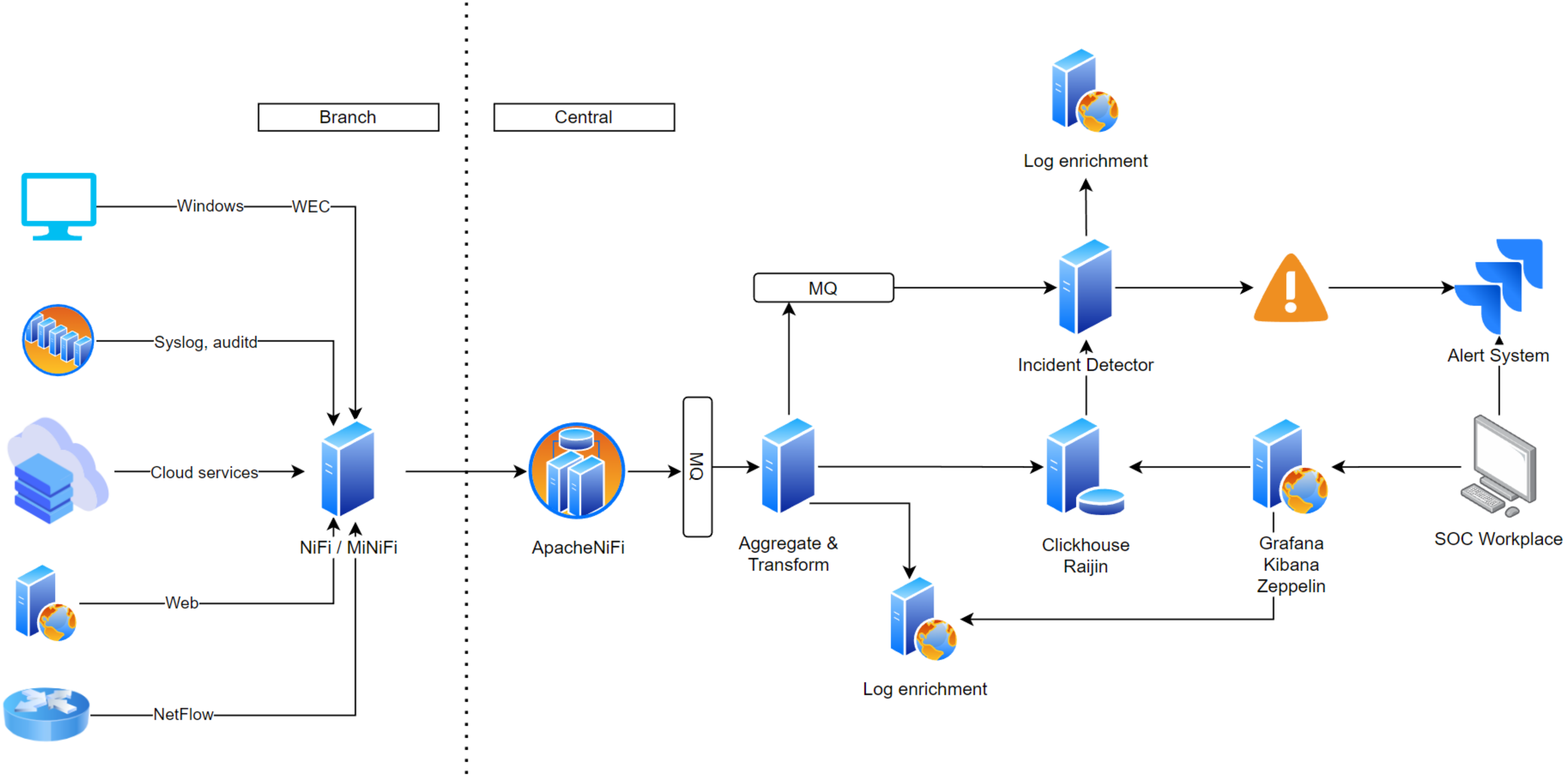
POCKETSIEM ☺

NXLog

Challenges

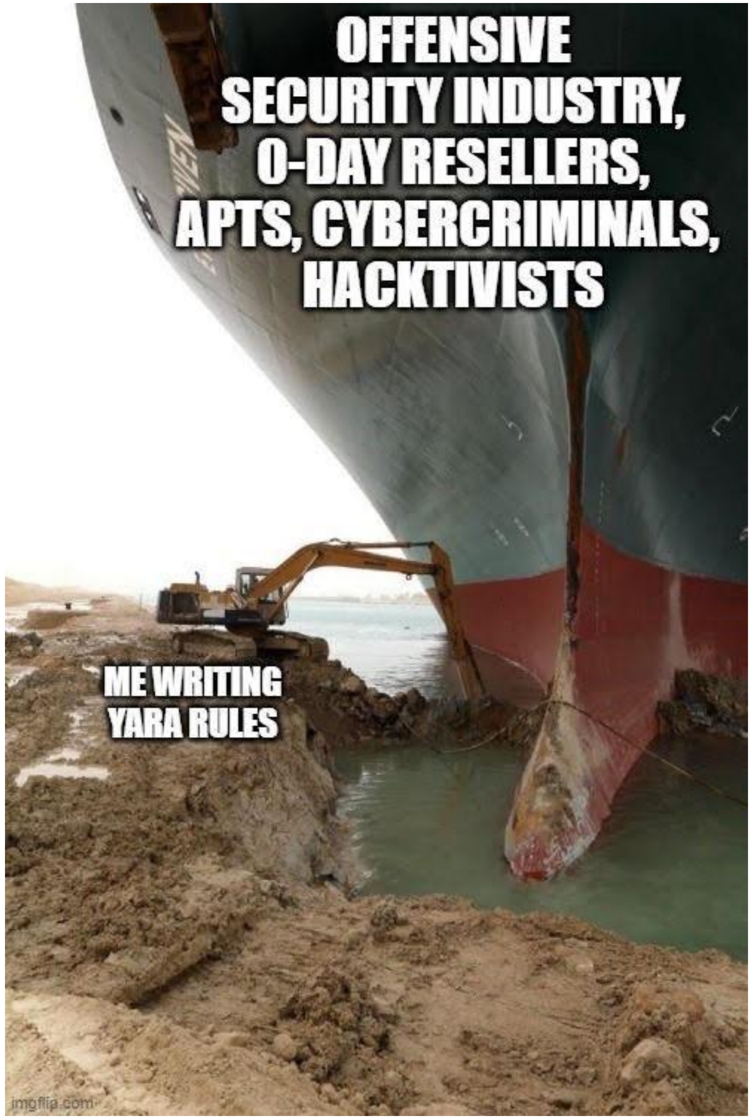
- Stick to the vendor with limitations and T&C
- Most useful features are in paid version
- May not support the log format you need
- Elasticsearch DB is very resource consuming
- Partial scaling is difficult
- Collecting logs from remote branches and clients is not straightforward

Agentless SIEM



Sergey Egorov

SIEM Detection

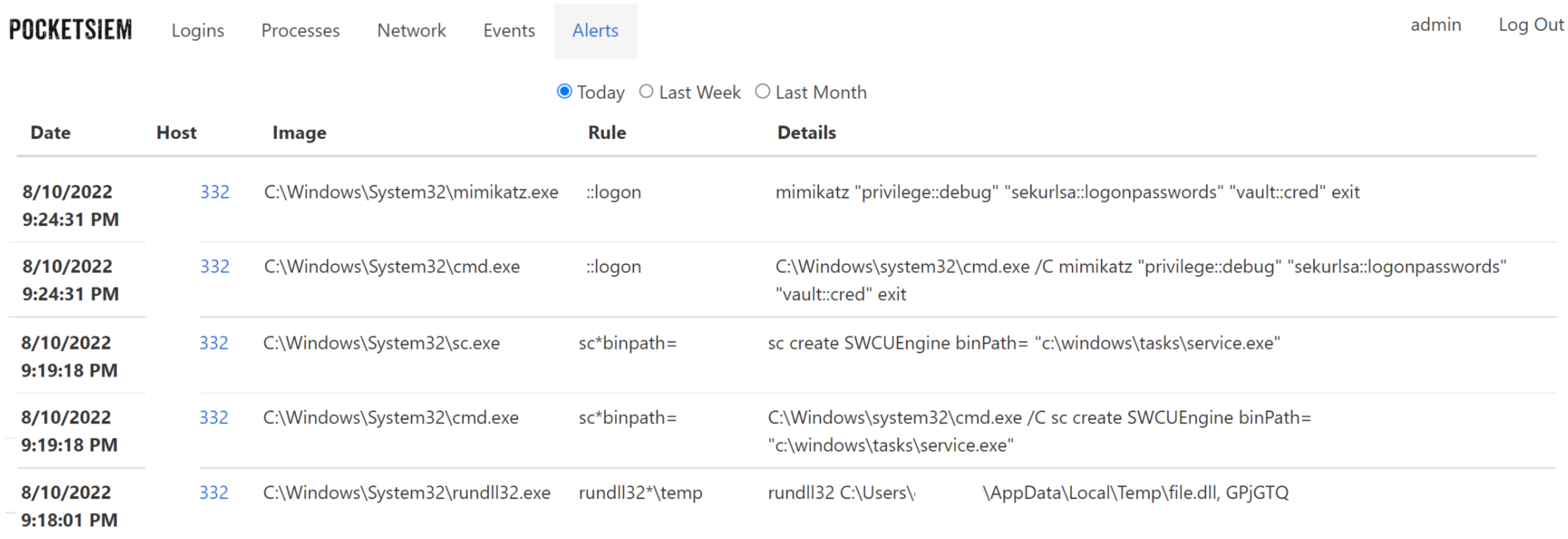

OFFENSIVE SECURITY INDUSTRY, 0-DAY RESELLERS, APTS, CYBERCRIMINALS, HACKTIVISTS
ME WRITING YARA RULES
imgflip.com

- Real-time vs Periodic
- MITRE Attack & Defend mappings
- Public rules (Sigma, Yara etc.)
- Custom pattern and log correlation rules
- Anomaly detection / ML
- TI Platforms (MIPS, Yeti, OpenCTI, ThreatMiner, VirusTotal and a lot more)

POCKETSIEM

Available at:
https://github.com/cepxeo/PocketSIEM

- Simplified SIEM functionality
- Collects and processes Sysmon events
- Over 1500 Sigma and custom rules
- For researches and CTFs
- For personal and ad hoc IR



● Today ○ Last Week ○ Last Month

Date	Host	Image	Rule	Details
8/10/2022 9:24:31 PM	332	C:\Windows\System32\mimikatz.exe	::logon	mimikatz "privilege::debug" "sekurlsa::logonpasswords" "vault::cred" exit
8/10/2022 9:24:31 PM	332	C:\Windows\System32\cmd.exe	::logon	C:\Windows\system32\cmd.exe /C mimikatz "privilege::debug" "sekurlsa::logonpasswords" "vault::cred" exit
8/10/2022 9:19:18 PM	332	C:\Windows\System32\sc.exe	sc*binpath=	sc create SWCUEngine binPath= "c:\windows\tasks\service.exe"
8/10/2022 9:19:18 PM	332	C:\Windows\System32\cmd.exe	sc*binpath=	C:\Windows\system32\cmd.exe /C sc create SWCUEngine binPath= "c:\windows\tasks\service.exe"
8/10/2022 9:18:01 PM	332	C:\Windows\System32\rundll32.exe	rundll32*\temp	rundll32 C:\Users\ \AppData\Local\Temp\file.dll, GPjGTQ

Considerations

- Plan for heavy load at the log aggregation, real-time detection and database write / read points
- Collect logs based on use cases and periodically review
- Map detection rules to MITRE and actualize
- Detection by patterns + correlation + deception + external systems alerts is good combination
- Purple team to test detection and blind spots, Red Team to check IR