SOC (Security Operation Center)
ELK SIEM Guide

Presenter: JEN-SHENG, SHI

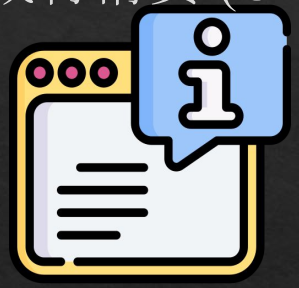
Outlook

- SOC 與常見 SOC 架構介紹
  - SOC 是什麼
  - SIEM、SORA、CTI
  - SIEM Endpoint Monitoring
- SIEM 建置教學
- Kibana Dashboard 資料視覺化

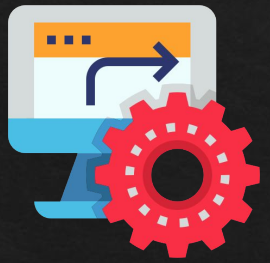
What’s SOC ?

- SOC (Security Operation Center)
- SIEM (事件管理)

- 威脅情資 (CTI)



- SORA (事件響應)



- 合規性管理

- SIEM (事件管理)

- SIEM 只是一個概念
- SIEM 目標在於監控、管理大量的服務
- 事件包括但不限於：系統日誌、網絡封包
- 解決方案:
  - 大多由資料庫、管理系統組成
  - 大多使用非關聯式資料庫
  - 管理系統通常具備警報、資料庫查詢
  - 最近大多公司的 SIEM 會掛個 AI


Elastic Search


WAZUH


OpenSearch


Security Command
Center


Chronicle

有關告警那件大事！

- 想像一下你是一間公司的資安長
- 你要負責一間公司的資安監控
- 但一台機器每分鐘就有幾千筆系統日誌
- 人類哪看得完阿！
- 有沒有辦法設定規則, 讓管理系統自己偵測就好了呢?

有關於偵測規則 - SigmaRule

```yaml
title: Vulnerable Driver Load
id: 7aaaf4b8-e47c-4295-92ee-6ed40a6f60c8
status: test
description: Detects loading of known vulnerable drivers via their hash.
references:
    - https://loldrivers.io/
author: Nasreddine Bencherchali (Nextron Systems)
date: 2022-08-18
modified: 2023-12-02
tags:
    - attack.privilege-escalation
    - attack.t1543.003
    - attack.t1068
logsource:
    product: windows
    category: driver_load
detection:
    selection:
        Hashes|contains:
            - 'MD5=c996d7971c49252c582171d9380360f2'
            - 'MD5=da7e98b23b49b7293ee06713032c74f6'
            - 'IMPHASH=fbfa302bf7eb5d615d0968541ee49ce4'
            - 'IMPHASH=f9b9487f25a2c1e08c02f391387c5323'
            - 'IMPHASH=ef102e058f6b88af0d66d26236257706'
            - 'IMPHASH=0f371a913e9fa3ba3a923718e489debb'
        condition: selection
    falsepositives:
        - Unknown
    level: high
```

Search site

About Premium

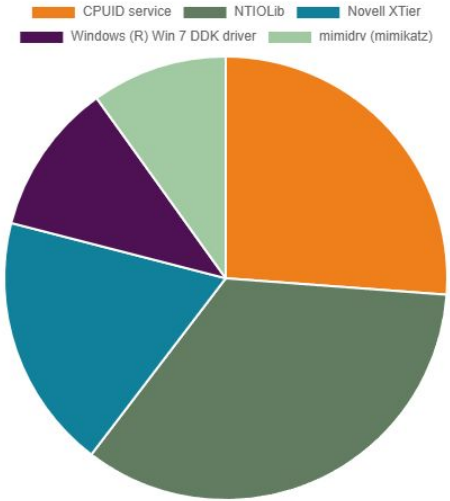
Living Off The Land Drivers

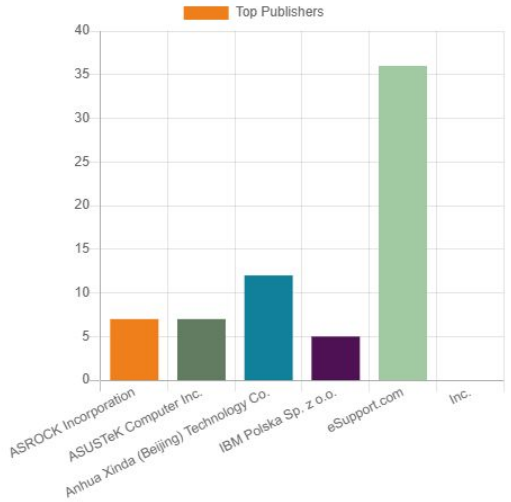
Living Off The Land Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks. The project helps security professionals stay informed and mitigate potential threats.

Feel free to open a PR, raise an issue(s) or request new driver(s) be added.

You can also get the malicious driver list via **API** using CSV or JSON. Sysmon users check out the pre-built config. There is a Sigma rule for SIEMs. If you've found this project valuable, you'll absolutely love our sister projects, LOLBAS and GTFOBins, check them out!

Top Products

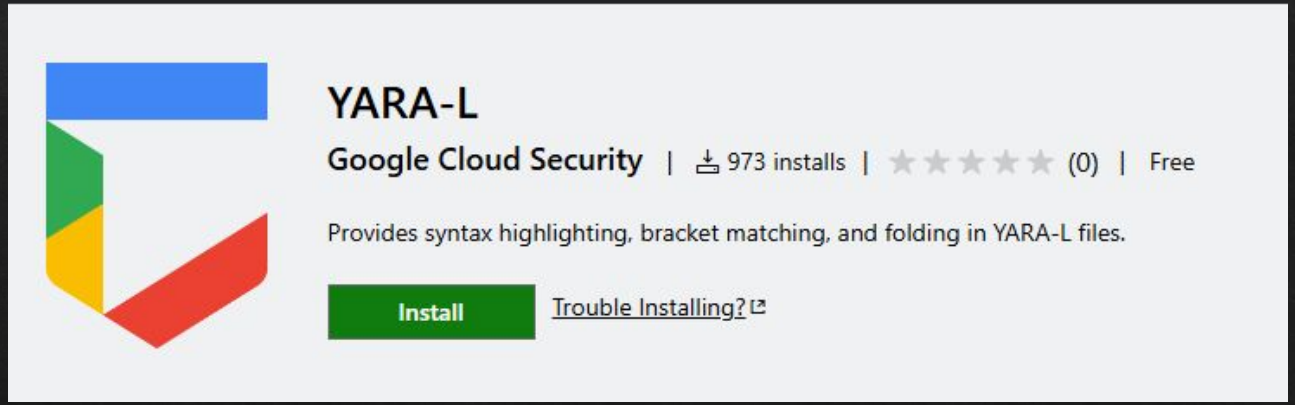




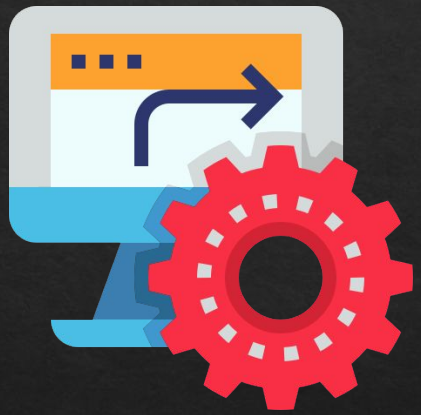
偵測規則的體系


SIGMA
RULE


/* YARA */

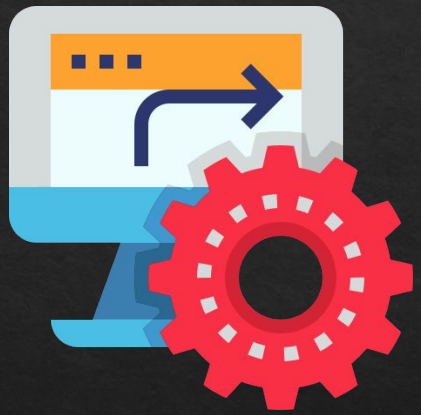

YARA-L
Google Cloud Security | 973 installs | (0) | Free
Provides syntax highlighting, bracket matching, and folding in YARA-L files.
Install
Trouble Installing?

- SORA (事件響應)



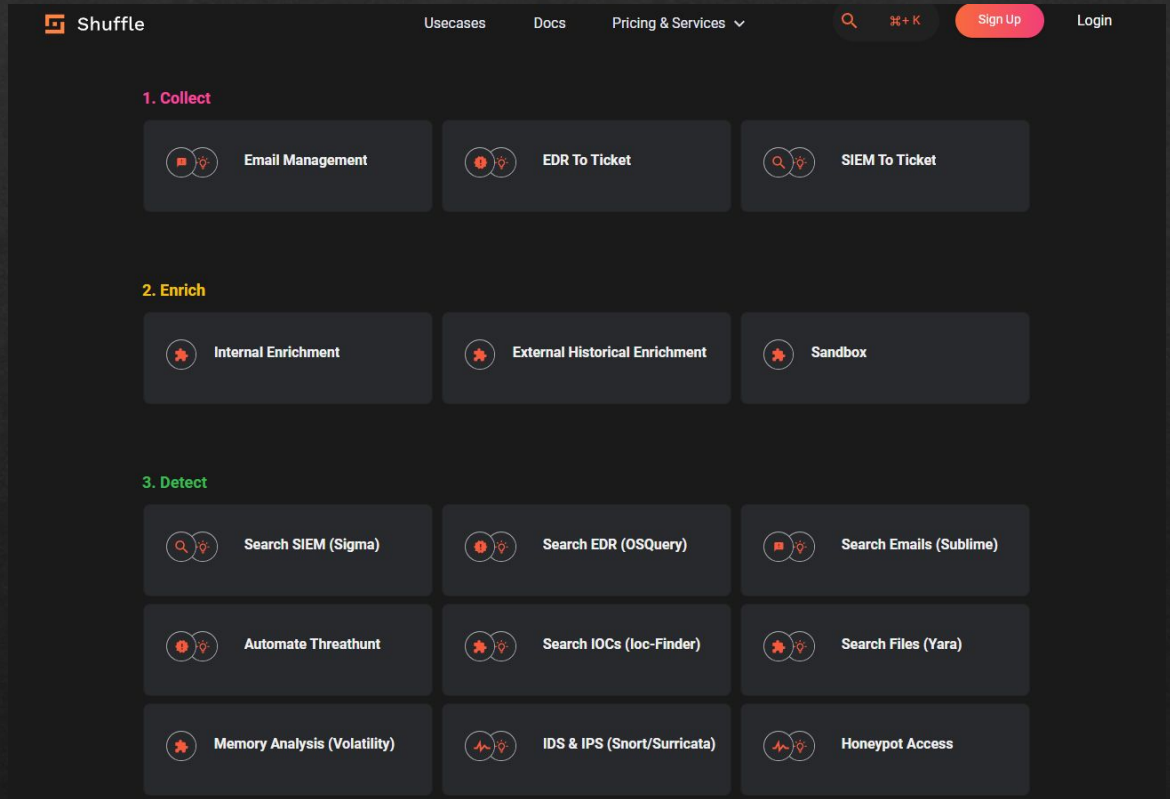
- SORA 只是一個概念
- SORA 目標當出現事件時, 進行自動化應變
- 舉凡如 資安事件、SIEM 告警
- 解決方案:
  - ？ 通常會有一個腳本管理系統

- SORA (事件響應)



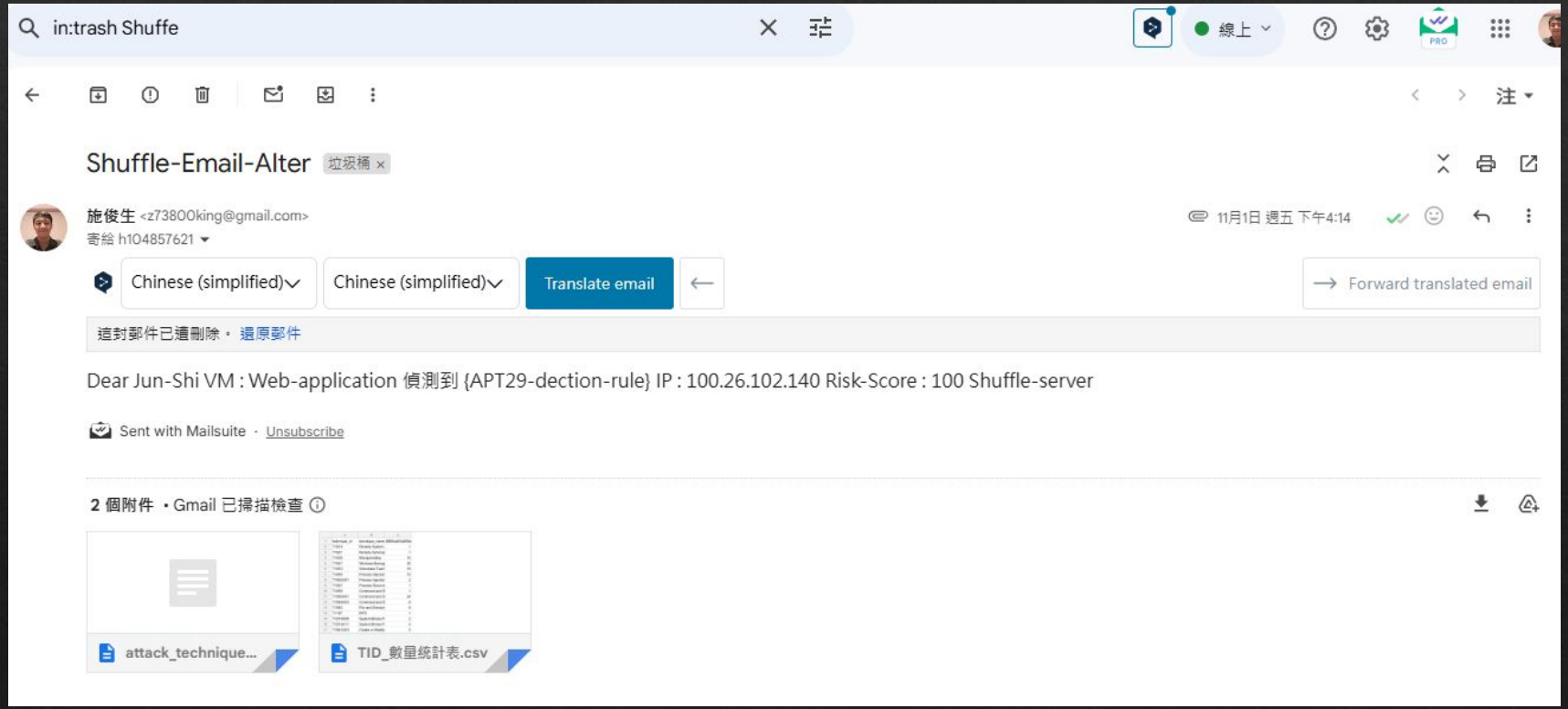
- SORA 的重要性
- 你做為一間公司的資安長
- 有一天發現告警響個不停,
- 這時候是不是有哪些 SOP 可以先做呢?
- 像是幫你寄信給管理層
- 像是幫你關閉那台被入侵的 server

SORA Solution - Shuffle Automation !



SORA Solution - Shuffle Automation !

如果要寄信最後會長這樣



- 威脅情資 (CTI)

- CTI 不太像一個概念
- CTI 目標在於利用各類資訊進行資安決策
- 各類資訊
  - 攻擊者的 TTP (Tactics 、Techniques、Procedures)
  - IoC (indicator of compromise)
  - 近年趨勢
- 情資層級
  - 戰略型威脅情資(Strategic Threat Intelligence)
  - 實戰型威脅情資(Operational Threat Intelligence)
  - 戰術型威脅情資(Tactical Threat Intelligence)

CTI 相關的重要資源

台灣會發 CVE 的機構

解決方案

Search the platform...

THREAT ACTORS
20 ↑ 9 (24 hours)

INTRUSION SETS
903 ↑ 365 (24 hours)

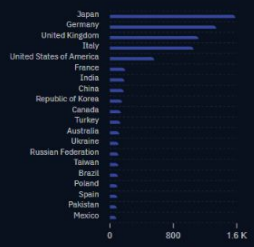
CAMPAIGNS
750 ↑ 279 (24 hours)

MALWARE
6.62K ↑ 2053 (24 hours)

INDICATORS
430.62K ↑ 307149 (24 hours)

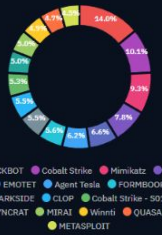
OBSERVABLES
460.65K ↑ 328265 (24 hours)

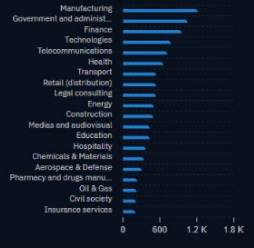
TARGETED REGIONS


TARGETED COUNTRIES


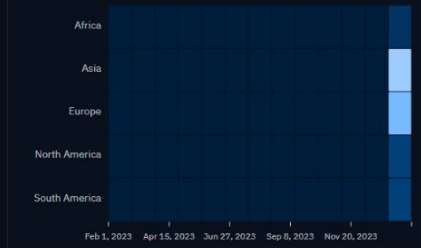
TARGETED COUNTRIES


ACTIVE INTRUSION SETS


ACTIVE MALWARE


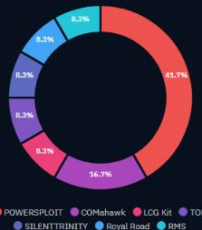
TARGETED SECTORS


TARGETED SECTORS


TARGETED REGIONS


ACTIVE VULNERABILITIES

CVE-2017-11882	214
CVE-2012-0158	157
CVE-2017-0199	145
CVE-2021-27065	138
CVE-2021-26855	131
CVE-2019-11510	128
CVE-2019-0708	122

ACTIVE TOOLS


LATEST CAMPAIGNS

May 24, 2023 at 10:18:27 AM

FATA MORGANA

Tortoiseshell's campaign which focuses on shipping and logistics companies based in Israel, aligning

LATEST REPORTS

Ranion Ransomware - Quiet a...	Feb 28,...	AlienVault	confuserex	NEW	TLP:CLEAR
Iranian APT Imperial Kitten ha...	Feb 28,...	Orange Cyber...	severity:2	NEW	ORANGE ...
CARBON SPIDER Embraces Bi...	Feb 28,...	AlienVault	bateleur	NEW	TLP:CLEAR

ACTIVE TTPS


INDICATORS SOURCES

[C] sekoia	170.49K
[C] riskiq	94.5K
[C] alienvault	56.35K

- 合規性管理

- 合規性管理是個概念
- 每個產品可能要遵守的法規不太一樣
- 金管會 - 金融資安行動方案 2.0 版
- 晶圓設備 - 半導體資安標準(SEMI E187)
- 數位發展部 - 資通安全管理法

SEMI E187 的資安標準的四大範疇

中華民國電腦稽核協會_SEMI E187-SEMI半導體晶圓設備資安標準

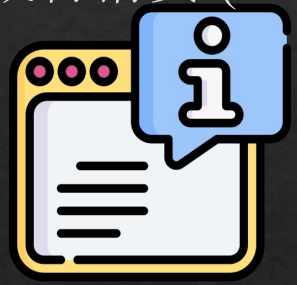
序號	類別	課程日期	課程系列	課程主題	講師	報名截止日	功能	開課狀態	是否額滿
1	台北班	2024/11/19	數位金融與電子支付系列	PCI DSS 4.0與ISO 27001:2022整合稽核實務(可抵內稽) **確定開課**	呂聰輝	2024/11/15		確定開課	
2	台北班	2024/11/25	內稽系列	獲利究竟被誰偷走了 - 物料編碼原則植入電腦記憶規則(上機操作)(可抵內稽)	洪嘉隆	2024/11/21		課程取消	
3	台北班	2024/11/26	舞弊稽核與數位鑑識系列	以財務資料分析(FDA)稽核技術破解虛假財務報表(可抵內稽)	蔡篤村	2024/11/22	報名	確認中	
4	台北班	2024/11/27	IT Audit與資訊治理系列	ZERO TRUST零信任 - 稽核的入門指引(可抵內稽) **確定開課**	方建國	2024/11/25		確定開課	已額滿
5	台北班	2024/11/28	內稽系列	獲利究竟被誰偷走了 - 視覺化簡報與稽核報告設計(上機操作)(可抵內稽)	洪嘉隆	2024/11/26	報名	確認中	

相關課程｜中華民國電腦稽核協會

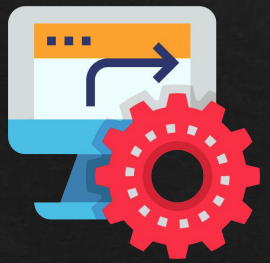
This is SOC !

- SOC (Security Operation Center)
- SIEM (事件管理)

- 威脅情資 (CTI)



- SORA (事件響應)



- 合規性管理