Leverage Endpoint Visibility

With ATT&CK Framework

Digit Oktavianto

@digitoktav

MITRE EU ATT&CK Community Workshop 18-19 May 2020

T1033: whoami

- Infosec Consulting Manager at Mitra Integrasi Informatika (MII)
- Co-Founder - BlueTeam.ID (https://blueteam.id)
- Community Leader - Cyber Defense Community Indonesia
- Honeynet Project - Indonesian Chapter
- Research Focus Area
  - Cyber Defense Operation
  - Threat Hunting
  - Threat Intelligence
  - Digital Forensic and Incident Response
  - Malware Analysis

Problem Statement

Although endpoint is one of the most critical component in organization, it is often not getting the attention it deserved. Most organizations are often investing their money to either network infrastructure or network security area first before buying any endpoint security solution.

Objective

This presentation will help security professionals to highlight the importance of endpoint security solution to their management by using MITRE ATT&CK framework to:

- Perform endpoint security (solution) assessment
- Track coverage and hunting (results and findings) of endpoint visibility over the time

When to Apply?

The first use case is to be employed before the organization acquired the endpoint security technology and at the Proof of Concept stage with the vendor. We can use the same baseline used against all the brands and vendors.

The second use case is applicable after the organization has their Endpoint Security technology deployed and need to track the coverage of their detection over the time, while also needs to cover the hunt result and findings in centralized space.

Use Case I

Endpoint Security Assessment

Using MITRE ATT&CK, we can perform a proper **Endpoint Security Assessment** by simulating threat actor TTPs.

The simulation will be done by using Open Source Tools or Commercial Tools that are mapped to MITRE ATT&CK tools evaluation framework.

With this method, the organization will see whether certain technique or tactic is already covered by the endpoint security solutions (both detection or prevention), and spot what detection is not covered by the security products.

For sample evaluation of assessment, we can see the method and the results on MITRE ATT&CK Evaluation page: https://attackevals.mitre.org/

Endpoint Security Assessment Method

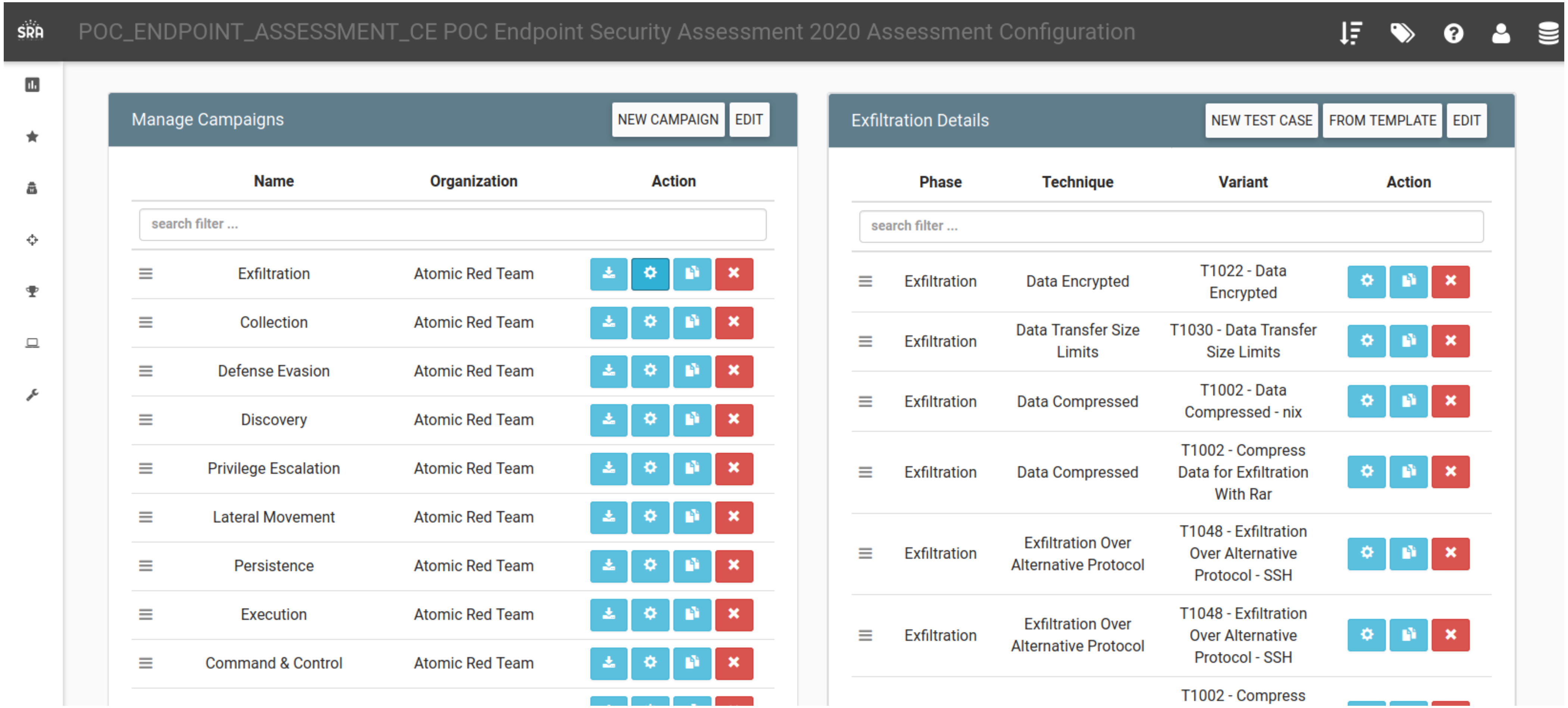
- Create a simulation plan based on TTPs that we want to test
- Map the TTPs for simulation into a platform
- Test the endpoint security products according on the simulation plan
- Analyze the result and identify any gaps from the platform

Endpoint Security Assessment Toolkit

Vectr.io from **SecurityRiskAdvisors** (https://github.com/SecurityRiskAdvisors/VECTR)

- 3 main components; Assessment Group, Campaign, and Test Case.
  - Each campaign can contains several test case.
- Create the test case for adversary emulation plans that are mapped to MITRE ATT&CK technique & tactic
- Set the Blue Team Tools (Endpoint Security product which are being assessed)
  - Configure the detection layer
- Set the Red Team Tools (BAS Tools which are being used to “test” the Endpoint Security product)
- See the summary and result of the assessment

VECTR Campaign



POC_ENDPOINT_ASSESSMENT_CE POC Endpoint Security Assessment 2020 Assessment Configuration

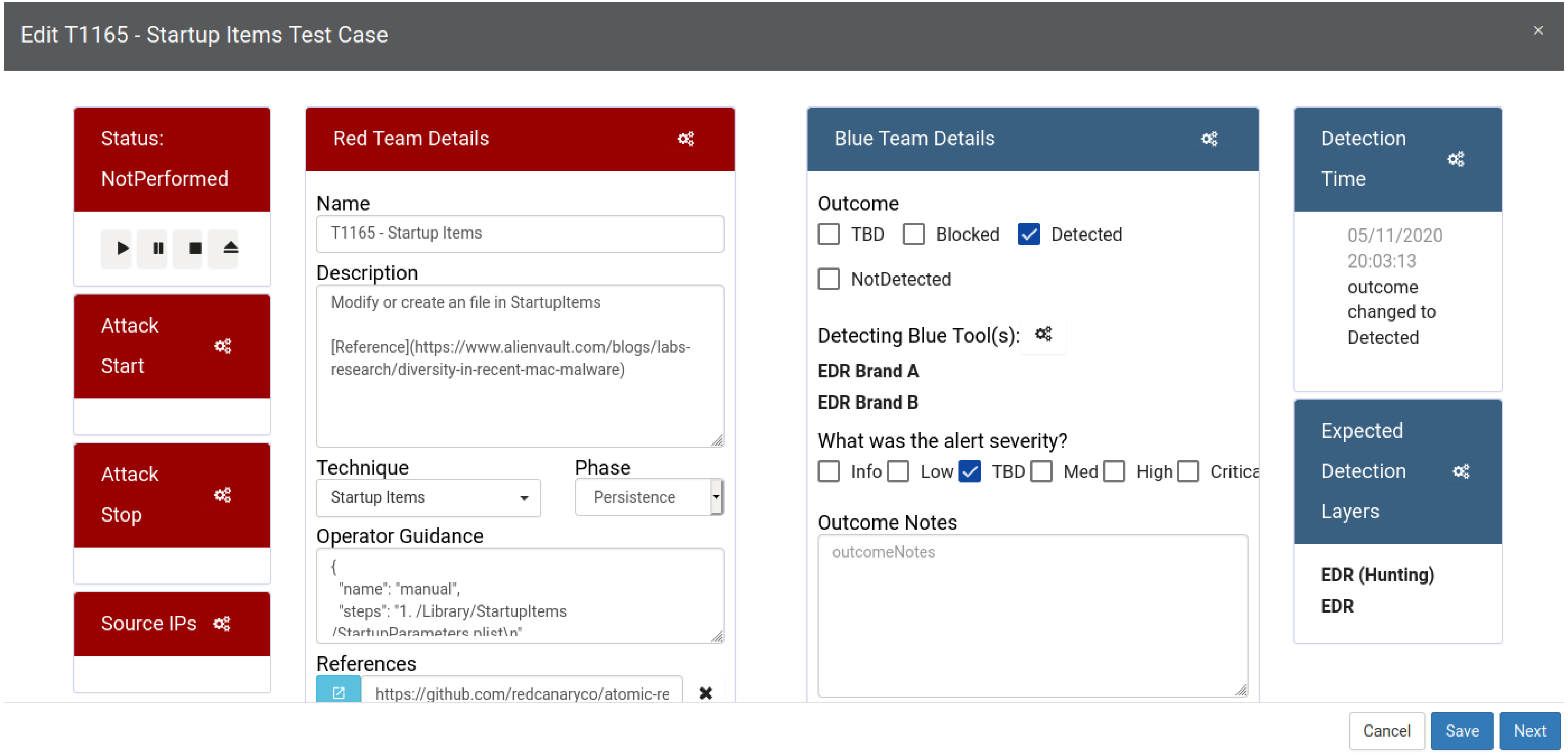
Manage Campaigns

	Name	Organization	Action
	search filter ...		
≡	Exfiltration	Atomic Red Team	⬇ ⚙ ❐ ✖
≡	Collection	Atomic Red Team	⬇ ⚙ ❐ ✖
≡	Defense Evasion	Atomic Red Team	⬇ ⚙ ❐ ✖
≡	Discovery	Atomic Red Team	⬇ ⚙ ❐ ✖
≡	Privilege Escalation	Atomic Red Team	⬇ ⚙ ❐ ✖
≡	Lateral Movement	Atomic Red Team	⬇ ⚙ ❐ ✖
≡	Persistence	Atomic Red Team	⬇ ⚙ ❐ ✖
≡	Execution	Atomic Red Team	⬇ ⚙ ❐ ✖
≡	Command & Control	Atomic Red Team	⬇ ⚙ ❐ ✖

Exfiltration Details

	Phase	Technique	Variant	Action
	search filter ...			
≡	Exfiltration	Data Encrypted	T1022 - Data Encrypted	⚙ ❐ ✖
≡	Exfiltration	Data Transfer Size Limits	T1030 - Data Transfer Size Limits	⚙ ❐ ✖
≡	Exfiltration	Data Compressed	T1002 - Data Compressed - nix	⚙ ❐ ✖
≡	Exfiltration	Data Compressed	T1002 - Compress Data for Exfiltration With Rar	⚙ ❐ ✖
≡	Exfiltration	Exfiltration Over Alternative Protocol	T1048 - Exfiltration Over Alternative Protocol - SSH	⚙ ❐ ✖
≡	Exfiltration	Exfiltration Over Alternative Protocol	T1048 - Exfiltration Over Alternative Protocol - SSH	⚙ ❐ ✖
			T1002 - Compress	

VECTR Test Case (Red & Blue) Team



Edit T1165 - Startup Items Test Case

Status: NotPerformed

Attack Start

Attack Stop

Source IPs

Red Team Details

Name: T1165 - Startup Items

Description:

Modify or create an file in StartupItems

[Reference](https://www.alienvault.com/blogs/labs-research/diversity-in-recent-mac-malware)

Technique: Startup Items

Phase: Persistence

Operator Guidance:

```
{
  "name": "manual",
  "steps": "1. /Library/StartupItems
/StartupParameters.plist\n"
```

References: https://github.com/redcanaryco/atomic-re

Blue Team Details

Outcome

□ TBD □ Blocked ☑ Detected

□ NotDetected

Detecting Blue Tool(s):

EDR Brand A

EDR Brand B

What was the alert severity?

□ Info □ Low ☑ TBD □ Med □ High □ Critica

Outcome Notes

outcomeNotes

Detection Time

05/11/2020 20:03:13

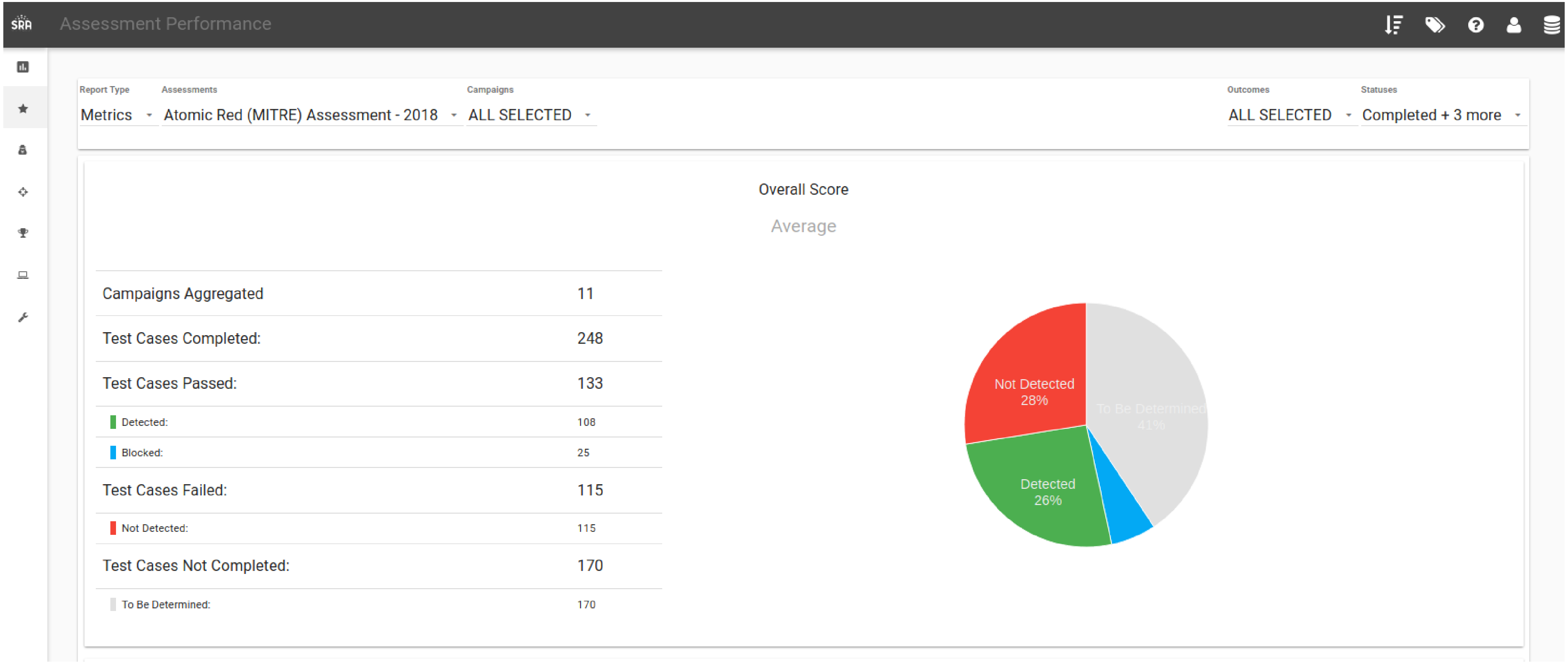
outcome changed to Detected

Expected Detection Layers

EDR (Hunting)

EDR

VECTR Reporting



Report Type: Metrics

Assessments: Atomic Red (MITRE) Assessment - 2018

Campaigns: ALL SELECTED

Outcomes: ALL SELECTED

Statuses: Completed + 3 more

Overall Score

Average

Campaigns Aggregated	11
Test Cases Completed:	248
Test Cases Passed:	133
🟩 Detected:	108
🟦 Blocked:	25
Test Cases Failed:	115
🟥 Not Detected:	115
Test Cases Not Completed:	170
⬜ To Be Determined:	170

Use Case 2
Track Coverage and Hunting

The idea is every team member may create the rules and policy to cover as much as possible the MITRE ATT&CK Framework TTPs. And along the way there is some improvement about new technique or new detection rules, every team member may know the details about it.

Based on the knowledge information provided from the platform, every team member can start doing the hunting, and also if they have a new hypothesis or ideas for hunting, they can add the knowledge into the platform, so every other member will know the updates.

Tracking Coverage and Hunting Method

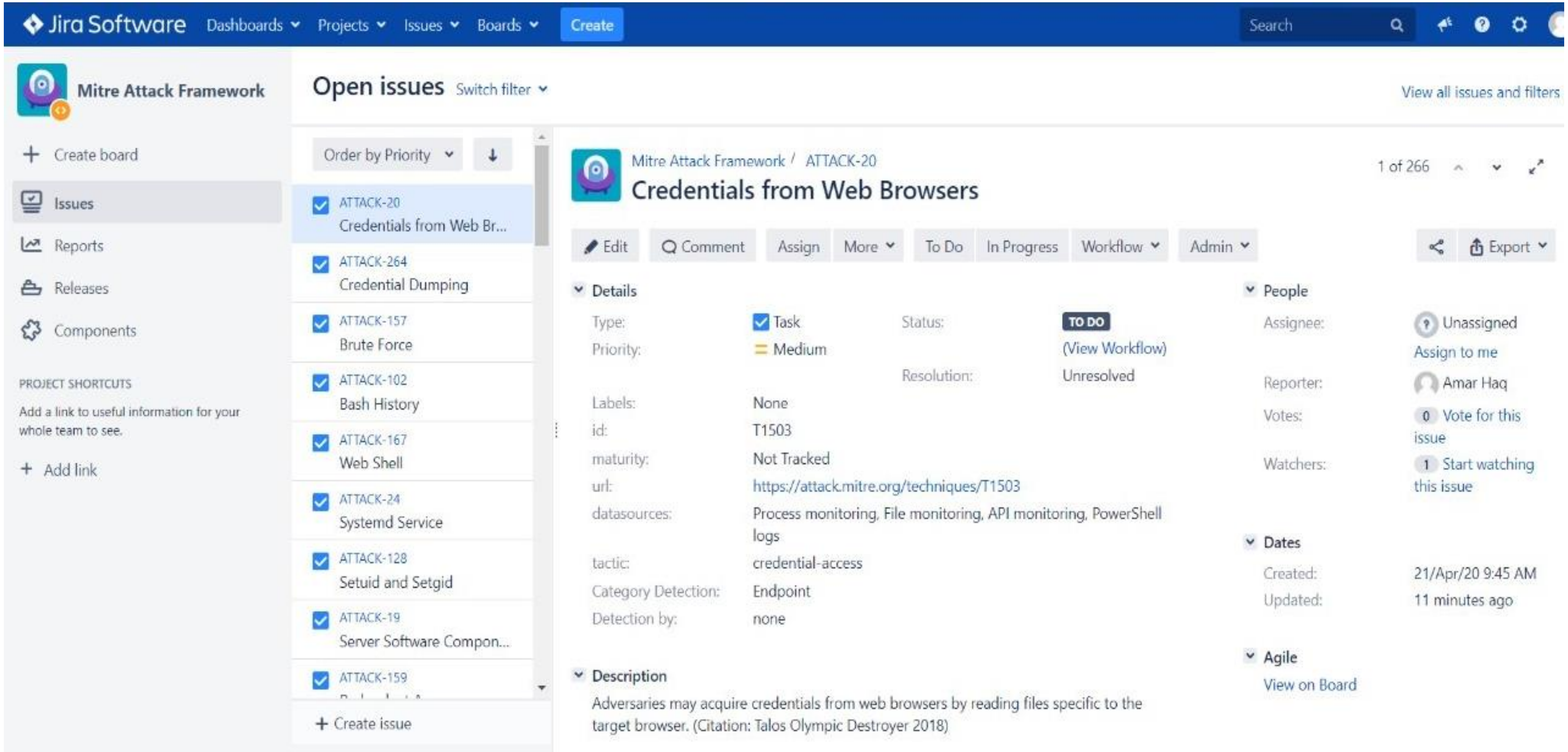
- Oversee the current capabilities of Endpoint Detection Tools and mapped into MITRE ATT&CK
- Create tracking and coverage platform to identified the issue (gaps and testing)
- Testing and Validate the detection capabilities based on rules / policy developed at endpoint side (Does the rules still valid, tune the rules for false positive, or need some improvement)
- Oversee the gaps which is not filled yet by the detection capabilities of the endpoint detection tools
- Create a platform as knowledge management for newcomers to identified the detection rules / policy for threat hunting

Tracking Coverage and Hunting Toolkit

Attack2Jira from Mauricio Velazco (https://github.com/mvelazc0/attack2jira)

- Manage ATT&CK Techniques as entities
- Tracking Coverage of the Detection Technology Rules and Policy Over the Time
- Allow collaboration within Internal Team to improve visibility from endpoint side
- As a baseline and threat hunting knowledge for each member about the detection rules (so new member will know, which rules or policy applied to detect the Technique from the MITRE ATT&CK Framework)

Attack2Jira Dashboard



Mitre Attack Framework

- Create board
- Issues
- Reports
- Releases
- Components

PROJECT SHORTCUTS

Add a link to useful information for your whole team to see.

+ Add link

Open issues

Switch filter

View all issues and filters

Order by Priority

- ☑ ATTACK-20 Credentials from Web Br...
- ☑ ATTACK-264 Credential Dumping
- ☑ ATTACK-157 Brute Force
- ☑ ATTACK-102 Bash History
- ☑ ATTACK-167 Web Shell
- ☑ ATTACK-24 Systemd Service
- ☑ ATTACK-128 Setuid and Setgid
- ☑ ATTACK-19 Server Software Compon...
- ☑ ATTACK-159

+ Create issue

Mitre Attack Framework / ATTACK-20

Credentials from Web Browsers

1 of 266

Details

Type: ☑ Task

Priority: Medium

Status: TO DO (View Workflow)

Resolution: Unresolved

Labels: None

id: T1503

maturity: Not Tracked

url: https://attack.mitre.org/techniques/T1503

datasources: Process monitoring, File monitoring, API monitoring, PowerShell logs

tactic: credential-access

Category Detection: Endpoint

Detection by: none

Description

Adversaries may acquire credentials from web browsers by reading files specific to the target browser. (Citation: Talos Olympic Destroyer 2018)

People

Assignee: Unassigned

Assign to me

Reporter: Amar Haq

Votes: 0 Vote for this issue

Watchers: 1 Start watching this issue

Dates

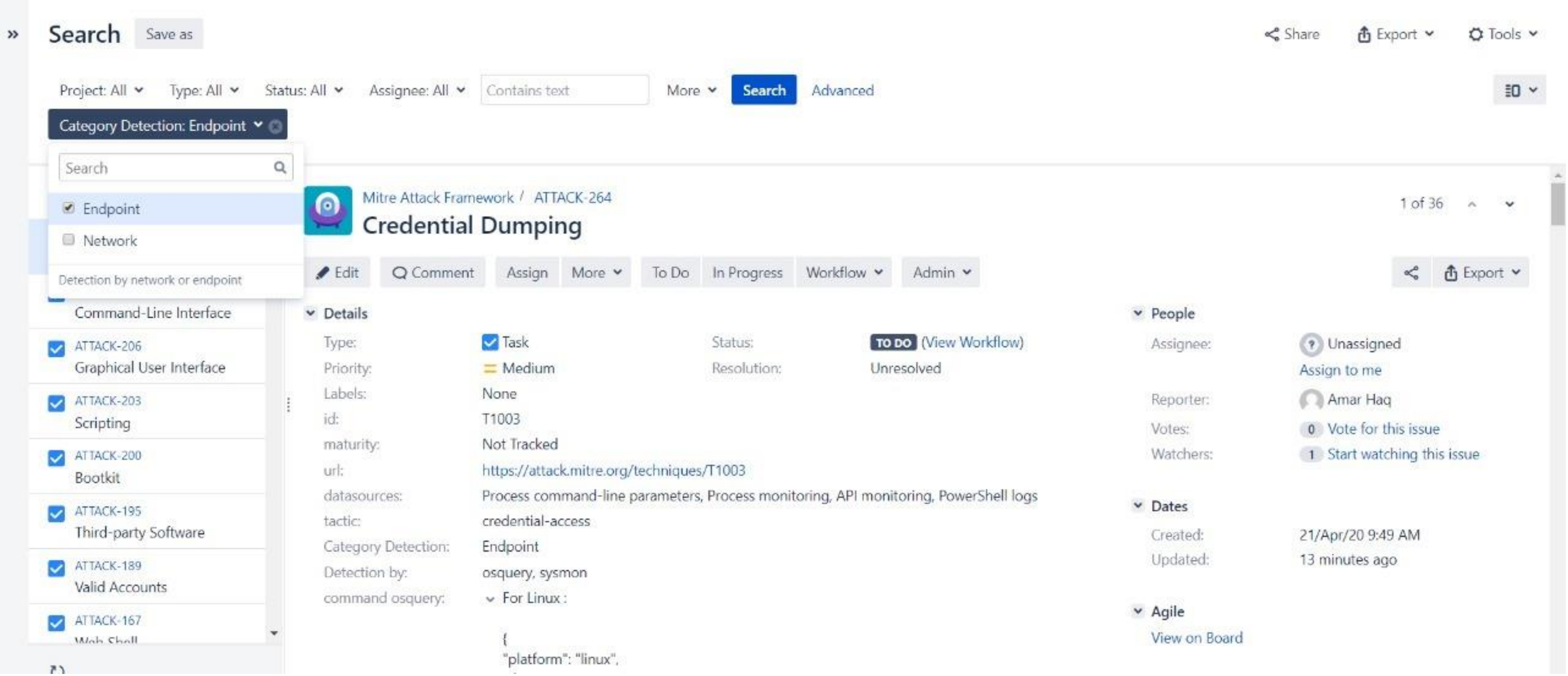
Created: 21/Apr/20 9:45 AM

Updated: 11 minutes ago

Agile

View on Board

Attack2Jira Category



Category Detection: Endpoint

Search

☑ Endpoint

□ Network

Detection by network or endpoint

Command-Line Interface

☑ ATTACK-206 Graphical User Interface

☑ ATTACK-203 Scripting

☑ ATTACK-200 Bootkit

☑ ATTACK-195 Third-party Software

☑ ATTACK-189 Valid Accounts

☑ ATTACK-167 Web Shell

Mitre Attack Framework / ATTACK-264

Credential Dumping

1 of 36

Details

Type: Task

Status: TO DO (View Workflow)

Priority: Medium

Resolution: Unresolved

Labels: None

id: T1003

maturity: Not Tracked

url: https://attack.mitre.org/techniques/T1003

datasources: Process command-line parameters, Process monitoring, API monitoring, PowerShell logs

tactic: credential-access

Category Detection: Endpoint

Detection by: osquery, sysmon

command osquery: For Linux :

```
{
"platform": "linux",
```

People

Assignee: Unassigned

Assign to me

Reporter: Amar Haq

Votes: 0 Vote for this issue

Watchers: 1 Start watching this issue

Dates

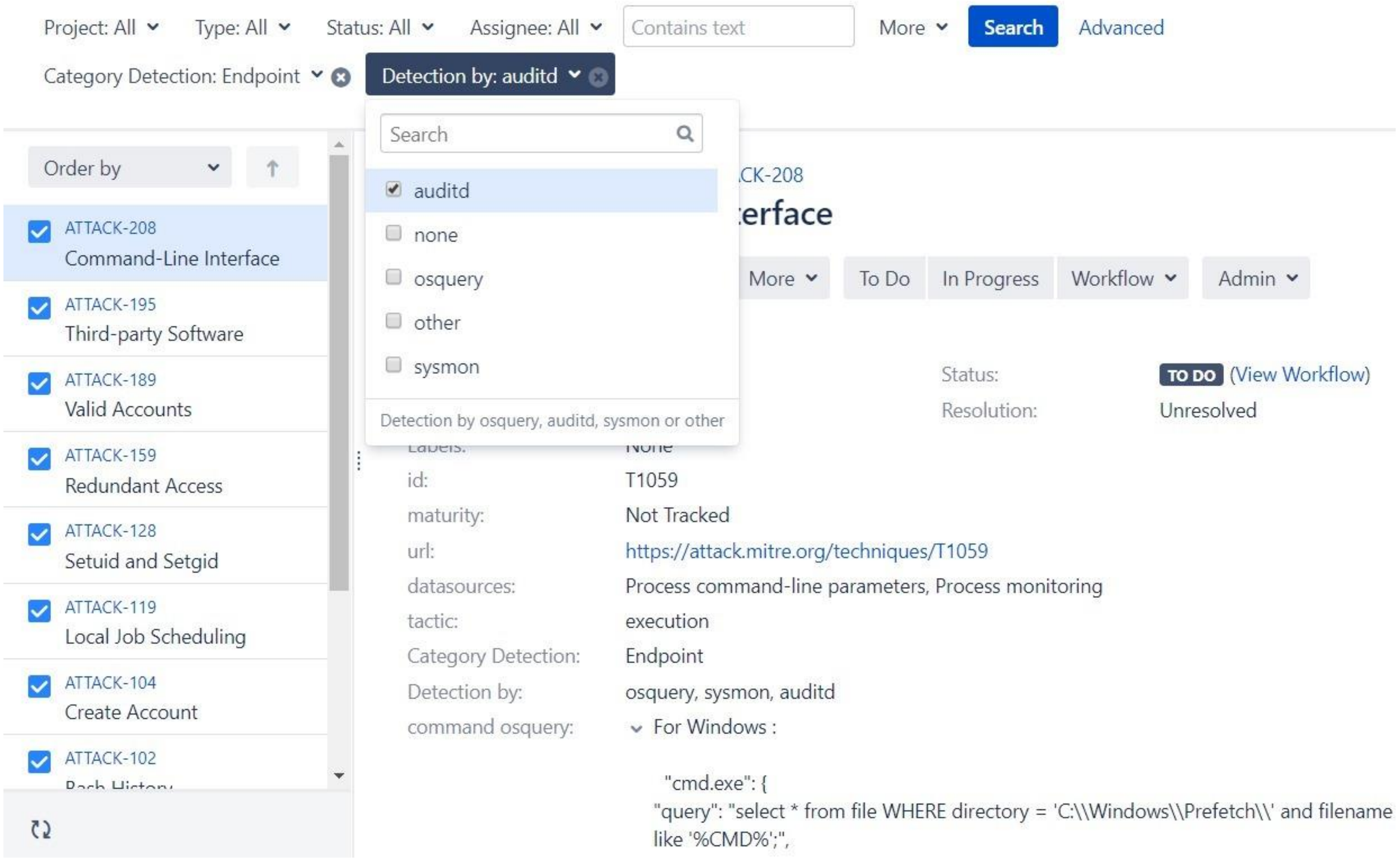
Created: 21/Apr/20 9:49 AM

Updated: 13 minutes ago

Agile

View on Board

Attack2Jira Endpoint Detection



☑ auditd
□ none
□ osquery
□ other
□ sysmon

Detection by osquery, auditd, sysmon or other

☑ ATTACK-208 Command-Line Interface
☑ ATTACK-195 Third-party Software
☑ ATTACK-189 Valid Accounts
☑ ATTACK-159 Redundant Access
☑ ATTACK-128 Setuid and Setgid
☑ ATTACK-119 Local Job Scheduling
☑ ATTACK-104 Create Account
☑ ATTACK-102 Bash History

Status:	TO DO (View Workflow)
Resolution:	Unresolved

Labels:	None
id:	T1059
maturity:	Not Tracked
url:	https://attack.mitre.org/techniques/T1059
datasources:	Process command-line parameters, Process monitoring
tactic:	execution
Category Detection:	Endpoint
Detection by:	osquery, sysmon, auditd
command osquery:	For Windows :

```
  "cmd.exe": {
"query": "select * from file WHERE directory = 'C:\\Windows\\Prefetch\\' and filename
like '%CMD%';",
```

Summary

- ATT&CK Framework Can be used to evaluate the Endpoint Security before our organization acquired the technology and after the acquisition of the technology for operational process
- Continuous Assessment for Endpoint Visibility is a must and closing the gaps as much as possible from the attacker TTPs
- ATT&CK Framework helps us focusing on specific Technique and Tactic which we want to prioritized for our Endpoint Security visibility

Thank You!

- Thank you to MITRE Engenuity
- Thank you to MITRE EU ATT&CK Community
- Thank you to Freddy Dezeure

Contact Me :

@digitoktav

/in/digitoktavianto

https://medium.com/@digit.oktavianto