PURPLE TEAMING

An intro

Anton

- Previously Academics, Service Desk, GRC
- Now: Adversarial Collaboration Engineer (Purple / Blue team)
- Help organizations improve their defensive posture
- Blogging: https://www.lares.com/resources/blog/
- Love logs, SIEM, DFIR, querying things, catching malware
- @Antonlovesdnb on Twitter –share detection content here
- Email aovrutsky@lares.com – love talking shop!

What is Purple Teaming???

- https://www.lares.com/business-security-services/services-purple-team-collaboration/

- https://www.scythe.io/ptef

- https://danielmiessler.com/study/purple-team

- https://www.sans.org/purple-team

Is your head Exploding? Mine is!

SIMPLIFIED

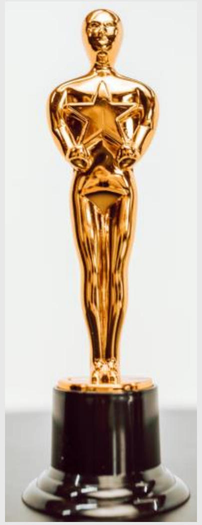
Purple Team is a collaborative & iterative process, involving folks from various departments, with the common goal of pushing the defensive needle forward.

What does Purple look like?

- Running TTPS and Hunting for them
- “Interactive” & collaborative IR
- Replay of TTPs from pen test, red team or incident
- TTP playbook from threat intel report
- Log pipeline analysis
- Anything that pushes the needle forward*

Purple Team Wins

- Closed a detection gap
- Found a detection gap
- Found a data source gap
- Demonstrated risk
- Provided “ammo”
- Tested assumptions
- Transferred knowledge



Purple Team Checklist

❑Buy in

❑Authorization

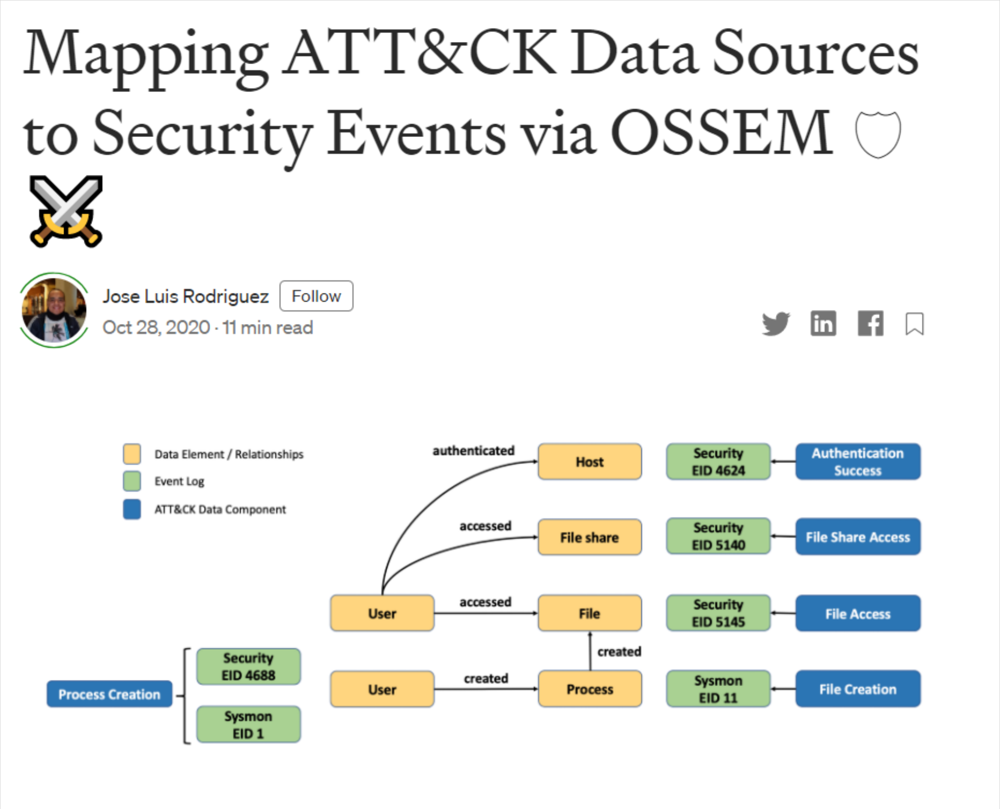
❑Access

❑TTPs

❑Data

❑Tracking / Metrics

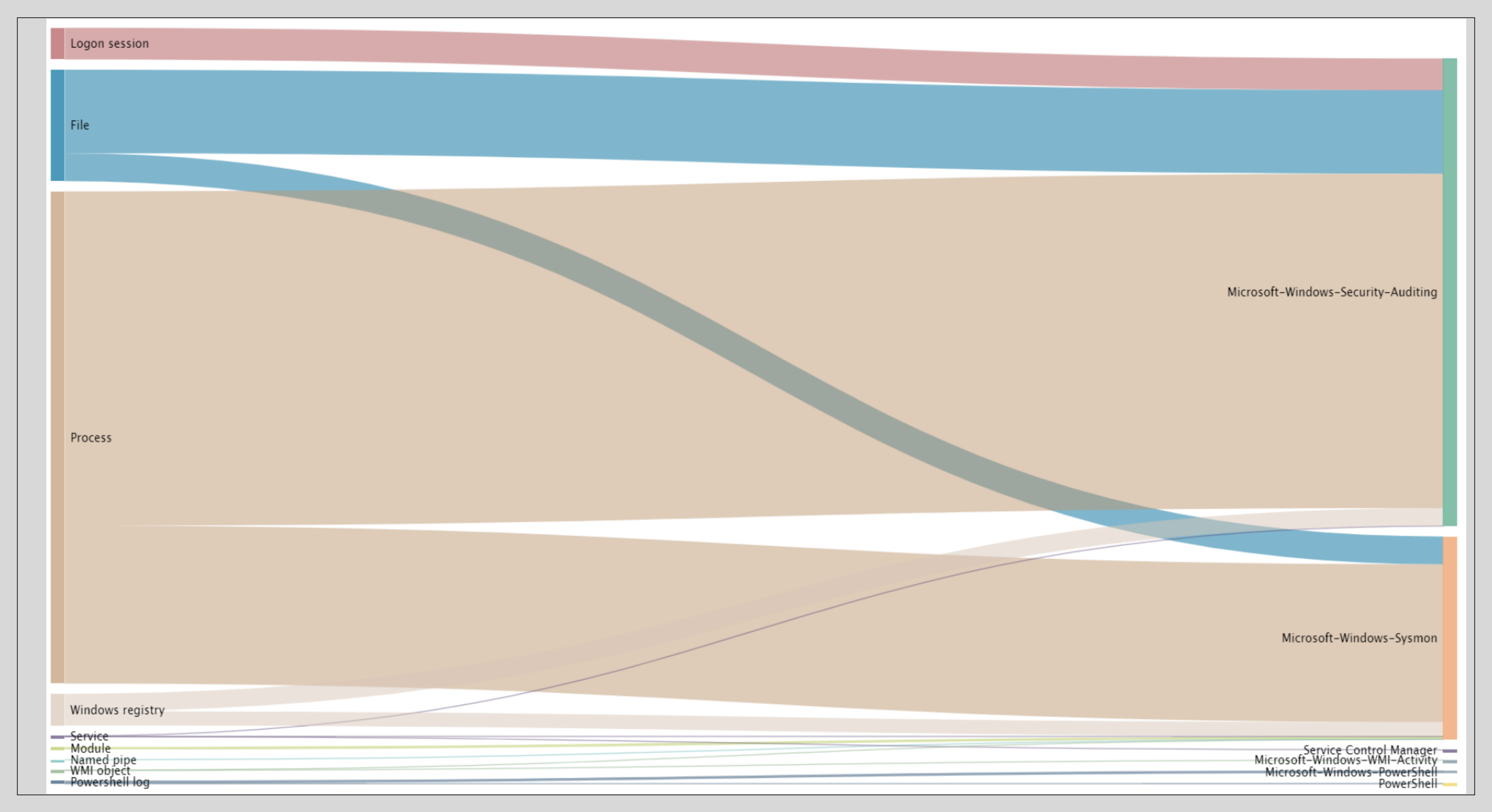
What data?

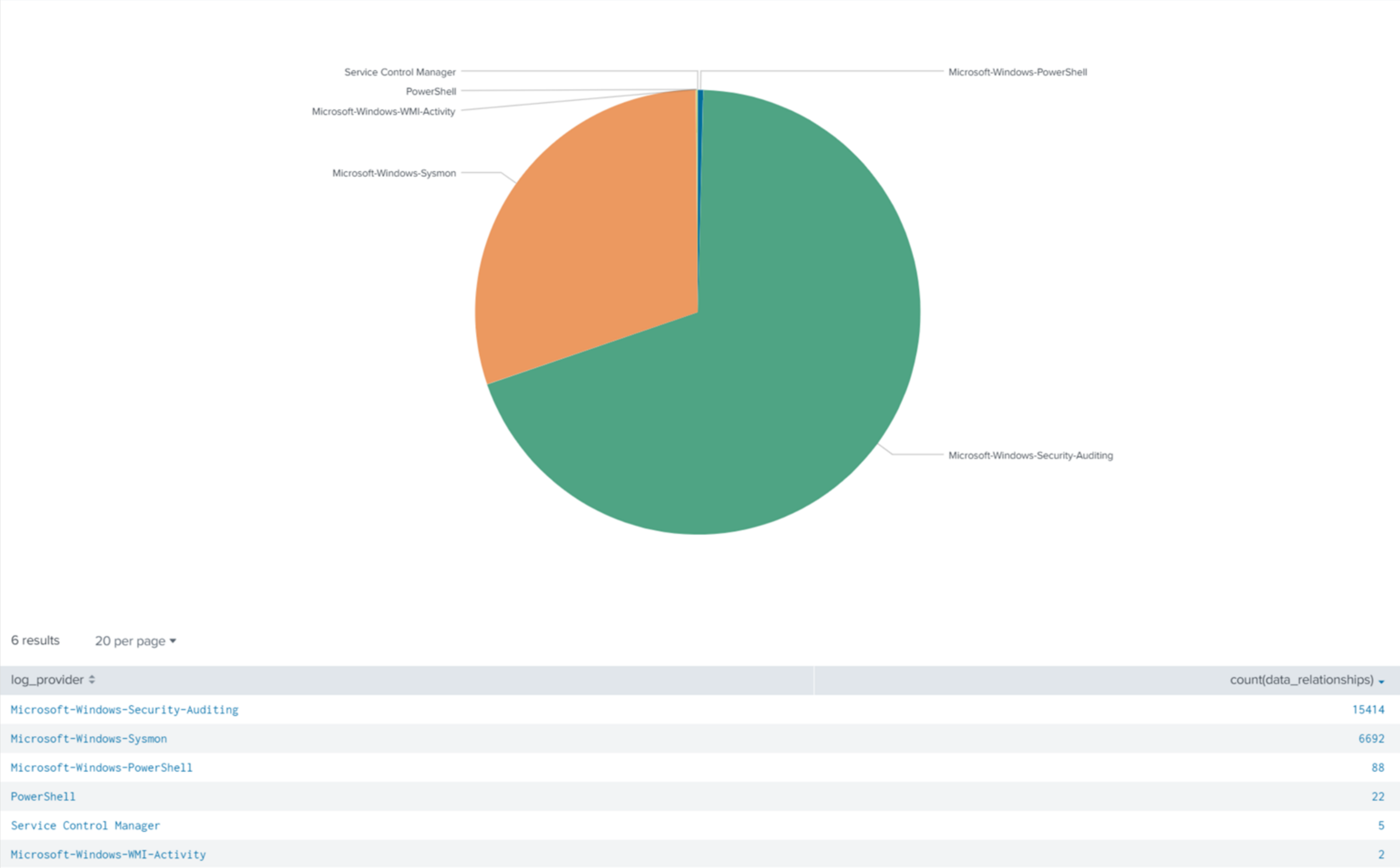


Mapping ATT&CK Data Sources to Security Events via OSSEM 🛡 ⚔

Jose Luis Rodriguez Follow

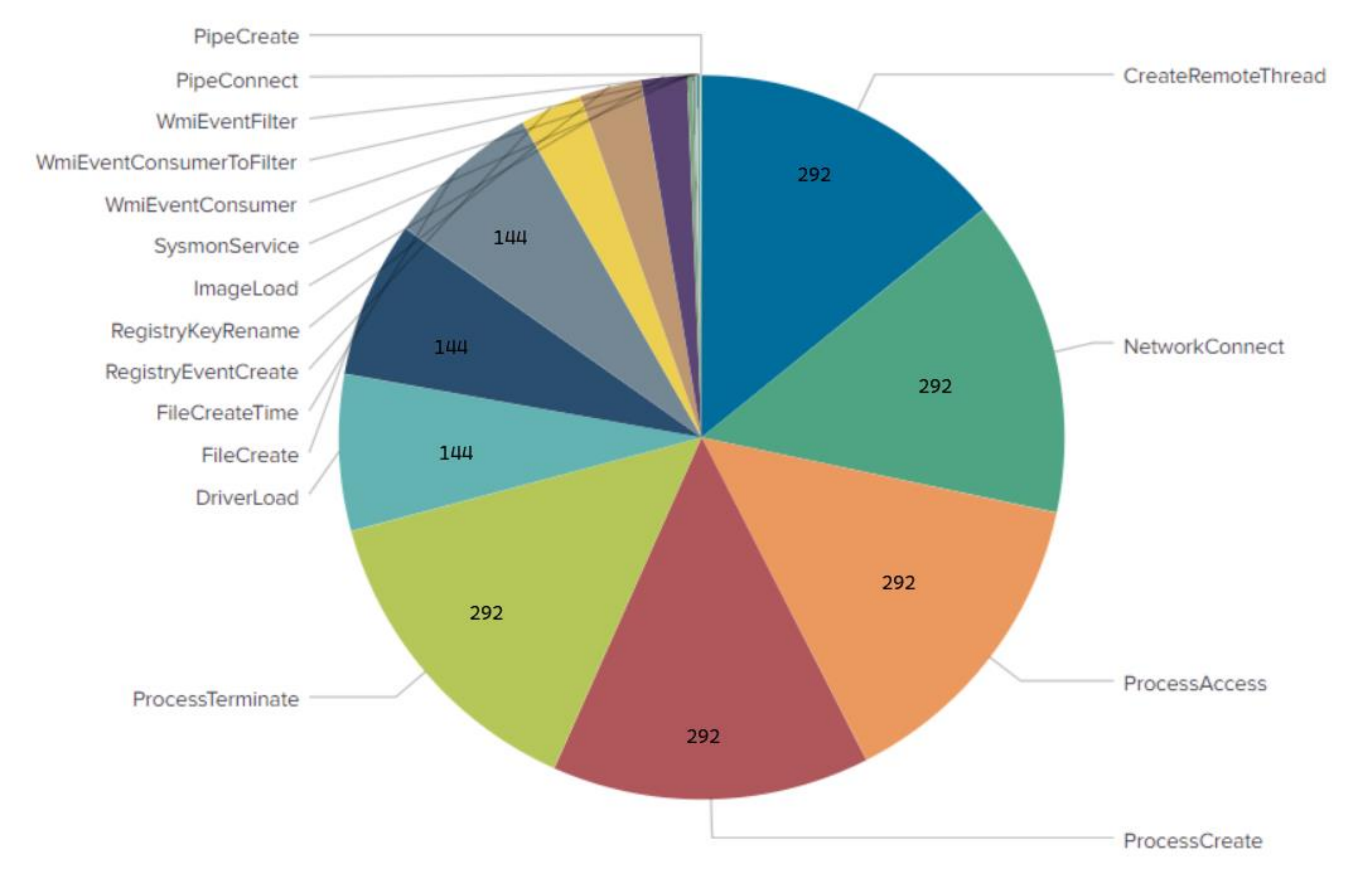
Oct 28, 2020 · 11 min read


Logon session
File
Process
Windows registry
Service
Module
Named pipe
WMI object
Powershell log
Microsoft-Windows-Security-Auditing
Microsoft-Windows-Sysmon
Service Control Manager
Microsoft-Windows-WMI-Activity
Microsoft-Windows-PowerShell
PowerShell


Service Control Manager
PowerShell
Microsoft-Windows-WMI-Activity
Microsoft-Windows-Sysmon
Microsoft-Windows-PowerShell
Microsoft-Windows-Security-Auditing

6 results   20 per page ▾

log_provider ⇕	count(data_relationships) ▾
Microsoft-Windows-Security-Auditing	15414
Microsoft-Windows-Sysmon	6692
Microsoft-Windows-PowerShell	88
PowerShell	22
Service Control Manager	5
Microsoft-Windows-WMI-Activity	2

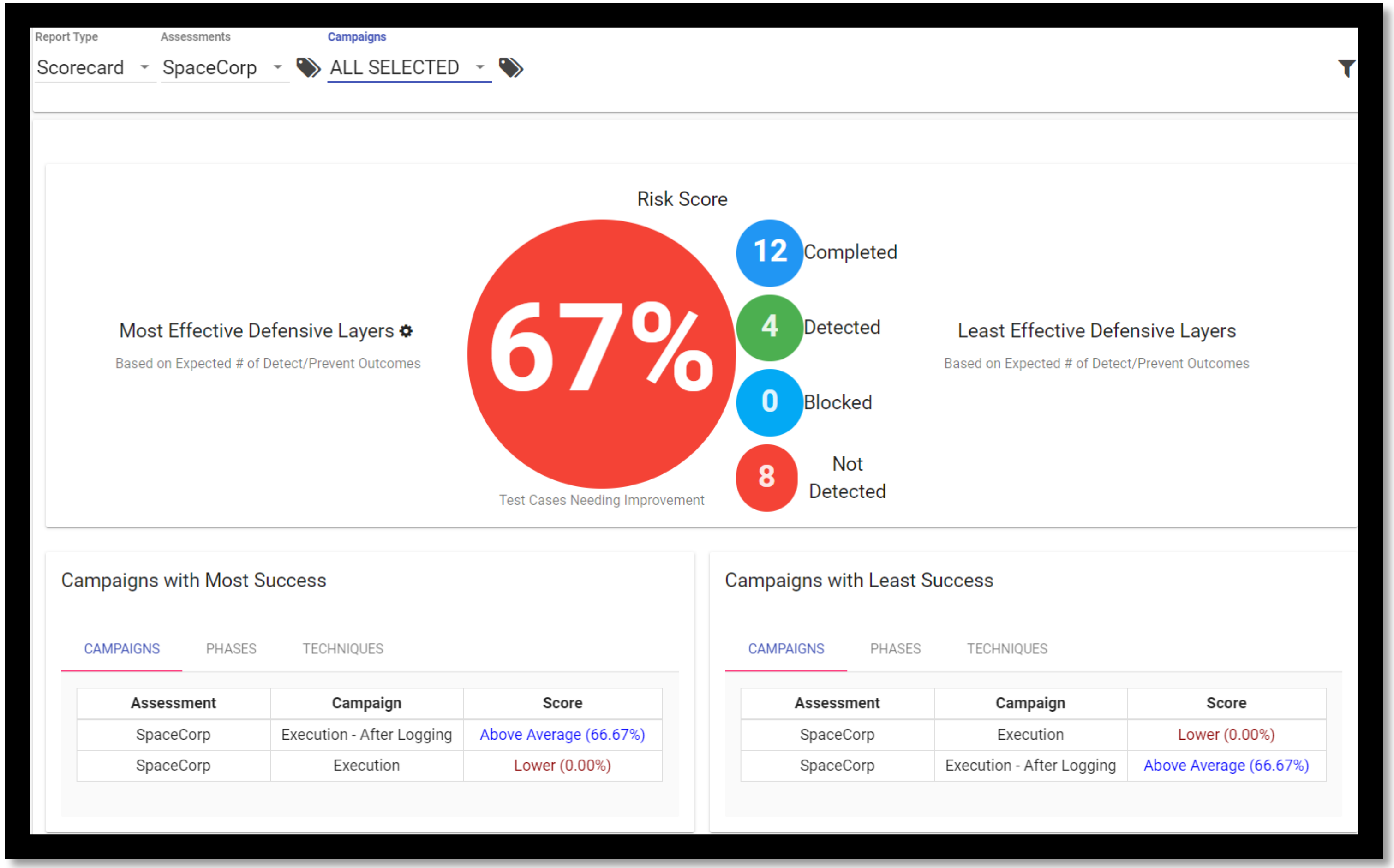

PipeCreate
PipeConnect
WmiEventFilter
WmiEventConsumerToFilter
WmiEventConsumer
SysmonService
ImageLoad
RegistryKeyRename
RegistryEventCreate
FileCreateTime
FileCreate
DriverLoad
ProcessTerminate
CreateRemoteThread
NetworkConnect
ProcessAccess
ProcessCreate
292
292
292
292
292
144
144
144

Setting Expectations

- I want to do PowerShell TTPs
  - No PowerShell logs 😕
- I want to emulate APT783 and UNC382020
  - No process creation logs ☹
- I want to test my Azure defenses
  - ….. No Azure Logs! 😦
- EDRs with no telemetry
  - Bypassed and then … ¯_(ツ)_/¯

Metrics

- What was detected ?
- What was blocked ?
- Was a log or alert generated at all ?
- How long did it take for the log to get into the SIEM ?
- Are we doing better than last quarter / year / week ?
- What are our “weak” spots ?
- Is one defensive layer doing most of the work?



Report Type: Scorecard

Assessments: SpaceCorp

Campaigns: ALL SELECTED

Risk Score

67%

Test Cases Needing Improvement

12 Completed

4 Detected

0 Blocked

8 Not Detected

Most Effective Defensive Layers

Based on Expected # of Detect/Prevent Outcomes

Least Effective Defensive Layers

Based on Expected # of Detect/Prevent Outcomes

Campaigns with Most Success

Assessment	Campaign	Score
SpaceCorp	Execution - After Logging	Above Average (66.67%)
SpaceCorp	Execution	Lower (0.00%)

Campaigns with Least Success

Assessment	Campaign	Score
SpaceCorp	Execution	Lower (0.00%)
SpaceCorp	Execution - After Logging	Above Average (66.67%)

Metrics

Leadership LOVES METRICS – You can help them!

https://github.com/SecurityRiskAdvisors/VECTR

Pain Points We See

- Clunky EDR Consoles / EDR that does not expose telemetry
- Lack of logs
- PowerShell / Scriptlets
- Golang / NIM
- Understaffed teams
- SIEMs underutilized
- Active Directory? Never heard of it.

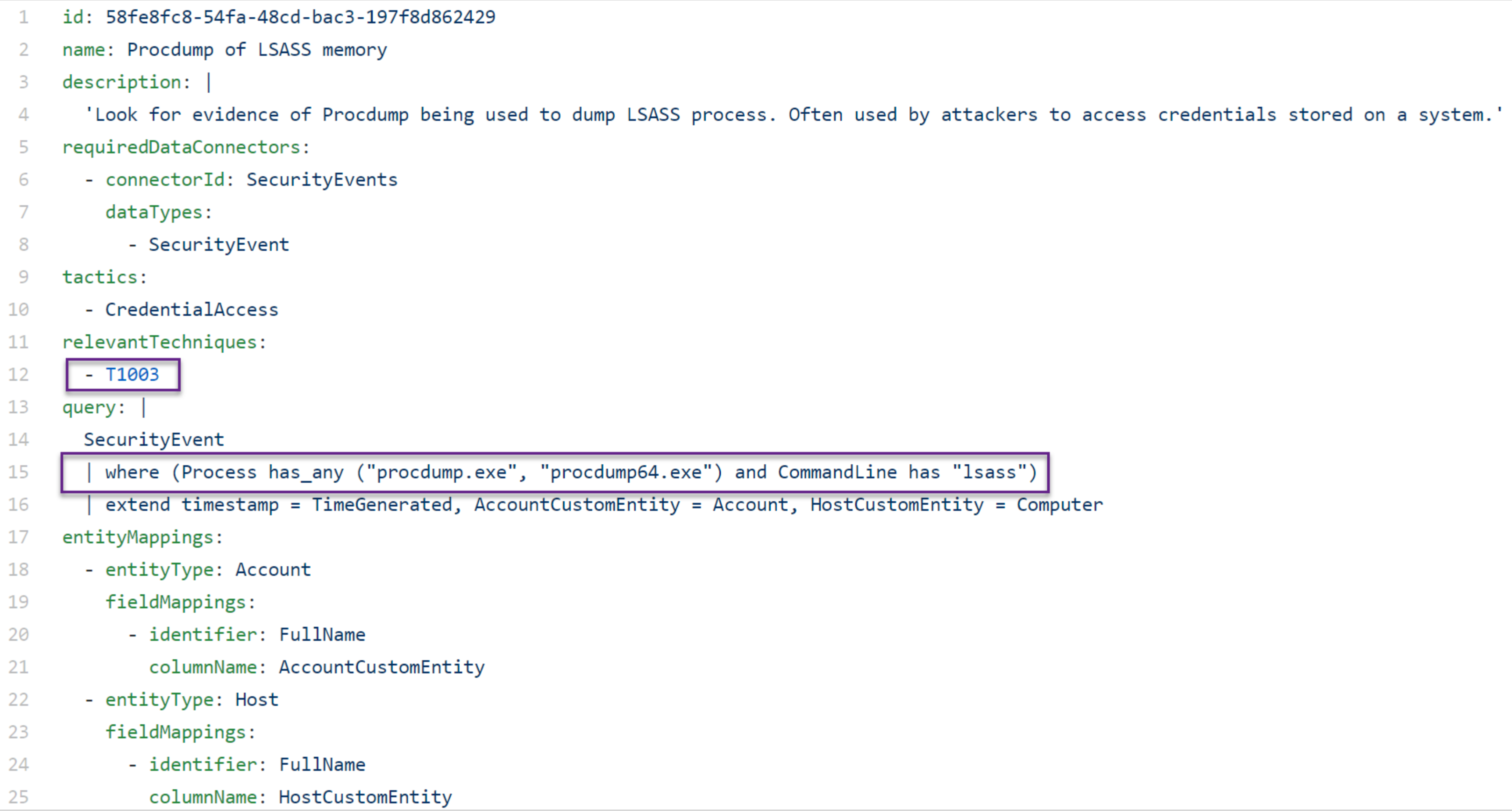
EDR NUANCE

TTP	**EDR?**
Phishing Email	**No**
Malicious PDF/Word Document	Yes
Beacon / Empire / Meterpreter	Yes
Persistence	Yes
Recon – BloodHound / ADFind	**No**
Lateral Movement – WMIC / SMB through beacon	Yes
Lateral Movement – Native Windows Utilities (net)	**No**
Lateral Movement – RDP	**No**
Privilege Escalation – Mimikatz	Yes
Privilege Escalation – Kerberoast	**No**

Don’t get.. Attacked.. By ATT&CK

- Don’t tar & feather me, I love ATT&CK ☺
- Order of operations:
  - Threat model
  - Logs
  - Pipeline / Alerting
  - Validation
  - … then map to ATT&CK

Everyone can pack it up! We got T1003 coverage



```
id: 58fe8fc8-54fa-48cd-bac3-197f8d862429
name: Procdump of LSASS memory
description: |
  'Look for evidence of Procdump being used to dump LSASS process. Often used by attackers to access credentials stored on a system.'
requiredDataConnectors:
  - connectorId: SecurityEvents
    dataTypes:
      - SecurityEvent
tactics:
  - CredentialAccess
relevantTechniques:
  - T1003
query: |
  SecurityEvent
  | where (Process has_any ("procdump.exe", "procdump64.exe") and CommandLine has "lsass")
  | extend timestamp = TimeGenerated, AccountCustomEntity = Account, HostCustomEntity = Computer
entityMappings:
  - entityType: Account
    fieldMappings:
      - identifier: FullName
        columnName: AccountCustomEntity
  - entityType: Host
    fieldMappings:
      - identifier: FullName
        columnName: HostCustomEntity
```

What Purple Team is Not

- Silver Bullet
- Fix for all your issues
- A pen test / Red Team
- Manifestation of hundreds of perfect SIEM rules

Closing Thoughts

- Do not get caught up in formal definitions and frameworks, if what you are doing is providing value and pushing the defensive needle forward, keep going
- In Purple Teaming, gaps can still be wins
- Tracking of activities and metrics is a force multiplier
- EDR is a piece of the puzzle and a layer in the proverbial security onion, do not lean on it too heavily
- Please enable more logs