Lessons in Purple Team Testing with MITRE ATT&CK™

from Priceline and Praetorian

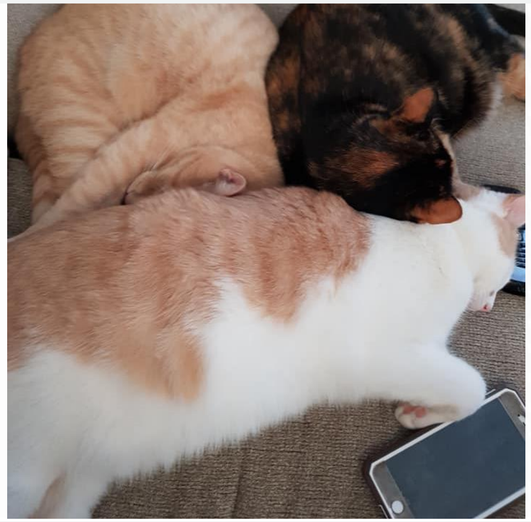
priceline.com®

PRAETORIAN

Who

Matt Southworth.

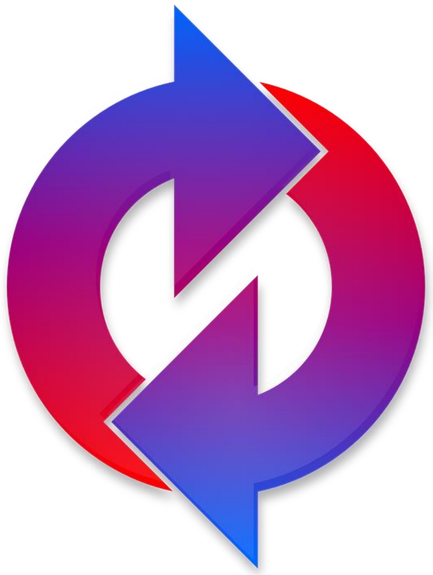
- **CISO @ Priceline**
- [Previous] Security engineer in financial services, DNs, etc
- Lots of coffee



Daniel Wyleczuk-Stern.

- **Practice Manager @ Praetorian**
- [Previous] Officer @ USAF (92d COS)
- Some certs, lots of cats ¯_(ツ)_/¯

The Problems



Worldwide Security Spending by Segment, 2017-2019 (Millions of US Dollars)

Market Segment	2017	2018	2019
Application Security	2,434	2,742	3,003
Cloud Security	185	304	459
Data Security	2,563	3,063	3,524
Identity Access Management	8,823	9,768	10,578
Infrastructure Protection	12,583	14,106	15,337
Integrated Risk Management	3,949	4,347	4,712
Network Security Equipment	10,911	12,427	13,321
Other Information Security Software	1,832	2,079	2,285
Security Services	52,315	58,920	64,237
Consumer Security Software	5,948	6,395	6,661
Total	**101,544**	**114,152**	**124,116**

Source: Gartner (August 2018)

priceline.com®

PRAETORIAN

Symptoms

Praetorian.

- Clients failing to detect activities on Red Teams
- On penetration tests after getting flagged for something…

"Well we would've caught you when you did this so make sure to note our strong detection"

Priceline.

- Repeat findings through adversarial testing
- Fidelity loss between adversarial test, reporting, attempts to recreate

"Bring me pictures of Spider-Man!"

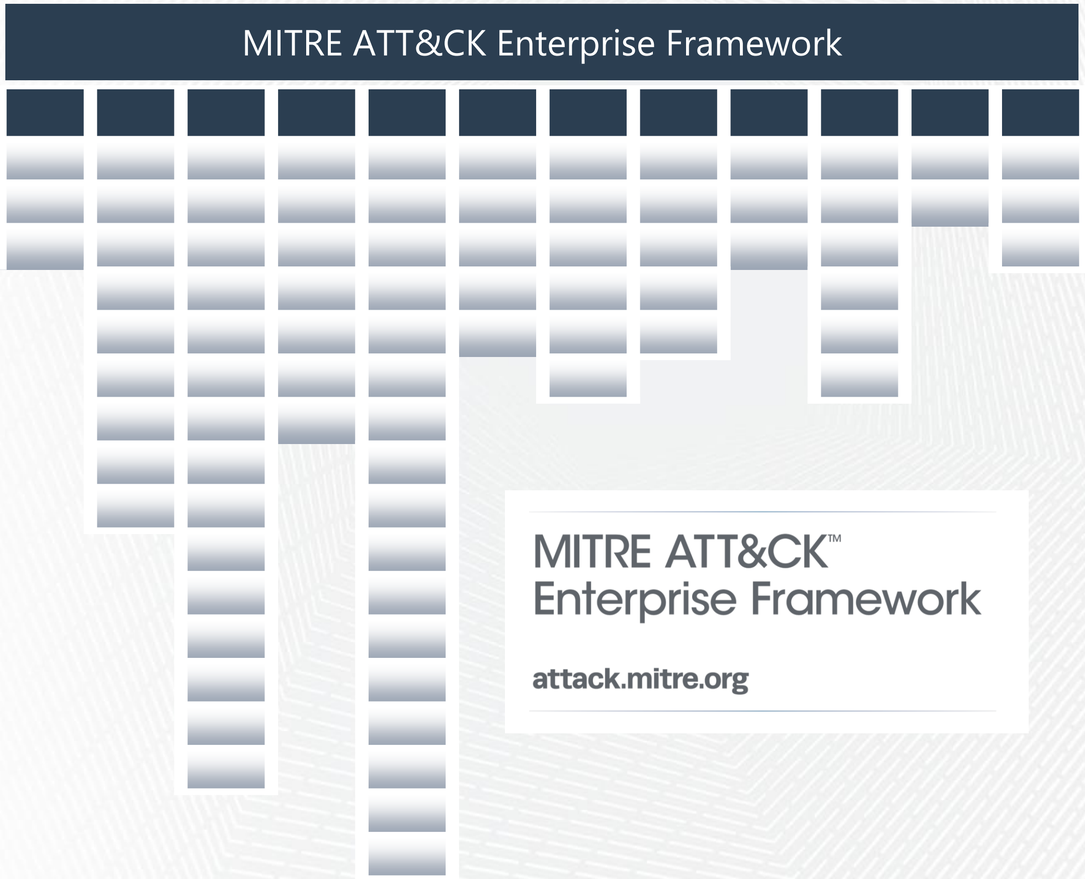
MITRE ATT&CK™

MITRE.

- Federally funded non-profit focused on research in support of various federal agencies

ATT&CK™.

- “a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations”
- Attacker techniques are organized into 12 columns based on their tactic



Why ATT&CK™?

Praetorian.

- Repeatable process
- Aligned with industry
- Defensible
- Show improvements over time
- Provide metrics as well as strategic (tactic) and technical (procedure) recommendations

Priceline.

- Opportunity for comparative metrics between security teams
- Common language when talking to security vendors
- Allow prioritization among the whole universe of TTPs
- Provide a burn down list to show improvement over time and justify investments

Purple Team Objectives

Improve detection capabilities through targeted emulation of attacker techniques

Collect metrics related to an organization's ability to detect the specific technique under test

Telemetry and Analysis - is the right data being collected and is it being processed correctly?

Develop recommendations that are both tactical (specific alerts for specific procedures) as well as strategic (deploying new tools, enriching data, etc)

Constraints

TIME
T1030

THREATS
T1205

CAPABILITY
T1207

Outsider Perspective

Cooperation is key

- Fail and learn quickly
- Quick triaging of findings

Prioritize Accordingly

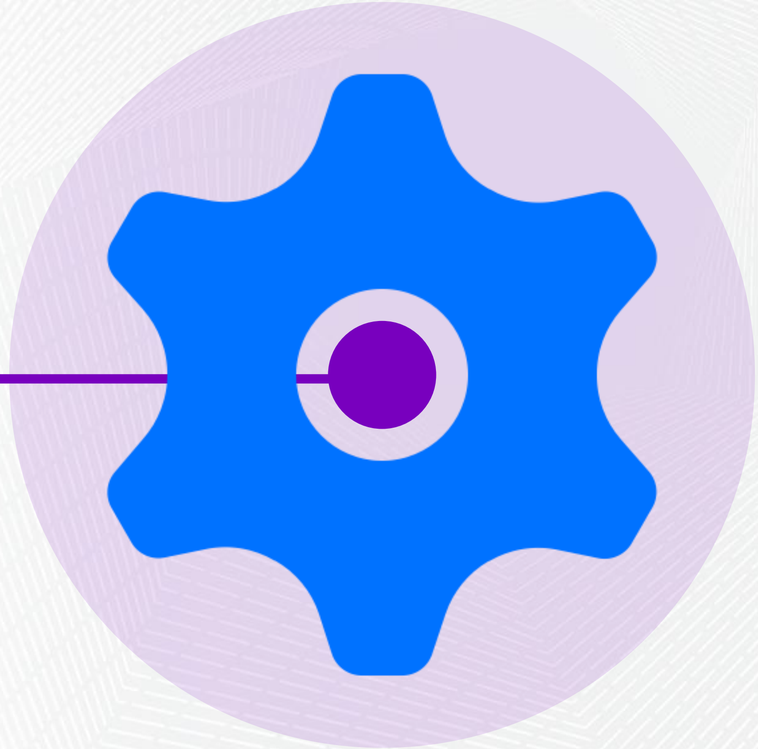
- Difficulty to execute
- Difficulty to fix
- Client input

Flexibility

- Breadth vs depth

Automation

- **Metasploit Framework (Rapid 7)**
- Caldera (MITRE)
- Metta (Uber)
- Atomic Red Team (Red Canary)
- Invoke-Adversary (Microsoft)



Why Metasploit Framework (MSF)?

- Alert on the behavior, not the tool
- Strong flexibility and automation capabilities
- Can integrate with PowerShell and .NET that other teams are creating
- Easy to develop for - clear standards and documentation
- Large, active open source community
- Support Windows, Linux, macOS, or none

Why Not MSF?

- Whitelisting the payload can be hard
- Deployment across an enterprise isn't easy
- Some things are hard to customize
- If you're not familiar with using MSF, there's a bit of a "retention curve"

Modules

```
msf5 exploit(multi/handler) > use post/windows/purple/
use post/windows/purple/adidns            use post/windows/purple/t1033            use post/windows/purple/t1075
use post/windows/purple/exec_bloodhound   use post/windows/purple/t1034            use post/windows/purple/t1077
use post/windows/purple/t1002             use post/windows/purple/t1035            use post/windows/purple/t1078
use post/windows/purple/t1003             use post/windows/purple/t1036            use post/windows/purple/t1081
use post/windows/purple/t1004             use post/windows/purple/t1037            use post/windows/purple/t1082
use post/windows/purple/t1005             use post/windows/purple/t1044            use post/windows/purple/t1083
use post/windows/purple/t1006             use post/windows/purple/t1047            use post/windows/purple/t1084
use post/windows/purple/t1007             use post/windows/purple/t1049            use post/windows/purple/t1085
use post/windows/purple/t1010             use post/windows/purple/t1050            use post/windows/purple/t1086
use post/windows/purple/t1012             use post/windows/purple/t1053            use post/windows/purple/t1087
use post/windows/purple/t1013             use post/windows/purple/t1055            use post/windows/purple/t1088
use post/windows/purple/t1015             use post/windows/purple/t1056            use post/windows/purple/t1089
use post/windows/purple/t1016             use post/windows/purple/t1057            use post/windows/purple/t1096
use post/windows/purple/t1018             use post/windows/purple/t1060            use post/windows/purple/t1098
use post/windows/purple/t1023             use post/windows/purple/t1063            use post/windows/purple/t1099
use post/windows/purple/t1028             use post/windows/purple/t1069            use post/windows/purple/t1101
use post/windows/purple/t1031             use post/windows/purple/t1070            use post/windows/purple/t1103
msf5 exploit(multi/handler) > use post/windows/purple/
```

https://github.com/praetorian-code/purple-team-attack-automation

Details

```
msf5 post(windows/purple/t1053) > info

       Name: Scheduled Task (T1053) Windows - Purple Team
     Module: post/windows/purple/t1053
   Platform: Windows
       Arch:
       Rank: Normal

Provided by:
  Praetorian

Compatible session types:
  Meterpreter

Basic options:
  Name       Current Setting
  ----       ---------------
  CLEANUP    true
  CMD        cmd /c calc.exe && echo T1053 > C:\t1053.txt && whoami >> C:\t1053.txt
  METHOD     2
  SESSION
  TASK_INT   ONCE
  TASK_NAME  Praetorian
  TASK_TIME  13:00

Description:
  Execution, Persistence, Privilege Escalation: Utilities such as at
  and schtasks, along with the Windows Task Scheduler, can be used to
  schedule programs or scripts to be executed at a date and time. The
  account used to create the task must be in the Administrators group
  on the local system. A task can also be scheduled on a remote
  system, provided the proper authentication is met to use RPC and
  file and printer sharing is turned on. An adversary may use task
  scheduling to execute programs at system startup or on a scheduled
  basis for persistence, to conduct remote Execution as part of
  Lateral Movement, to gain SYSTEM privileges, or to run a process
  under the context of a specified account.

References:
  https://attack.mitre.org/wiki/Technique/T1053
```

```
session => 2
msf5 post(windows/purple/t1053) > exploit

[*] Scheduling task using schtasks...
[*] Executing 'cmd /c schtasks /Create /SC once /TN Praetorian /TR "cmd /c calc.e
.185.128:58827 (192.168.38.104) "WIN10\vagrant @ WIN10">
[!] WARNING: Task may not run because /ST is earlier than current time.
SUCCESS: The scheduled task "Praetorian" has successfully been created.
[*] Executing 'cmd /c schtasks.exe /Run /TN Praetorian' on #<Session:meterpreter
[!] SUCCESS: Attempted to run the scheduled task "Praetorian".
[+] Found running calc process!
[+] Found persistence file!
[*] Cleaning up...
[*] Executing 'cmd /c cmd /c schtasks.exe /Delete /TN Praetorian /f' on #<Session
[!] SUCCESS: The scheduled task "Praetorian" was successfully deleted.
[*] Killing calc process if it exists...
[+] Found an instance of Calculator running. Killing it.
[+] Module T1053W execution successful.
[*] Post module execution completed
msf5 post(windows/purple/t1053) >
```

Demo 1 — Scheduled Task

```
msf5 post(windows/purple/t1053) > exploit

[*] Scheduling task using schtasks...
[*] Executing 'cmd /c schtasks /Create /SC once /TN Praetorian /TR "cmd /c calc.exe && echo T1053 > C:\t1053.txt && whoami >>
[redacted] (192.168.38.104) "WIN10\vagrant @ WIN10">
[!] WARNING: Task may not run because /ST is earlier than current time.
SUCCESS: The scheduled task "Praetorian" has successfully been created.
[*] Executing 'cmd /c schtasks.exe /Run /TN Praetorian' on #<Session:meterpreter [redacted] (192.168.38.104) "WIN10\va
[!] SUCCESS: Attempted to run the scheduled task "Praetorian".
[+] Found running calc process!
[+] Found persistence file!
[*] Cleaning up...
[*] Executing 'cmd /c cmd /c schtasks.exe /Delete /TN Praetorian /f' on #<Session:meterpreter [redacted] (192.168.38.1
[!] SUCCESS: The scheduled task "Praetorian" was successfully deleted.
[*] Killing calc process if it exists...
[+] Found an instance of Calculator running. Killing it.
[+] Module T1053W execution successful.
[*] Post module execution completed
```

Demo 1 — Successful Alert

10/6/19
11:03:24.000 PM

```
10/06/2019 23:03:24 +0000, search_name="[T1053] Scheduled Task - Process", search_now=1570403700.000, info_s
cess_parent_path="C:\\Windows\\System32\\cmd.exe", process_parent_command_line="cmd /c schtasks /Create /SC
t;&gt; C:\\t1053.txt\" /ST 13:00 /f", event_description="Process Create", process_parent_id=5044, process_id
te /t &gt;&gt; C:\\t1053.txt &amp;&amp; time /t &gt;&gt; C:\\t1053.txt\" /ST 13:00 /f", hash_sha256=b0a35a62
ence,Privilege_Escalation,Execution",mitre_technique="Scheduled Task",mitre_technique_id="T1053"
```

Event Actions

Type	✓	Field	Value	Actions
Selected	✓	host	logger	
	✓	source	[T1053] Scheduled Task - Process	
	✓	sourcetype	stash	
Event		search_name	[T1053] Scheduled Task - Process	
Time		_time	2019-10-06T23:03:24.000+00:00	
Default		index	threathunting	
		linecount	1	
		splunk_server	logger	

Successful Alert

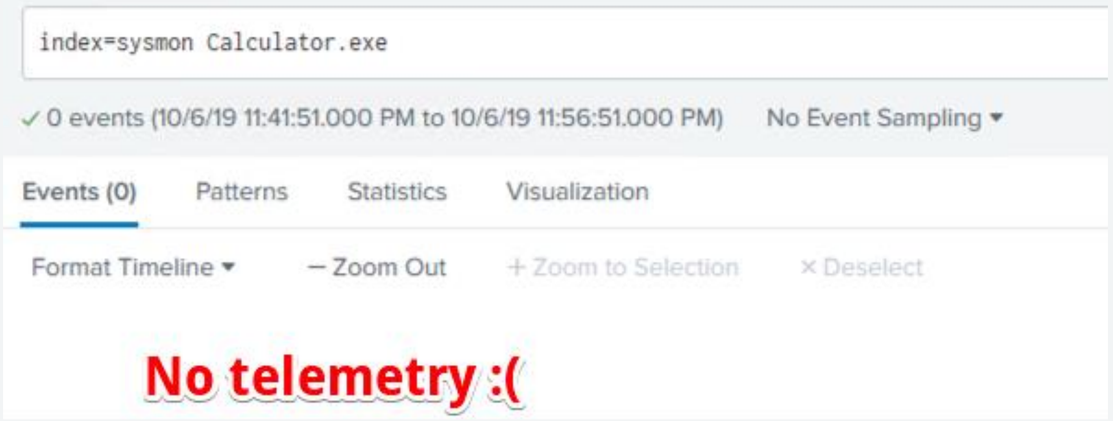
priceline.com

PRAETORIAN

Demo 2 — No Telemetry

```
msf5 post(windows/purple/t1055) > exploit

[*] Killing any existing instances of notepad.exe...
Filtering on '[Nn]otepad'
No matching processes were found.
[*] Uploading injection binary and required dlls...
[*] Uploading /usr/src/metasploit-framework/data/purple/t1055/inject_x64.exe to C:\t1055.exe
[*] Uploading /usr/src/metasploit-framework/data/purple/t1055/dllmain_x64.dll to C:\dllmain.dll
[*] Uploading /usr/src/metasploit-framework/data/purple/t1055/dllpoc_x64.dll to C:\dllpoc.dll
[*] Uploading /usr/src/metasploit-framework/data/purple/t1055/carriage_return.txt to C:\carriage_return.txt
[*] Uploading /usr/src/metasploit-framework/data/purple/t1055/rdll_x64.dll to C:\rdll.dll
[*] Killing any existing instances of notepad.exe...
Filtering on '[Nn]otepad'
No matching processes were found.
[*] Killing any existing instances of calc.exe...
Filtering on '[Cc]alc'
No matching processes were found.
[*] Executing command 'notepad.exe' on #<Session:meterpreter [redacted] (192.168.38.104) "WIN10\vagrant @ WIN10">
[*] Executing inject method CreateRemoteThread on target machine...
[+] Found running calc process!
[+] CreateRemoteThread success, calc found it worked.
Filtering on '[Cc]alc'
Killing: 3084
Filtering on '[Nn]otepad'
Killing: 5036
[*] Removing uploaded binaries...
[+] Module T1055W execution successful.
[*] Post module execution completed
```



Demo 3 — Actual Alerts

💀 `CrowdStrike Detection` 💀

Severity: **Critical**

ComputerName: [redacted]

User: `szabel`

File Name: **procdump64.exe**

SHA256:

16f413862efda3aba631d8a7ae2bfff6d84acd9f454a7adaa518c7a8a6f375a5

CrowdStrike Console

✅ 1

SplunkES APP 2:45 PM

Kerberoasting Attack

Kerberoasting Attack detected from:

Account_Name = SZabel@[redacted]

Client_Address = [redacted]

Service_ID =

Count = 655

Splunk

✅ 1

SplunkES APP 4:00 PM

⚠️ **Excessive Root Login Failures**

Root login failures detected on the server [redacted] **401** from [redacted] **5** times in past 60 minutes.

Splunk

✅ 1

priceline.com

PRAETORIAN

Demo 3 — Actual Alerts

SplunkES APP 8:20 PI

💀 `CrowdStrike Detection` 💀

Severity: **High**

ComputerName: [redacted]

User: `szabel`

File Name: **powershell.exe**

SHA256:

e0c662d10b852b23f2d8a240afc82a72b0995 19fa71cddf9d5d0f0be08169b6e

CrowdStrike Console

✔ 1

SplunkES APP 5:30 AM

🙍‍♀️ **::ffff**[redacted] was testing credentials in more than **100** accounts in the past 24hours

Alert "4768 - Authentication Ticket TGT (24hours)" has been `suppressed` *for the next 6 hours. Check manually if needed.*

View Results

✔ 1

priceline.com

PRAETORIAN

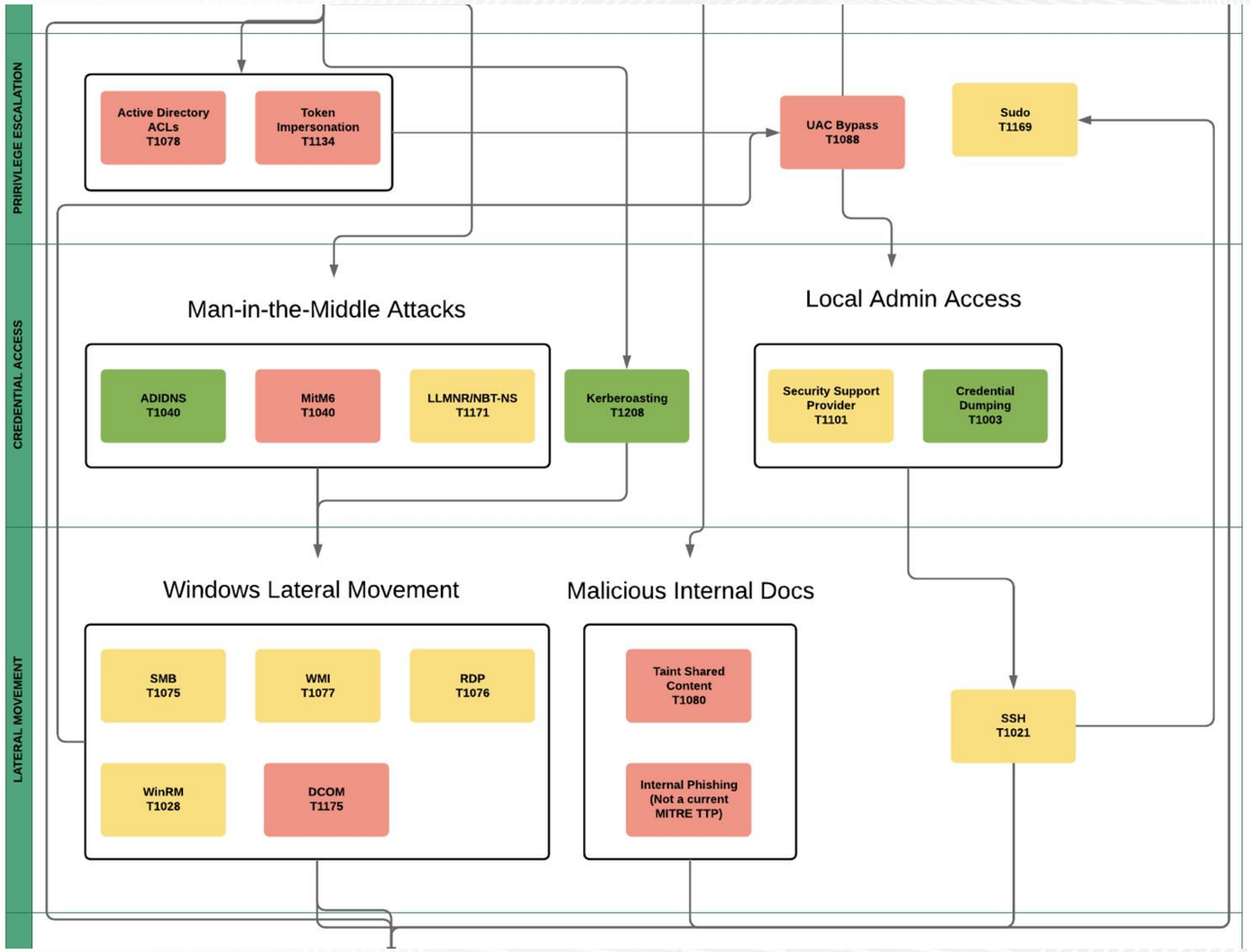
Two Cats — On Stairs

"Attackers only need to get it right once"

- Attackers also only need to get it wrong once
- You don't need a cat on every stair if you strategically place your cats where a human is likely to step

Thinking with Chains

- Overlap Purple Team with internal assessments
- Map the compromise and findings to ATT&CK
- Threat model your network



When ATT&CK is Not Enough

Examples

- SaaS Applications
- Internal APIs
- ~~Cloud~~ (added in latest release)

Solutions

- External communication
- Internal communication
- Technical breadth

Priceline Examples

Duo Bypass.

- index=security_access bypass sourcetype="duo:auth" NOT {{whitelisted users}}| dedup user| eval Report= user." %"| rex mode=sed field=Report "s/%/\n/g" | stats list(Report) as Report

GCP org changes.

- index="gcp" | search "data.resource.type"=organization

Delivering Value

- **Think outside the PDF**
  - Excel
  - Web
  - Tickets
- **Think tactically and strategically**
  - TTP specific
  - People, process, product
- **Prioritization**
  - ROI
  - Most common and easiest to fix
  - Land of diminishing returns
- **Don’t just find - solve**

Executive Summary | Dashboard | MITRE ATT&CK™ Matrix | Test Cases

The full ATT&CK Matrix below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Have Questions? → See the FAQ

Threat Model | Custom Queries

Scoring:

MITRE ATT&CK Matrix

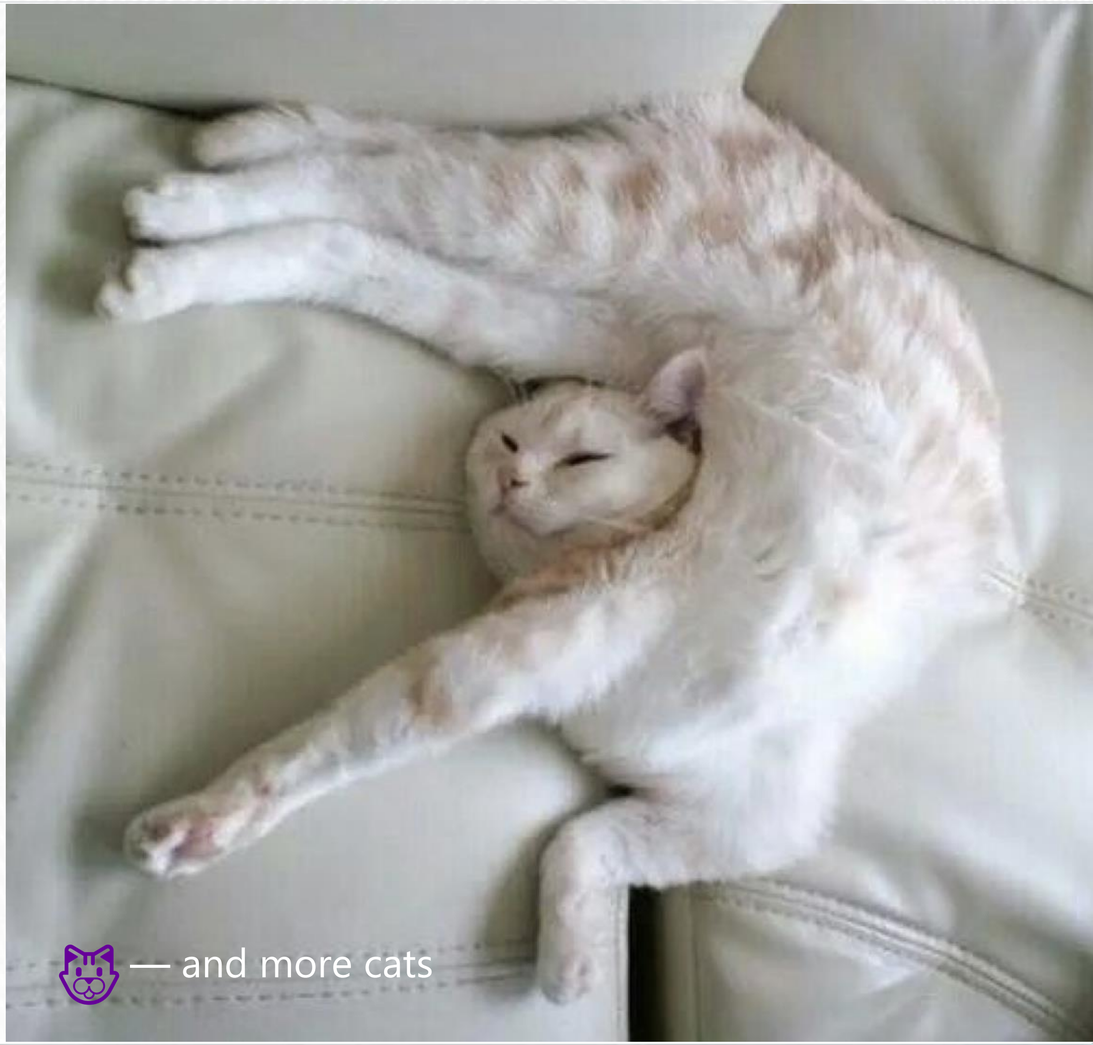
Operating System: Windows | Linux | Mac

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution
Winlogon Helper DLL	Port Monitors	File System Logical Offsets	Credential Dumping	System Service Discovery	Application Deployment Software	Windows Remote Management
Port Monitors	Accessibility Features	Binary Padding	Network Sniffing	Application Window Discovery	Remote Services	Service Execution
Accessibility Features	Path Interception	Rootkit	Input Capture	Query Registry	Windows Remote Management	Scheduled Task
System Firmware	DLL Search Order Hijacking	Obfuscated Files or Information	Exploitation for Credential Access	System Network Configuration Discovery	Logon Scripts	Command-Line Interface
Shortcut Modification	File System Permissions Weakness	Masquerading	Credentials in Files	Remote System Discovery	Shared Webroot	Graphical User Interface
Modify Existing Service	New Service	DLL Search Order Hijacking	Replication Through Removable Media	System Owner/User Discovery	Exploitation of Remote Services	Scripting
Path Interception	Scheduled Task	Software Packing	Account Manipulation	Network Service Scanning	Third-party Software	Third-party Software
Logon Scripts	Process Injection	Indicator Blocking	Brute Force	System Network Connections Discovery	Pass the Hash	Rundll32
DLL Search Order Hijacking	Service Registry Permissions Weakness	Process Injection	Two-Factor Authentication Interception	Process Discovery	Remote Desktop Protocol	PowerShell
Change Default File Association	Exploitation for Privilege Escalation	Scripting	Create Account	Security Software Discovery	Windows Admin Shares	Process Hollowing
File System	Valid Accounts	Indicator Removal from	Private Keys	Permission Groups	Taint Shared Content	Execution through API

priceline.com® PRAETORIAN

Managing the Purple team – CISO's Perspective

- Remember, "the purple team" isn't just redeployed adversarial testers
- Don't expect testers to do all the work!
- Preparation is important
- Consider what success looks like, including KPIs
- Encourage flexibility

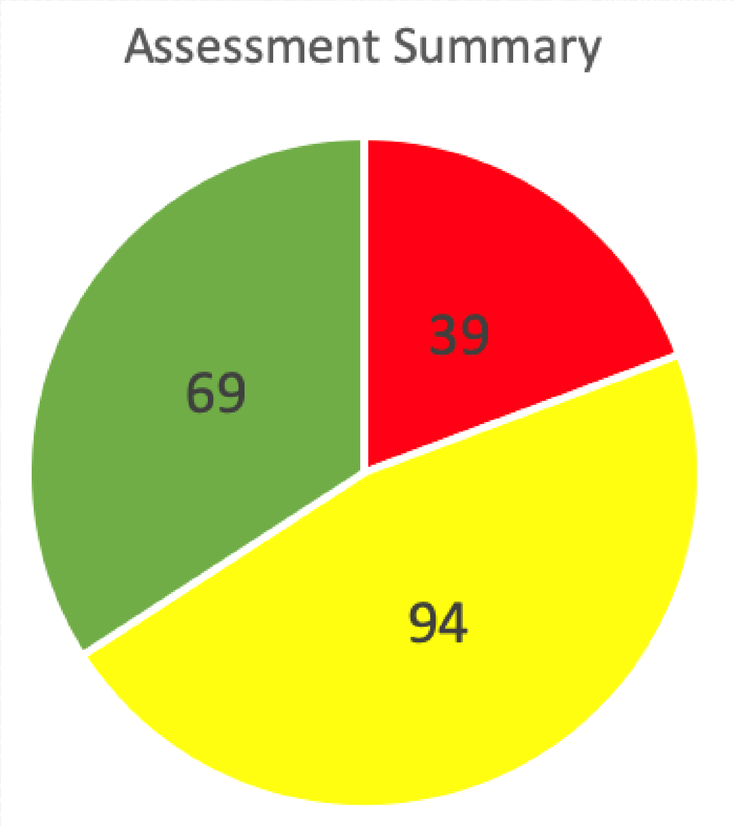


Managing the Purple Team – Preparation and Pre-work

- **Don’t ignore the people:**
  - Know roles and responsibilities are
  - Have a comms channel (Slack/Teams/Discord/Carrier Pigeon)
  - Have accounts created, systems provisioned, access validated
  - Daily rhythm (standups, status reports)
  - Align incentives: we prioritized collaboration over coverage
- **Consider objectives: TTPS you want to concentrate on or ignore**
- **Have some expectations about which detective tools will cover which TTPs**
- **Promote the upcoming test internally**

It's Like a Pentest You ***Want*** to Succeed

- **Expected results include:**
  - Alerts are validated, taxonimized per ATT&CK
  - New team members get an intense onboarding through this process
  - "Hit list" of improvements, taxonomized and ready to share with vendors
  - Quick, reproduceable demos using common pentester tools
- **Our most important outcome is Collaboration and knowledge transfer**
- **Measurements and KPIs**
  - TTP coverage
  - Alerts created/improved
  - Rate of ticket closure



So You've Done This Assessment, Now What?

Tactical next steps.

- Track your findings
- Make sure your existing alerts are categorized per ATT&CK
- Document existing TTP coverage
- Working with security product vendors
  - ATT&CK is a badge in marketing materials, but there's more needed
  - Be as explicit as you can with your vendors: *We want you to cover these TTPs, here are sample attacks for tuning*

Strategic improvements.

- Plan your next test objectives
- Suggest KPIs
- Reprioritize projects in light of findings

priceline.com

PRAETORIAN

Track Your Findings

project != INFOSEC and resolution = Unresolved AND labels in (purpleteam_2018_remediation, purpleteam2018) ORDER BY summary DESC, status DESC

Search | Switch to basic

1–8 of 8

Columns

T	Key	Summary	P	Status	Resolution
	IT-6755	Enable powershell 'constrained language mode' on endpoints and servers	2	WORK IN PROGRESS	*Unresolved*
	IT-5954	CSF improvement: Restrict powershell version	1	WORK NEEDED	*Unresolved*
	IT-5961	CSF Improvement: Require MFA for any a-admin account access	1	WORK NEEDED	*Unresolved*
	IT-7453	CSF Improvement: log all powershell actions on servers	1	FINAL REVIEW	*Unresolved*
	NET-26624	CSF improvement: Firmware updates process - network devices	2	OPEN	*Unresolved*
	IT-5953	CSF Improvement: deploy LAPS for servers	1	WORK IN PROGRESS	*Unresolved*
	NET-26626	CSF improvement: Patch JunOS	2	OPEN	*Unresolved*
	IT-15376	Create ADIDNS defenses	1	WORK IN PROGRESS	*Unresolved*

Corporate IT / IT-25159

Trendmicro not forwarding logs to splunk

Comment

Type: Security Issues
Priority: 3 Priority 3 (Medium)
Affects versions: None
Components: None

Status: OPEN
Resolution: Unresolved
Fix versions: None
Security Level: Security Level 3 (Low) (*Least restrictive*: Generally used for general-audience issues: accessible by *Project-Admins + Project-Developers + Project-Users*, reporter, assignee, and Security/Audit/office-services teams. Read: https://priceline.atlassian.net/wiki/x/pvs8B)

Labels: security
Scrum Team: Corporate IT Engineering
Customer Request Type: Security Issue
Requester Priority: Priority 1 (Highest)
Service Category: Problem
Sprint:

Description

On Sept 3rd Trendmicro stopped forwarding logs to splunk.

Google Drive attachments

Sign in to attach from Google Drive

People

Assignee: JD
Reporter: RE Ronald Iraheta Escobar
Request participants: None
Votes: 0
Watchers: 1 Stop watching this issue

Dates

Due: 11/Oct/19
Created: 2 days ago
Updated: Yesterday

Automations

No automations available.
Manage automations

PagerDuty Incident

PagerDuty is not configured for this project and issue type.

priceline.com

PRAETORIAN

Align Alerts with ATT&CK

Name	Status	Requires Akamai URL Update?	Revise Alert Slack Action Link to Akamai URL	Description of Alert IOC's	TTP Action Detection (where possible reference MITRE Attack Framework)	SPL Query
Kerberoasting Attack	Enabled	Splunk Akamai based URL added now	Requires additional revisions and testing	IOC = Windows event id 4769 indicates Kerberos service ticket is requested and Ticket_Encryption_Type=0x17 indicates RC4 encryption is used to encrypt part of Kerberos ticket. This method can be used to brute force the hash of the service account associated with the Service principal names	https://attack.mitre.org/techniques/T1208/	index=security_winevents sourcetype="Win Account_Name!=[redacted] Account_Name!=[redacted] Account_Name!=[redacted] | stats count by Account_Name Client_Addr | eval Report= Account_Name. " " .Client_A

- **Use what works for your team**
  - Spreadsheets, Wiki, Version control system
  - **https://github.com/hunters-forge/ThreatHunter-Playbook**

priceline.com

PRAETORIAN

Tips for Success

Checklists.

- Make sure you request what you need

Sharing.

- Google sheets, Box folders, etc – don't silo information during the engagement

Planning.

- Each Purple Team will be unique and each partner will be unique
- No plan survives first contact, but having a plan will allow you to be flexible from that plan to still stay on track

Define Objectives.

- Review previous adversarial understanding

Understand your Environment.

- Know in general what tools you expect to give you general coverage

Internal Promotion.

- Communicate with other tech teams
- They know if weird stuff happens who to go to
- Other folks have dropped in during the test just to see how things are going

Team Diversity.

- Internal – variety of experience and skillsets
- External – strong red teamers, blue teamers, application security

Thank You!

References

- https://www.iteuropa.com/news/services-rise-over-half-security-software-spend
- https://attack.mitre.org/docs/ATTACK_Framework_Board_4x3.pdf

Security Spend.

- https://dsimg.ubm-us.net/envelope/390213/526993/TCM_DR_1705079_Dark%20Reading%20Security%20Spending%20Report.pdf
- https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

Images.

- Excuse me, miss, I asked for the large cup of coffee. Hello ...