數位鑑識

Lab

某人說過一句很有名的話

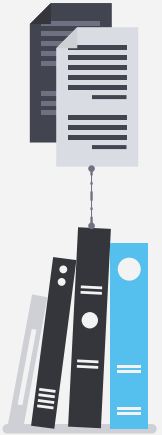
偷窺記憶體

memory dump tool

- WinPmem
- RAMCapturer

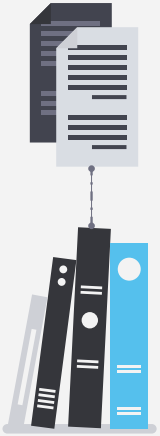
memory analysis

- Bulk Extractor + Java
- Volatility



memory dump

winpmem.exe physmem.raw



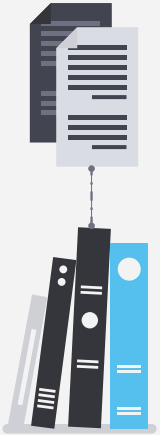
Volatility

volatility.exe -f physmem.raw imageinfo

volatility.exe -f physmem.raw —profile=Win10x64 volshell

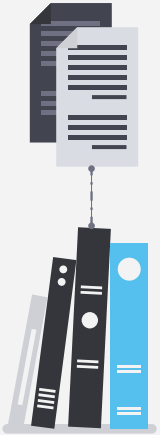
volatility.exe -f physmem.raw —profile=Win10x64 plist

volatility.exe -f physmem.raw —profile=Win10x64 hashdump

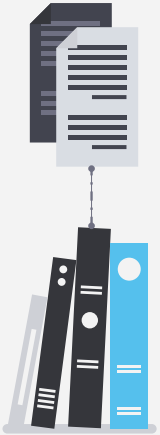


Blue Team

藍隊(Blue Teaming)是以守備的概念，對於企業管理制度、技術框架與人員訓練上進行強化，測試資安人員在紅隊(敵軍)攻擊來臨時，能否在面對攻擊的第一時間內有效地反應及處理，做出決策讓傷害降至最低，以及事件發生後是否能透過鑑識找出攻擊的全貌。



- 監控資安威脅
- 偵測資安事件
- 調查資安事件
- 修復資安事件
- 預防資安事件




一線
二線
三線
出事了！
監控
通知客戶
客戶場域
SOC Team
啟動事件
調查
IR Team
惡意程式
其他線索
APT Team
回饋
回饋
產品導入
Sales Team
客戶需求
完成開發
R&D Team

DF & IR

Digital Forensics 數位鑑識

證據收集
- 網路
- 系統
- 文件
- 記憶體

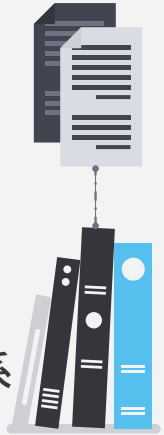
資料分析
撰寫報告

Incident Response 事件回應

事件識別與確認
遏制及根除
恢復及修復
事後分析

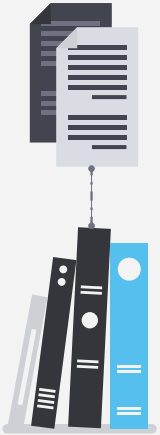
Digital Forensics

用於描述電子儲存資訊的收集和分析，以便可以將其作為證據或支持事實的發現。使用公認的方法收集的證據副本或由經驗豐富、有能力的分析師執行的證據副本可以在後續分析中以及在事件發生後提交時作為依據。對「取證級」資料捕獲的資料進行分析可以揭示電腦系統上現有內容日誌的審查可能無法揭示的偽影。取證分析旨在恢復所有可用信息，包括最近刪除的信息和工件，這些信息和工件可用於拼湊出可能丟失的一系列事件。

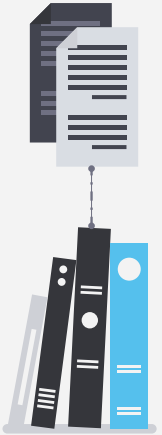


Incident Response

包括調查和修復網路攻擊，以將企業系統恢復正常運作。在「事件回應」期間，犯罪現場是即時的，因此數位證據收集方法需要適應場景，以確保證據收集和調查平衡並符合任何法律和監管義務以及恢復安全運營的需要。



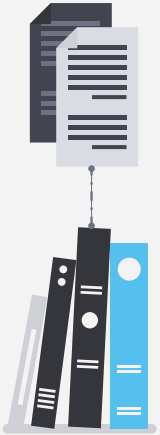
Digital Forensics Tools



- FTK Imager : image analysis
- The Sleuth Kit (TSK) : disk toolkit
- Autopsy : image analysis
- Volatility : memory analysis
- Eric Zimmerman : Toolkit
- Bulk Extractor : memory analysis
- Sysinternals Suite : Toolkit
- CSI Linux : Linux distribution
- KAPE : image analysis
- Redline : memory analysis

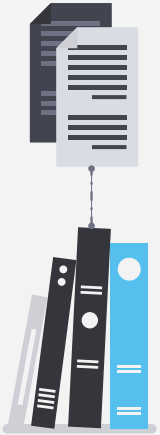
Incident Response Tools

- ELK : log analysis
- Splunk : log analysis
- Velociraptor : endpoint tool
- Wireshark : network analysis



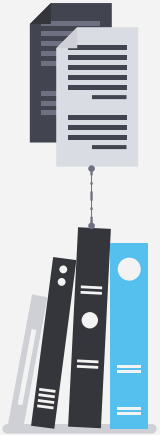
藍隊 vs DF&IR

藍隊專注於日常的防禦和監控，偵測、修補資安事件。
DF&IR 則負責在事件發生後進行調查。



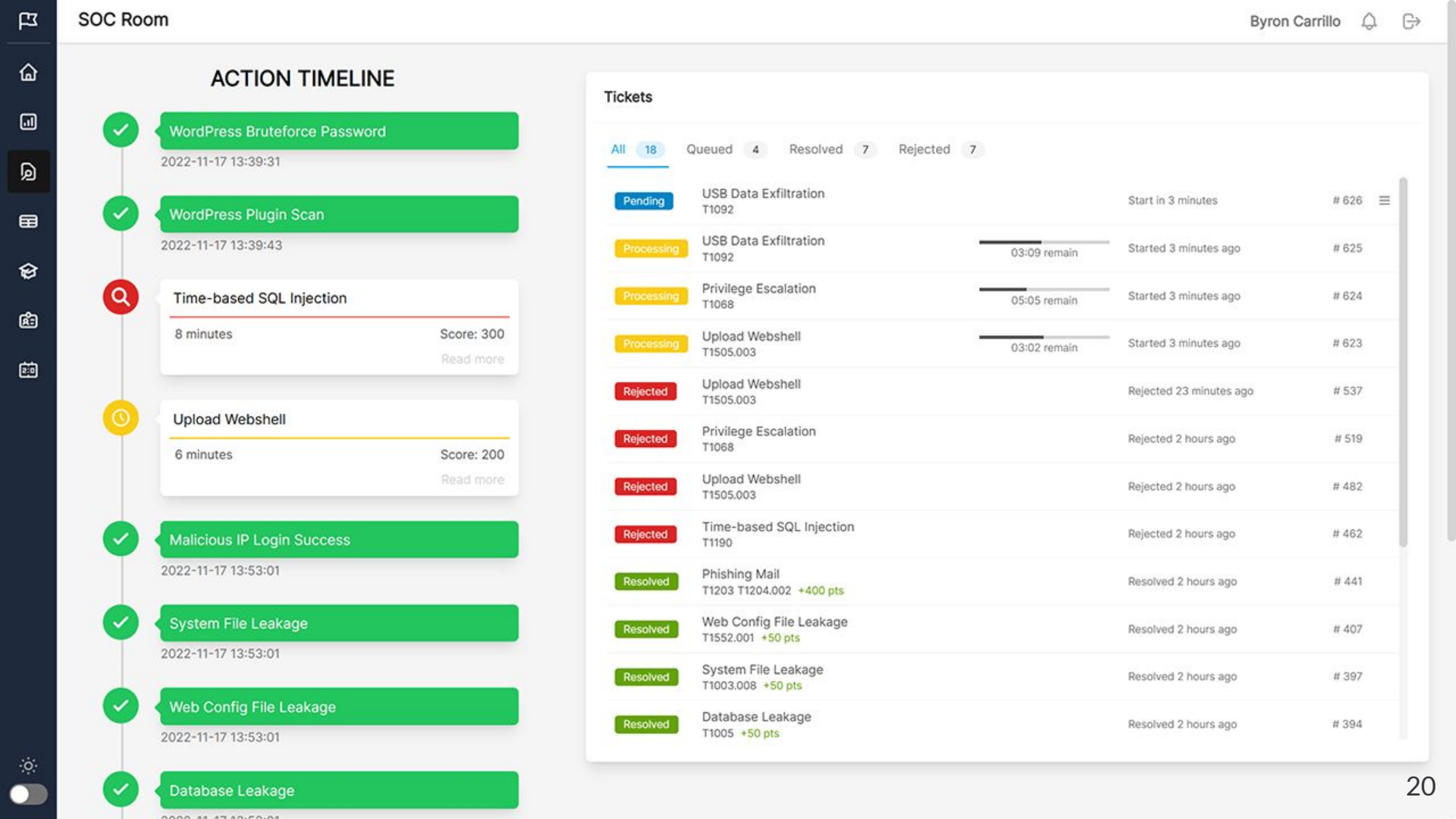
有趣的平台和活動

Cyber Range



Cyber Range 是一種實戰訓練方法：提供一個模擬網絡環境，並給予真實攻擊，學員以環境中的工具學習應對的技術。

- Cyberbit
- HITCON Cyber Range
- TRAPA CYBER RANGE
- 離島盃資安競賽


SOC Room
Byron Carrillo
ACTION TIMELINE
WordPress Bruteforce Password
2022-11-17 13:39:31
WordPress Plugin Scan
2022-11-17 13:39:43
Time-based SQL Injection
8 minutes
Score: 300
Read more
Upload Webshell
6 minutes
Score: 200
Read more
Malicious IP Login Success
2022-11-17 13:53:01
System File Leakage
2022-11-17 13:53:01
Web Config File Leakage
2022-11-17 13:53:01
Database Leakage
Tickets
All 18
Queued 4
Resolved 7
Rejected 7
Pending USB Data Exfiltration T1092 Start in 3 minutes # 626
Processing USB Data Exfiltration T1092 03:09 remain Started 3 minutes ago # 625
Processing Privilege Escalation T1068 05:05 remain Started 3 minutes ago # 624
Processing Upload Webshell T1505.003 03:02 remain Started 3 minutes ago # 623
Rejected Upload Webshell T1505.003 Rejected 23 minutes ago # 537
Rejected Privilege Escalation T1068 Rejected 2 hours ago # 519
Rejected Upload Webshell T1505.003 Rejected 2 hours ago # 482
Rejected Time-based SQL Injection T1190 Rejected 2 hours ago # 462
Resolved Phishing Mail T1203 T1204.002 +400 pts Resolved 2 hours ago # 441
Resolved Web Config File Leakage T1552.001 +50 pts Resolved 2 hours ago # 407
Resolved System File Leakage T1003.008 +50 pts Resolved 2 hours ago # 397
Resolved Database Leakage T1005 +50 pts Resolved 2 hours ago # 394