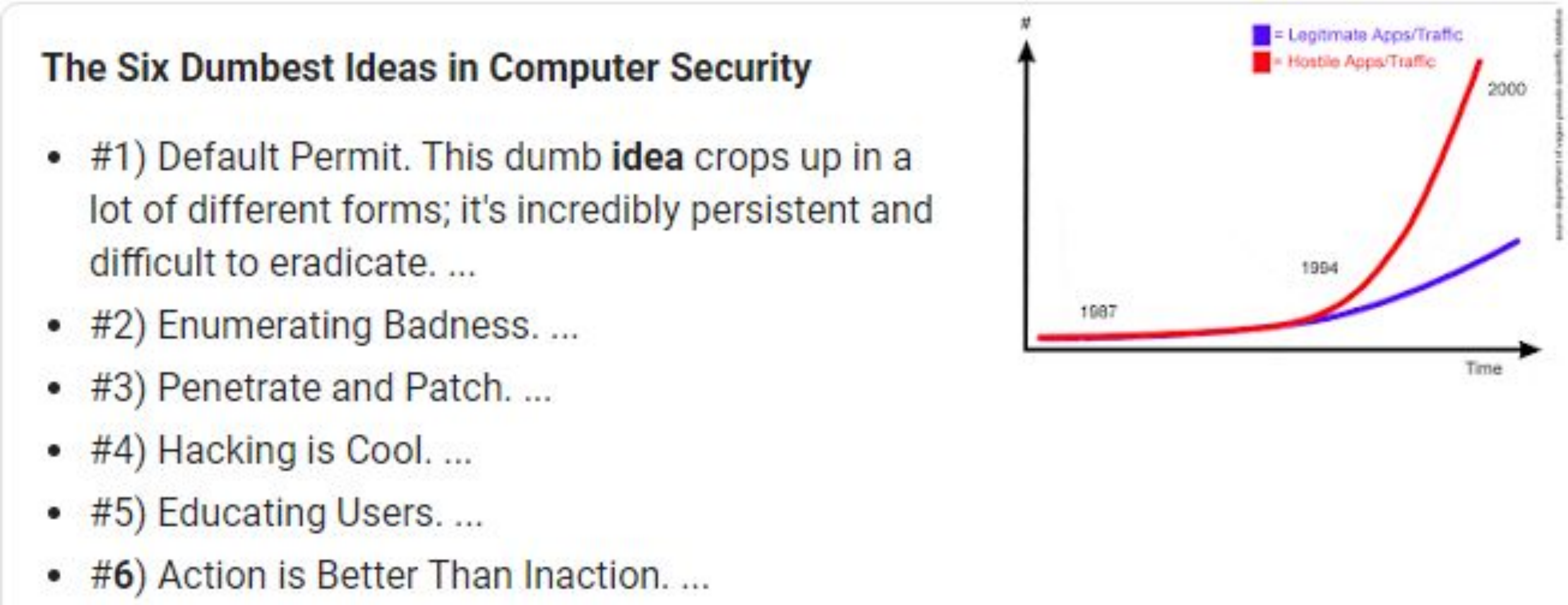
Threat Intel:

Yet Another Useless Rant With John Yelling At Clouds

John Strand

Let’s Talk About Bad Ideas

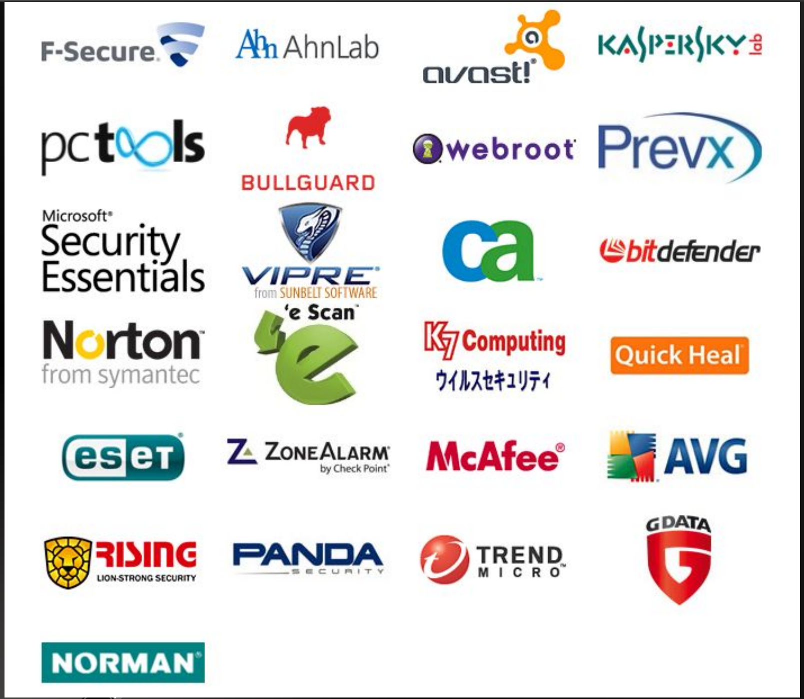


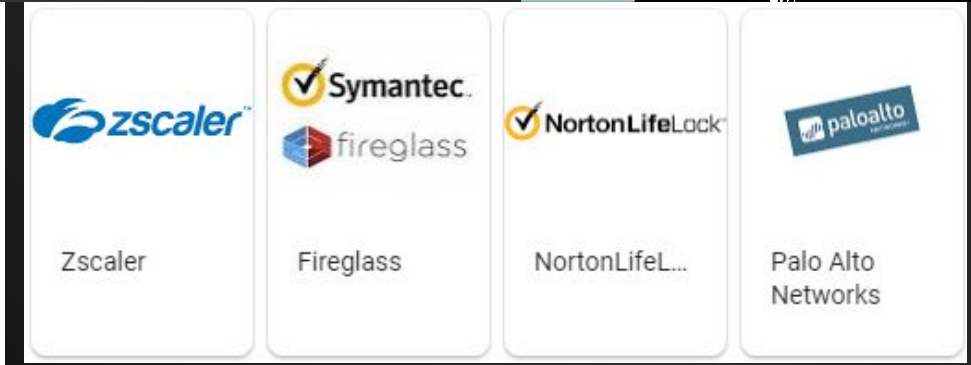
The Six Dumbest Ideas in Computer Security

- #1) Default Permit. This dumb **idea** crops up in a lot of different forms; it's incredibly persistent and difficult to eradicate. ...
- #2) Enumerating Badness. ...
- #3) Penetrate and Patch. ...
- #4) Hacking is Cool. ...
- #5) Educating Users. ...
- #6) Action is Better Than Inaction. ...

Why I Hate Threat Intel

Some Companies..

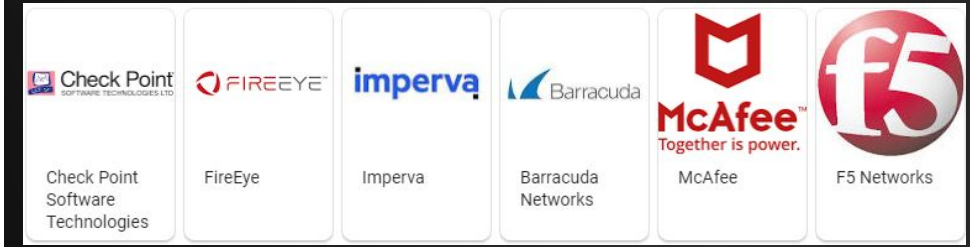



Zscaler

Fireglass

NortonLifeL...

Palo Alto Networks


Check Point Software Technologies

FireEye

Imperva

Barracuda Networks

McAfee

F5 Networks

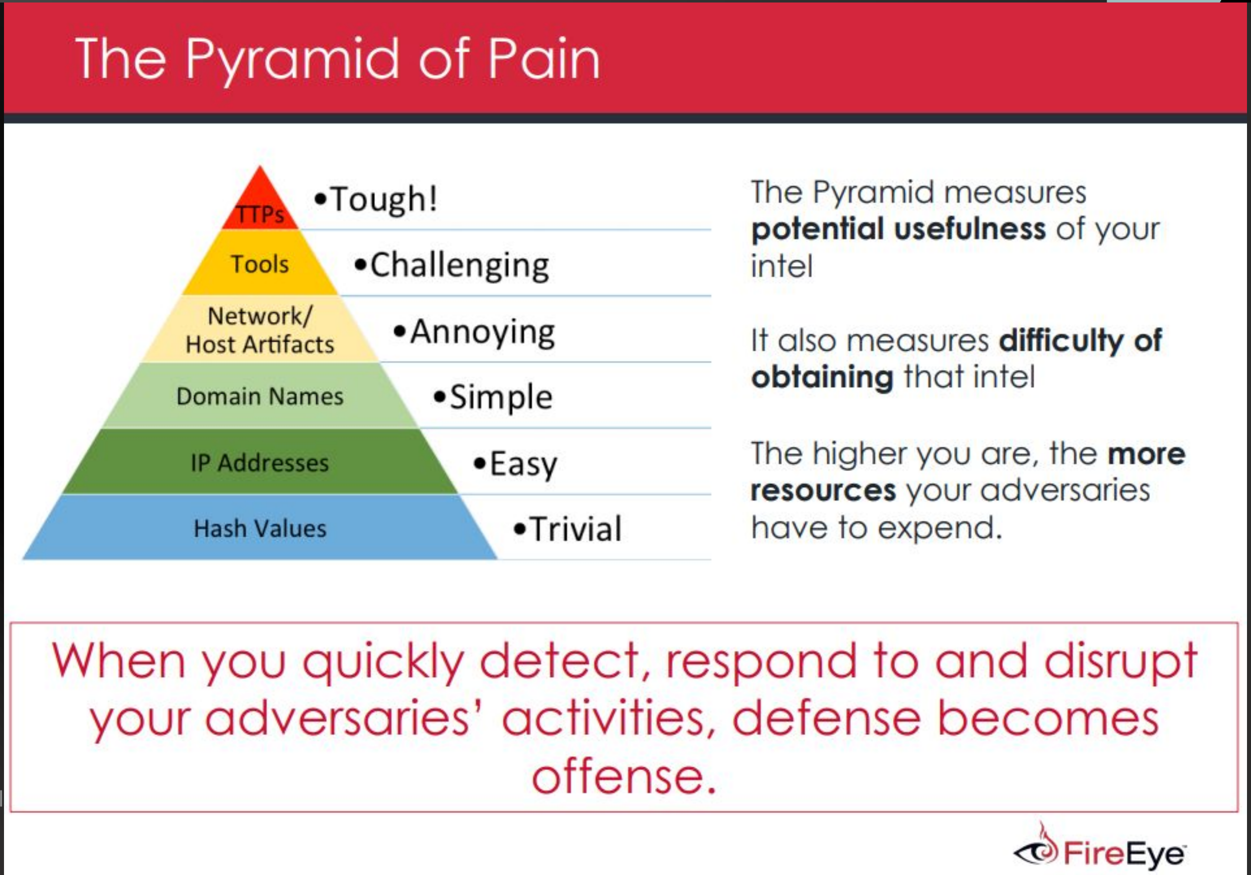
Check Point SOFTWARE TECHNOLOGIES LTD
FIREEYE
imperva
Barracuda
McAfee Together is power.
f5

For Reference..

HI HO! HI HO! ITS OFF TO WORK WE GO.
SIGNATURES AND HASHES ALL DAY LONG. HI HO! HI HO!
imgflip.com

Artist's rendering of AV employes going to work

Credit Where Credit is Due



The Pyramid of Pain

TTPs	•Tough!
Tools	•Challenging
Network/ Host Artifacts	•Annoying
Domain Names	•Simple
IP Addresses	•Easy
Hash Values	•Trivial

The Pyramid measures **potential usefulness** of your intel

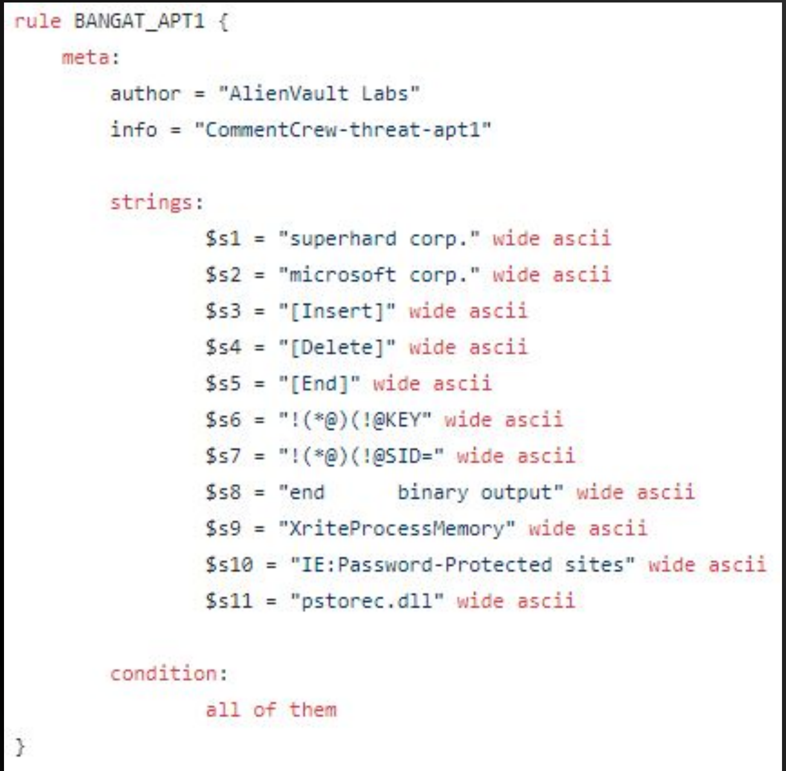
It also measures **difficulty of obtaining** that intel

The higher you are, the **more resources** your adversaries have to expend.

When you quickly detect, respond to and disrupt your adversaries' activities, defense becomes offense.

FireEye

Quick! Can You Spot the Problem?

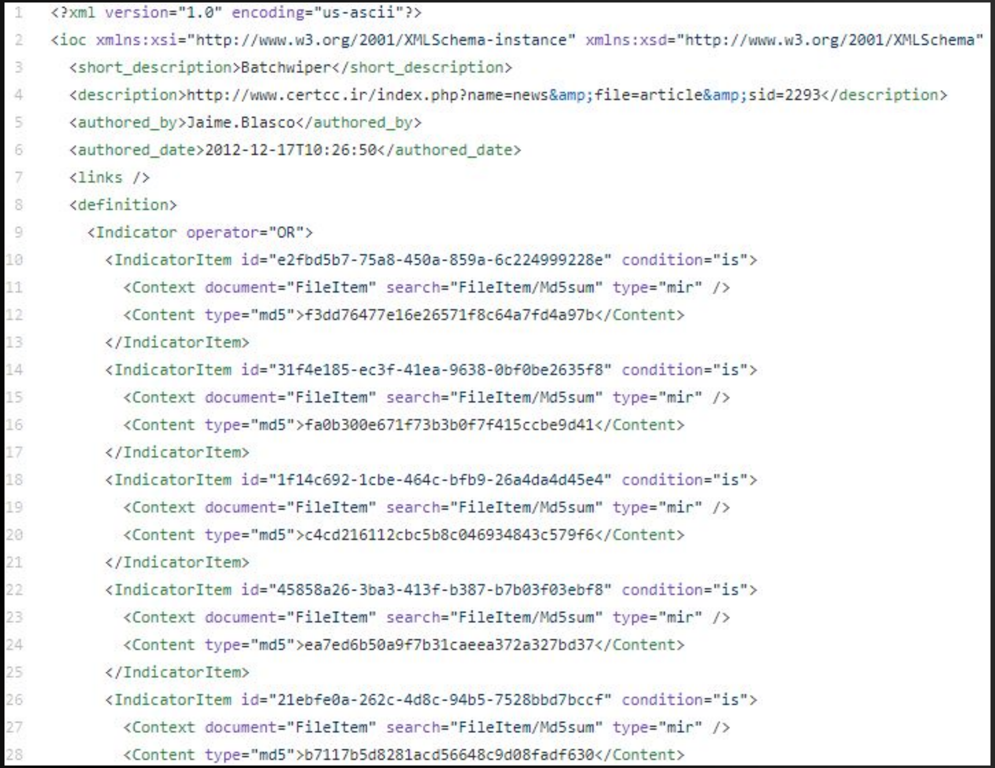


```
rule BANGAT_APT1 {
    meta:
        author = "AlienVault Labs"
        info = "CommentCrew-threat-apt1"

        strings:
                $s1 = "superhard corp." wide ascii
                $s2 = "microsoft corp." wide ascii
                $s3 = "[Insert]" wide ascii
                $s4 = "[Delete]" wide ascii
                $s5 = "[End]" wide ascii
                $s6 = "!(*@)(!@KEY" wide ascii
                $s7 = "!(*@)(!@SID=" wide ascii
                $s8 = "end      binary output" wide ascii
                $s9 = "XriteProcessMemory" wide ascii
                $s10 = "IE:Password-Protected sites" wide ascii
                $s11 = "pstorec.dll" wide ascii

        condition:
                all of them
}
```

Let’s Try Again



```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <short_description>Batchwiper</short_description>
  <description>http://www.certcc.ir/index.php?name=news&amp;file=article&amp;sid=2293</description>
  <authored_by>Jaime.Blasco</authored_by>
  <authored_date>2012-12-17T10:26:50</authored_date>
  <links />
  <definition>
    <Indicator operator="OR">
      <IndicatorItem id="e2fbd5b7-75a8-450a-859a-6c224999228e" condition="is">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
        <Content type="md5">f3dd76477e16e26571f8c64a7fd4a97b</Content>
      </IndicatorItem>
      <IndicatorItem id="31f4e185-ec3f-41ea-9638-0bf0be2635f8" condition="is">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
        <Content type="md5">fa0b300e671f73b3b0f7f415ccbe9d41</Content>
      </IndicatorItem>
      <IndicatorItem id="1f14c692-1cbe-464c-bfb9-26a4da4d45e4" condition="is">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
        <Content type="md5">c4cd216112cbc5b8c046934843c579f6</Content>
      </IndicatorItem>
      <IndicatorItem id="45858a26-3ba3-413f-b387-b7b03f03ebf8" condition="is">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
        <Content type="md5">ea7ed6b50a9f7b31caeea372a327bd37</Content>
      </IndicatorItem>
      <IndicatorItem id="21ebfe0a-262c-4d8c-94b5-7528bbd7bccf" condition="is">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
        <Content type="md5">b7117b5d8281acd56648c9d08fadf630</Content>
```

Conversations with John..

Conversation #1

Them: “So, we are going to take intel feeds from multiple sources and correlate hashes and IP addresses to find evil in our network.”

Me: “You mean like your AV/IDS/IPS/Firewall/Proxy Vendors?”

Them: “Yes, but we will do it better.”

Conversation #2

Them: “I know you hate threat intel feeds, but one time, last year, we caught an attacker with them!”

Me: “Good for you! Your skills are unparalleled and amazing. You are truly a credit to the industry. However, does that not speak more to the failure of your AV/IDS/IPS/Firewall vendor than your great and righteous success?”

Trying to Make Hacking Easy.

- For years, vendors have been trying to make “hacking” easy
- “We can automate a pentest!”
- “We can automate a Red Team”
- This leads us to the MITRE Problem
- MITRE ATT&CK is one of the best things to happen to the industry..
- But..

We Have a Problem.

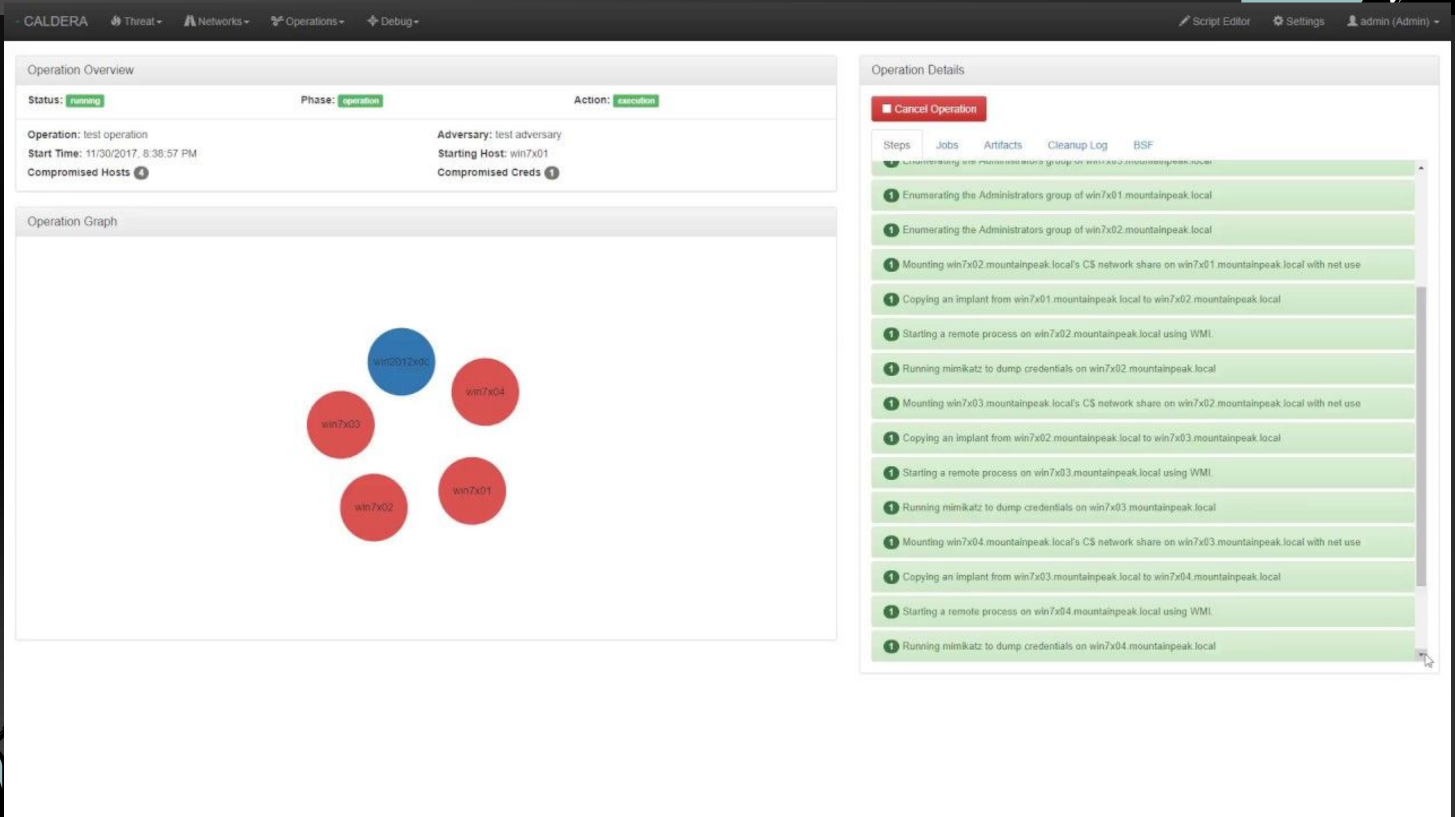
“Stop playing ATT&CK Bingo!”
-Bryson Bort, Scythe

“ATT&CK and Atomic Red Team are not signature databases” - John Strand, BHIS

But, We Should Be Emulating

- A lot…
- Like all the time
- With many, many different tools
- Believe it or not, this is Threat Intel
- Using tools and hiring testers is applied threat intelligence
    - But it requires repetition and understanding of the attacks
- It gives you the ability to see how your organization will react to a *dynamic* attack

Open Source Tool Example: Caldera



Operation Overview

Status: running **Phase:** operation **Action:** execution

Operation: test operation
Start Time: 11/30/2017, 8:38:57 PM
Compromised Hosts 4

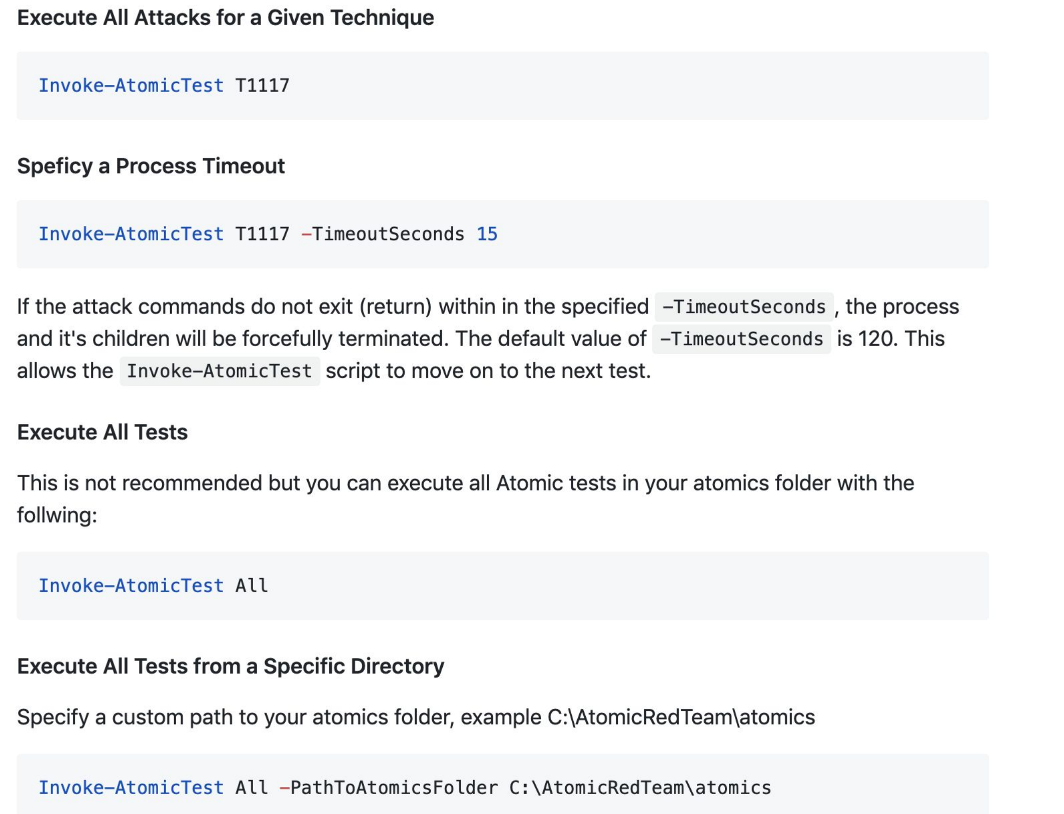
Adversary: test adversary
Starting Host: win7x01
Compromised Creds 1

Operation Graph

Operation Details

1 Enumerating the Administrators group of win7x03.mountainpeak.local
1 Enumerating the Administrators group of win7x01.mountainpeak.local
1 Enumerating the Administrators group of win7x02.mountainpeak.local
1 Mounting win7x02.mountainpeak.local's C$ network share on win7x01.mountainpeak.local with net use
1 Copying an implant from win7x01.mountainpeak.local to win7x02.mountainpeak.local
1 Starting a remote process on win7x02.mountainpeak.local using WMI.
1 Running mimikatz to dump credentials on win7x02.mountainpeak.local
1 Mounting win7x03.mountainpeak.local's C$ network share on win7x02.mountainpeak.local with net use
1 Copying an implant from win7x02.mountainpeak.local to win7x03.mountainpeak.local
1 Starting a remote process on win7x03.mountainpeak.local using WMI.
1 Running mimikatz to dump credentials on win7x03.mountainpeak.local
1 Mounting win7x04.mountainpeak.local's C$ network share on win7x03.mountainpeak.local with net use
1 Copying an implant from win7x03.mountainpeak.local to win7x04.mountainpeak.local
1 Starting a remote process on win7x04.mountainpeak.local using WMI.
1 Running mimikatz to dump credentials on win7x04.mountainpeak.local

Open Source Tool Example: Atomic Red Team



Execute All Attacks for a Given Technique

```
Invoke-AtomicTest T1117
```

Speficy a Process Timeout

```
Invoke-AtomicTest T1117 -TimeoutSeconds 15
```

If the attack commands do not exit (return) within in the specified `-TimeoutSeconds`, the process and it's children will be forcefully terminated. The default value of `-TimeoutSeconds` is 120. This allows the `Invoke-AtomicTest` script to move on to the next test.

Execute All Tests

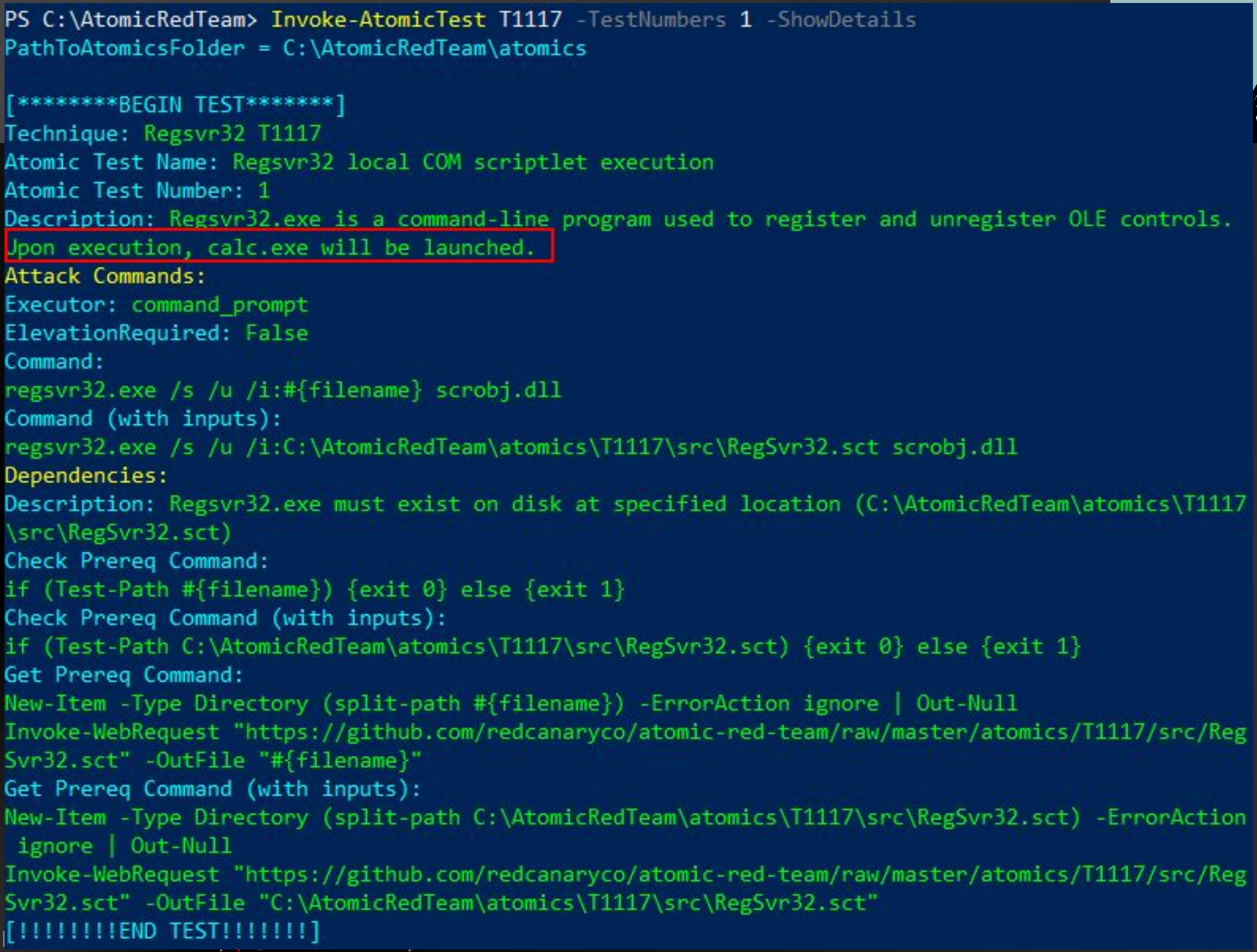
This is not recommended but you can execute all Atomic tests in your atomics folder with the follwing:

```
Invoke-AtomicTest All
```

Execute All Tests from a Specific Directory

Specify a custom path to your atomics folder, example C:\AtomicRedTeam\atomics

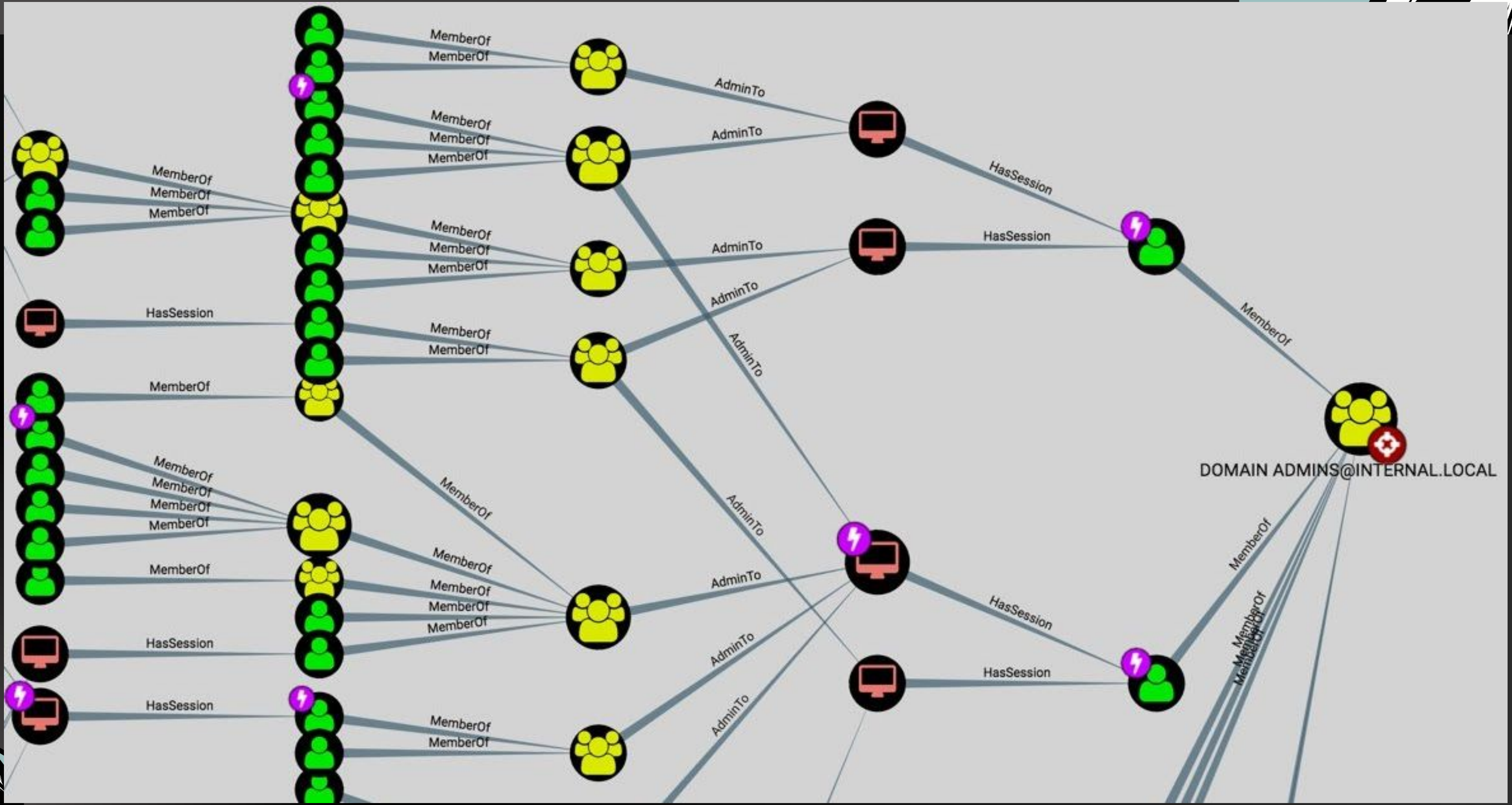
```
Invoke-AtomicTest All -PathToAtomicsFolder C:\AtomicRedTeam\atomics
```



```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1117 -TestNumbers 1 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: Regsvr32 T1117
Atomic Test Name: Regsvr32 local COM scriptlet execution
Atomic Test Number: 1
Description: Regsvr32.exe is a command-line program used to register and unregister OLE controls.
Jpon execution, calc.exe will be launched.
Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
regsvr32.exe /s /u /i:#{filename} scrobj.dll
Command (with inputs):
regsvr32.exe /s /u /i:C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct scrobj.dll
Dependencies:
Description: Regsvr32.exe must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1117
\src\RegSvr32.sct)
Check Prereq Command:
if (Test-Path #{filename}) {exit 0} else {exit 1}
Check Prereq Command (with inputs):
if (Test-Path C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct) {exit 0} else {exit 1}
Get Prereq Command:
New-Item -Type Directory (split-path #{filename}) -ErrorAction ignore | Out-Null
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1117/src/Reg
Svr32.sct" -OutFile "#{filename}"
Get Prereq Command (with inputs):
New-Item -Type Directory (split-path C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct) -ErrorAction
 ignore | Out-Null
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1117/src/Reg
Svr32.sct" -OutFile "C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct"
[!!!!!!!!END TEST!!!!!!!]
```

Open Source Tool Example: Bloodhound



© Black Hills Information Security | @BHInfoSecurity

Threat Emulation Warning

- One of the traps of the MITRE framework and threat emulation is we train or systems to detect specific attacks
- Most of the attacks in Atomic Red Team and MITRE are representations of classes of attacks
- We are seeing vendors simply detect those attacks
  - More on this later!
- A few modifications and you can easily bypass detection

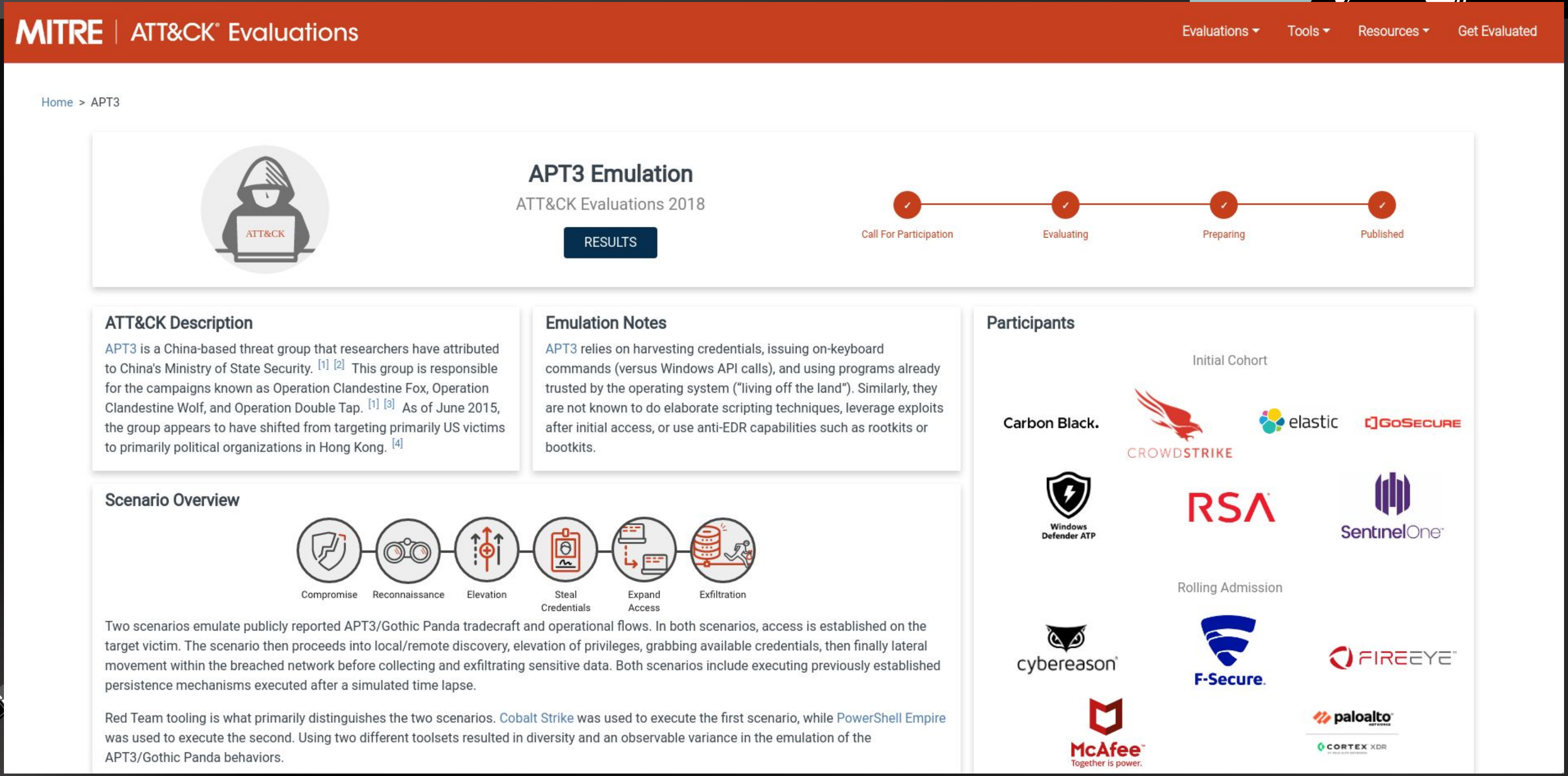
Commercial Offerings

ATTACKIQ

SCYTHE

XM CYBER

Everyone's a Winner!



APT3 Emulation

ATT&CK Evaluations 2018

ATT&CK Description

APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security. [1] [2] This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap. [1] [3] As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong. [4]

Emulation Notes

APT3 relies on harvesting credentials, issuing on-keyboard commands (versus Windows API calls), and using programs already trusted by the operating system ("living off the land"). Similarly, they are not known to do elaborate scripting techniques, leverage exploits after initial access, or use anti-EDR capabilities such as rootkits or bootkits.

Participants

Initial Cohort

Carbon Black. CrowdStrike elastic GoSecure Windows Defender ATP RSA SentinelOne

Rolling Admission

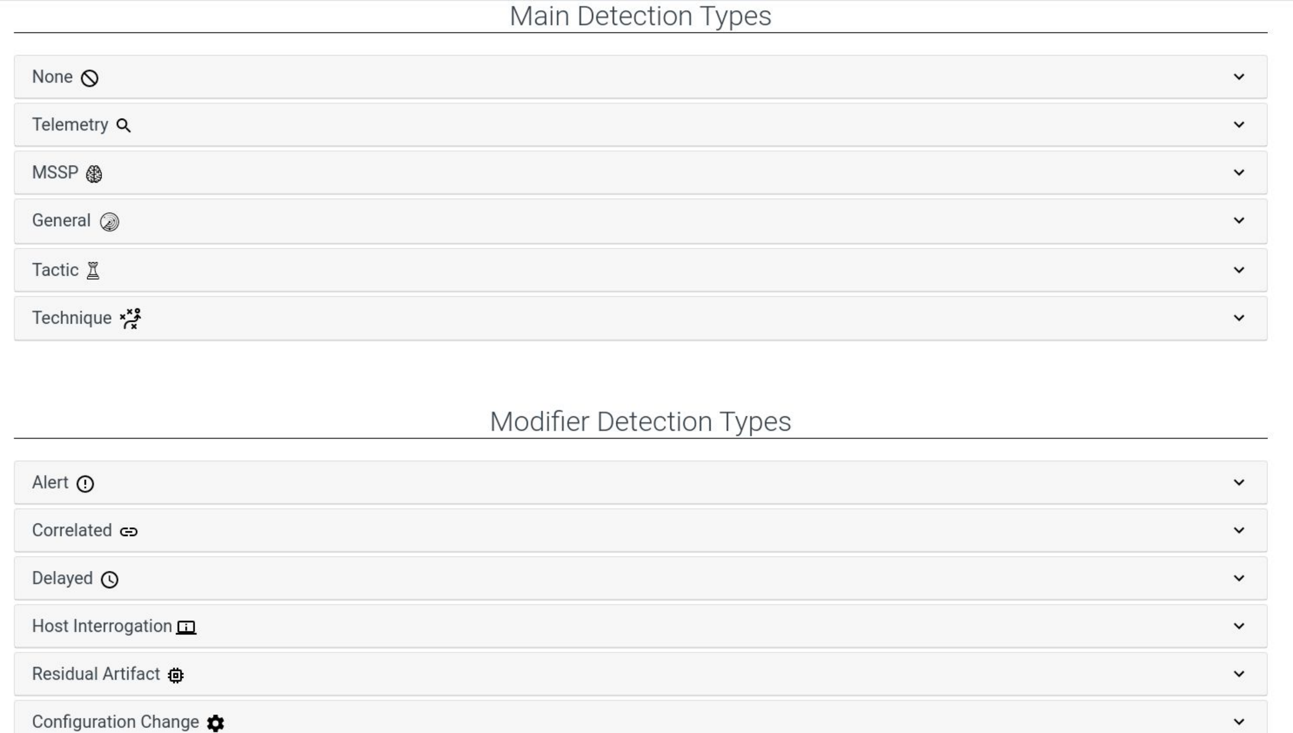
cybereason F-Secure. FireEye McAfee Together is power. paloalto Cortex XDR

Scenario Overview

Two scenarios emulate publicly reported APT3/Gothic Panda tradecraft and operational flows. In both scenarios, access is established on the target victim. The scenario then proceeds into local/remote discovery, elevation of privileges, grabbing available credentials, then finally lateral movement within the breached network before collecting and exfiltrating sensitive data. Both scenarios include executing previously established persistence mechanisms executed after a simulated time lapse.

Red Team tooling is what primarily distinguishes the two scenarios. Cobalt Strike was used to execute the first scenario, while PowerShell Empire was used to execute the second. Using two different toolsets resulted in diversity and an observable variance in the emulation of the APT3/Gothic Panda behaviors.

Detection Categories



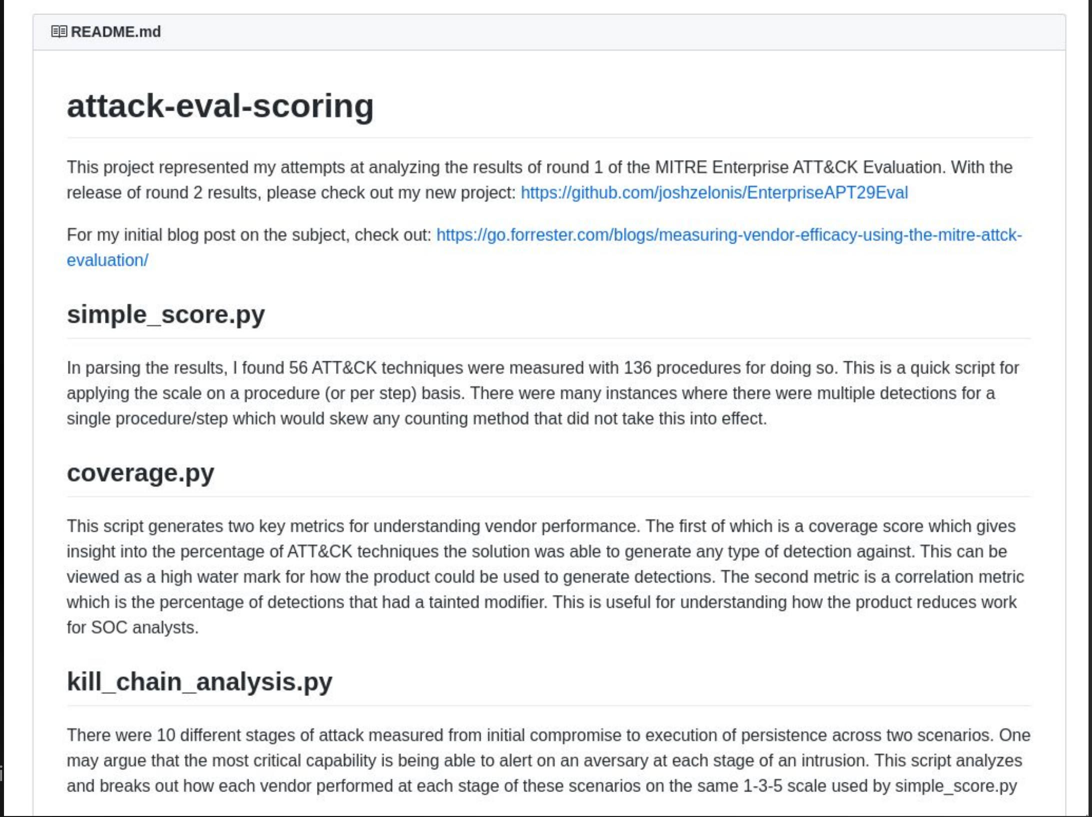
Main Detection Types

- None
- Telemetry
- MSSP
- General
- Tactic
- Technique

Modifier Detection Types

- Alert
- Correlated
- Delayed
- Host Interrogation
- Residual Artifact
- Configuration Change

Or not?



README.md

attack-eval-scoring

This project represented my attempts at analyzing the results of round 1 of the MITRE Enterprise ATT&CK Evaluation. With the release of round 2 results, please check out my new project: https://github.com/joshzelonis/EnterpriseAPT29Eval

For my initial blog post on the subject, check out: https://go.forrester.com/blogs/measuring-vendor-efficacy-using-the-mitre-attck-evaluation/

simple_score.py

In parsing the results, I found 56 ATT&CK techniques were measured with 136 procedures for doing so. This is a quick script for applying the scale on a procedure (or per step) basis. There were many instances where there were multiple detections for a single procedure/step which would skew any counting method that did not take this into effect.

coverage.py

This script generates two key metrics for understanding vendor performance. The first of which is a coverage score which gives insight into the percentage of ATT&CK techniques the solution was able to generate any type of detection against. This can be viewed as a high water mark for how the product could be used to generate detections. The second metric is a correlation metric which is the percentage of detections that had a tainted modifier. This is useful for understanding how the product reduces work for SOC analysts.

kill_chain_analysis.py

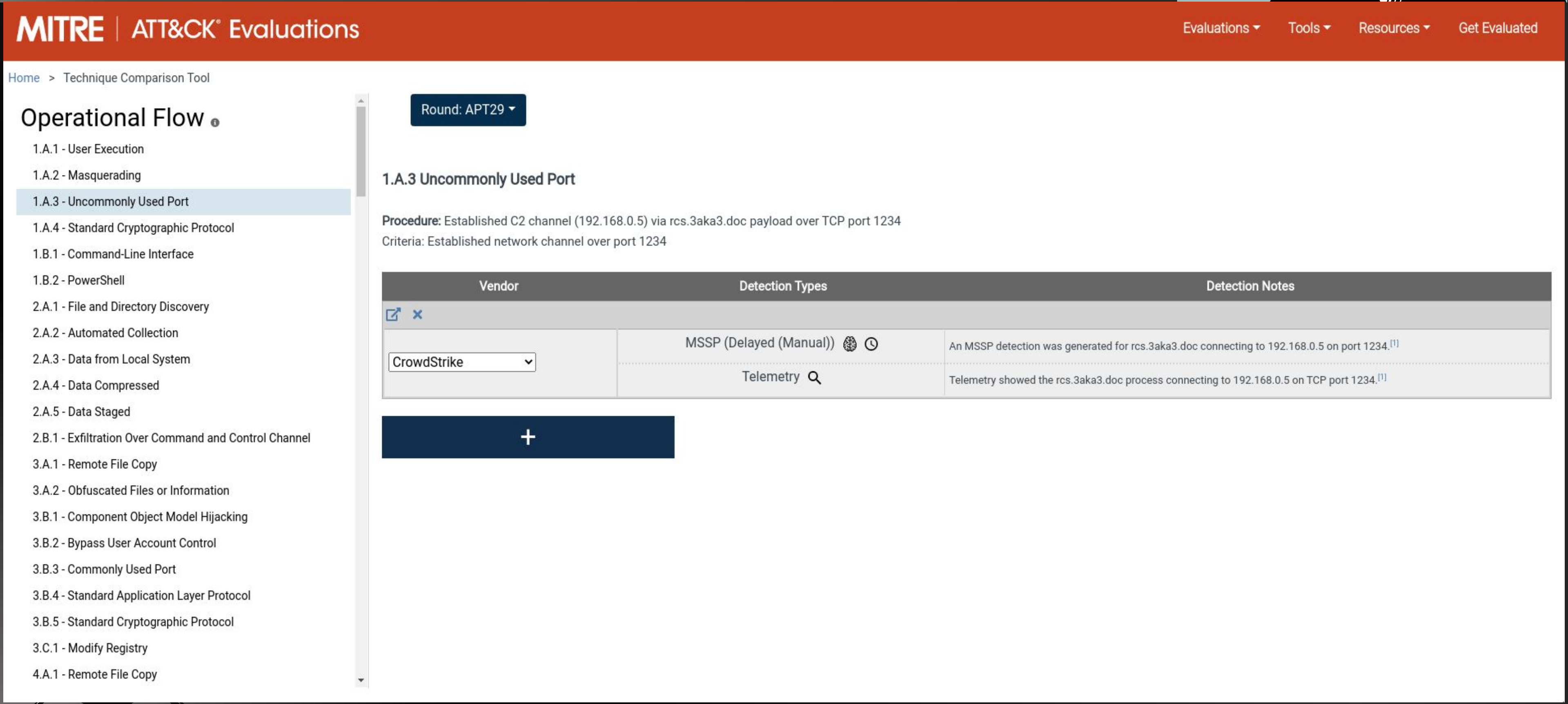
There were 10 different stages of attack measured from initial compromise to execution of persistence across two scenarios. One may argue that the most critical capability is being able to alert on an aversary at each stage of an intrusion. This script analyzes and breaks out how each vendor performed at each stage of these scenarios on the same 1-3-5 scale used by simple_score.py

What Does This Mean?

- Turns out… Not a lot
  - It seems that some vendors possibly, maybe, kind of did better?
- Does the MSSP detect count?
- Does logging without alerting count?
- Testing was not geared to an analyst sitting at a desk
- Far too many ways to say “We caught it!”
- What does the real world say?

Red Team Perspective

- Many of these products are very, very solid at detecting attacks
- They are very good at detecting lateral movement
- They can all be bypassed
- There is the problem
- If a tool can be bypassed, is it worthless?
- How hard is it?
- Does this test reflect reality?



Home > Technique Comparison Tool

Operational Flow

- 1.A.1 - User Execution
- 1.A.2 - Masquerading
- 1.A.3 - Uncommonly Used Port
- 1.A.4 - Standard Cryptographic Protocol
- 1.B.1 - Command-Line Interface
- 1.B.2 - PowerShell
- 2.A.1 - File and Directory Discovery
- 2.A.2 - Automated Collection
- 2.A.3 - Data from Local System
- 2.A.4 - Data Compressed
- 2.A.5 - Data Staged
- 2.B.1 - Exfiltration Over Command and Control Channel
- 3.A.1 - Remote File Copy
- 3.A.2 - Obfuscated Files or Information
- 3.B.1 - Component Object Model Hijacking
- 3.B.2 - Bypass User Account Control
- 3.B.3 - Commonly Used Port
- 3.B.4 - Standard Application Layer Protocol
- 3.B.5 - Standard Cryptographic Protocol
- 3.C.1 - Modify Registry
- 4.A.1 - Remote File Copy

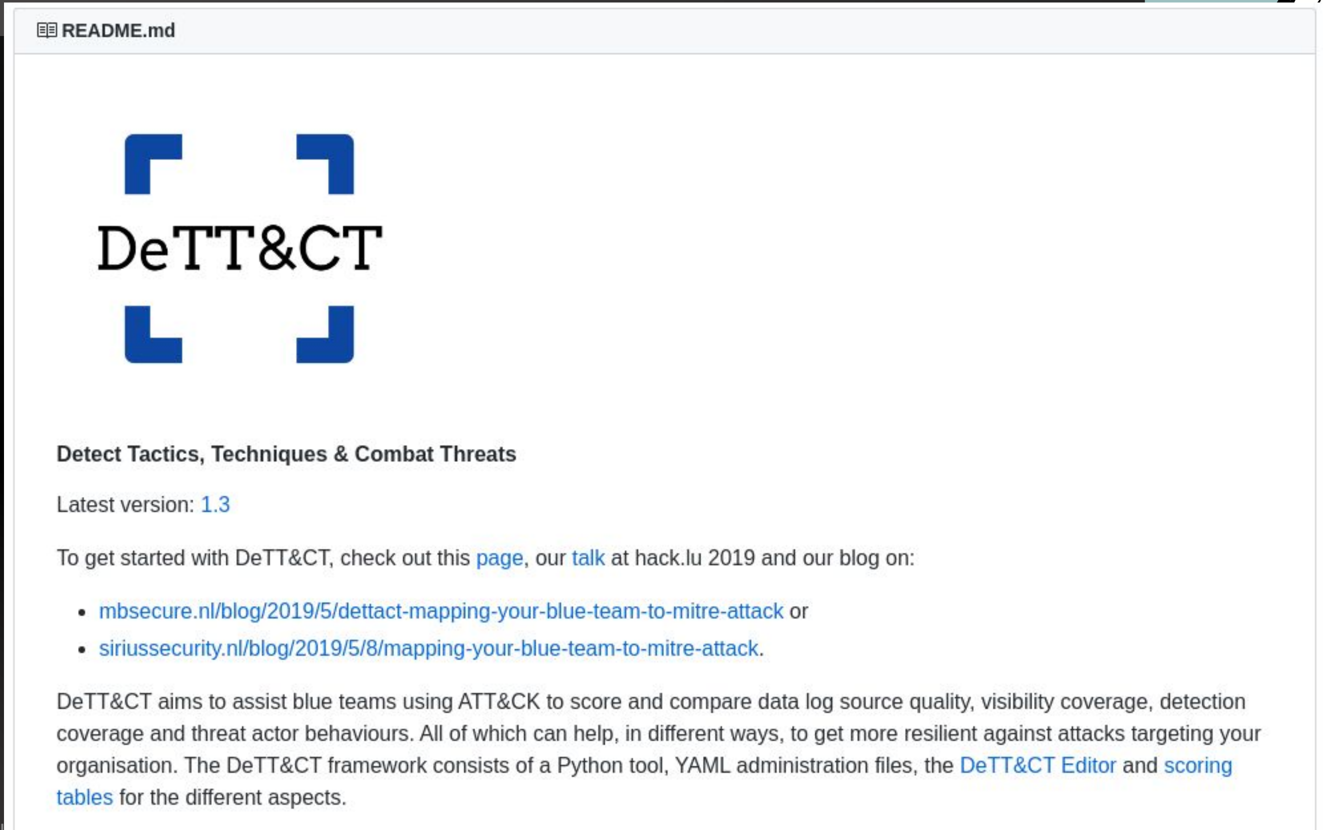
1.A.3 Uncommonly Used Port

Procedure: Established C2 channel (192.168.0.5) via rcs.3aka3.doc payload over TCP port 1234

Criteria: Established network channel over port 1234

Vendor	Detection Types	Detection Notes
CrowdStrike	MSSP (Delayed (Manual)) 🧠 🕒	An MSSP detection was generated for rcs.3aka3.doc connecting to 192.168.0.5 on port 1234.[1]
	Telemetry 🔍	Telemetry showed the rcs.3aka3.doc process connecting to 192.168.0.5 on TCP port 1234.[1]

DeTT&CT



README.md

DeTT&CT

Detect Tactics, Techniques & Combat Threats

Latest version: 1.3

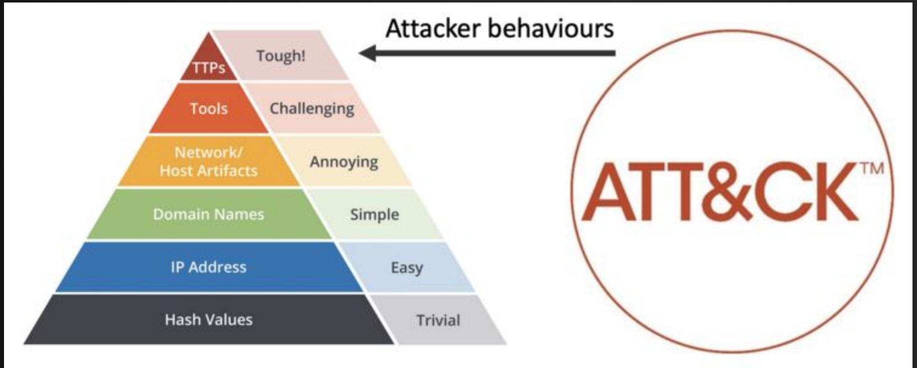
To get started with DeTT&CT, check out this page, our talk at hack.lu 2019 and our blog on:

- mbsecure.nl/blog/2019/5/dettact-mapping-your-blue-team-to-mitre-attack or
- siriussecurity.nl/blog/2019/5/8/mapping-your-blue-team-to-mitre-attack.

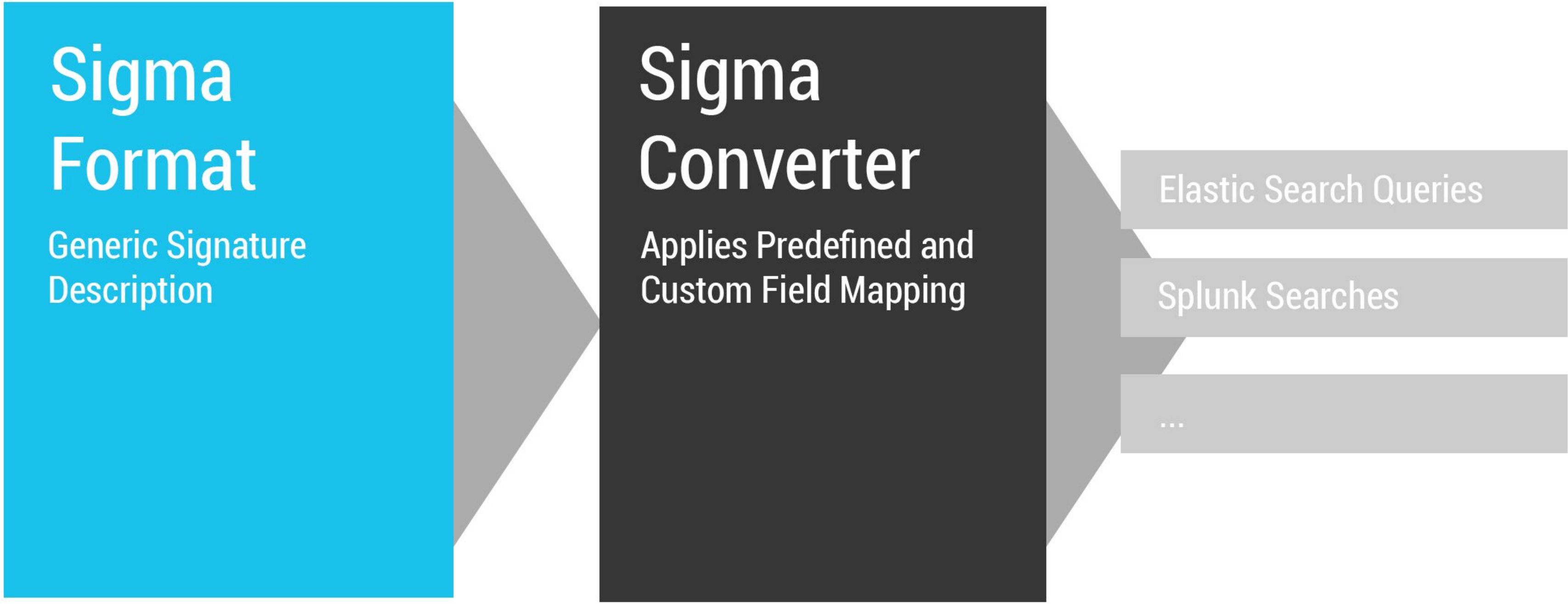
DeTT&CT aims to assist blue teams using ATT&CK to score and compare data log source quality, visibility coverage, detection coverage and threat actor behaviours. All of which can help, in different ways, to get more resilient against attacks targeting your organisation. The DeTT&CT framework consists of a Python tool, YAML administration files, the DeTT&CT Editor and scoring tables for the different aspects.

DeTT&CT

- Why just focus on the attacks?
- The goal of any assessment is to improve blue
- Every pentest report should have detection opportunities
  - But, is this not a given?
- Importance of data sources
- Integration with ATT&CK Navigator
- Gap analysis is the goal



Durable: Sigma



Sigma Format

Generic Signature Description

Sigma Converter

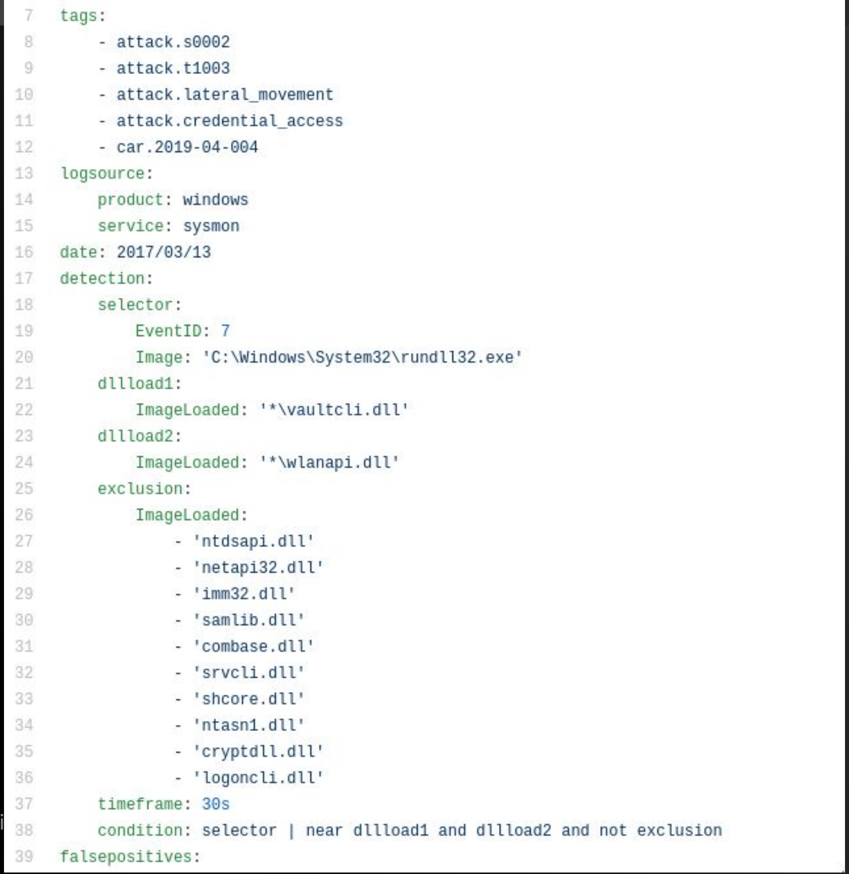
Applies Predefined and Custom Field Mapping

Elastic Search Queries

Splunk Searches

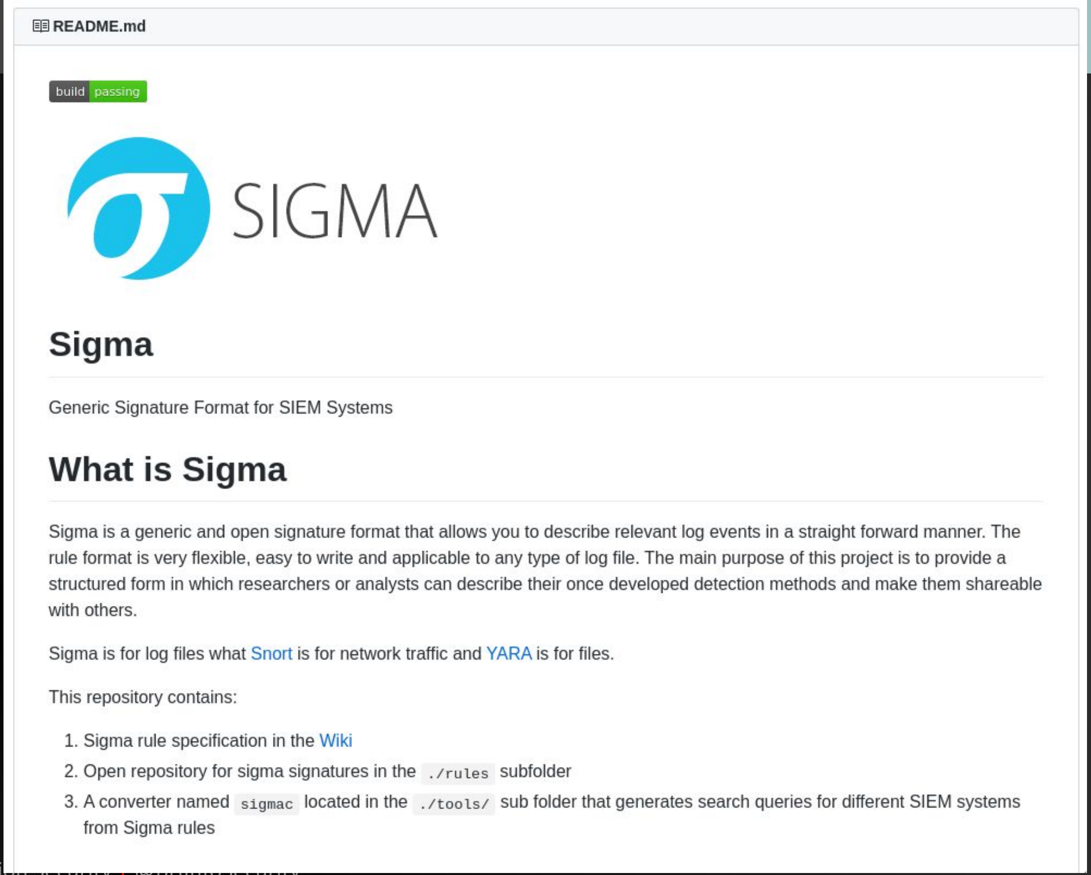
...

Durable: Sigma!



```
tags:
    - attack.s0002
    - attack.t1003
    - attack.lateral_movement
    - attack.credential_access
    - car.2019-04-004
logsource:
    product: windows
    service: sysmon
date: 2017/03/13
detection:
    selector:
        EventID: 7
        Image: 'C:\Windows\System32\rundll32.exe'
    dllload1:
        ImageLoaded: '*\vaultcli.dll'
    dllload2:
        ImageLoaded: '*\wlanapi.dll'
    exclusion:
        ImageLoaded:
            - 'ntdsapi.dll'
            - 'netapi32.dll'
            - 'imm32.dll'
            - 'samlib.dll'
            - 'combase.dll'
            - 'srvcli.dll'
            - 'shcore.dll'
            - 'ntasn1.dll'
            - 'cryptdll.dll'
            - 'logoncli.dll'
    timeframe: 30s
    condition: selector | near dllload1 and dllload2 and not exclusion
falsepositives:
```

Sigma



README.md

build passing

SIGMA

Sigma

Generic Signature Format for SIEM Systems

What is Sigma

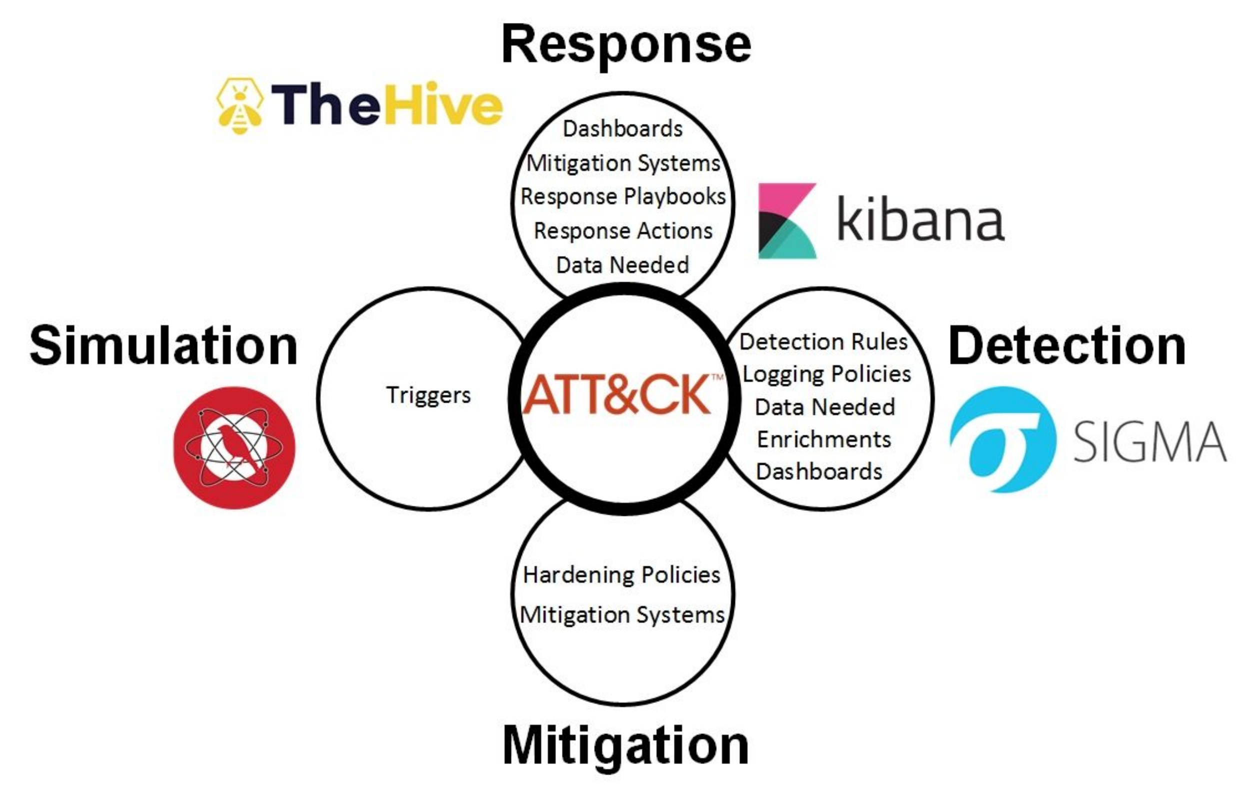
Sigma is a generic and open signature format that allows you to describe relevant log events in a straight forward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.

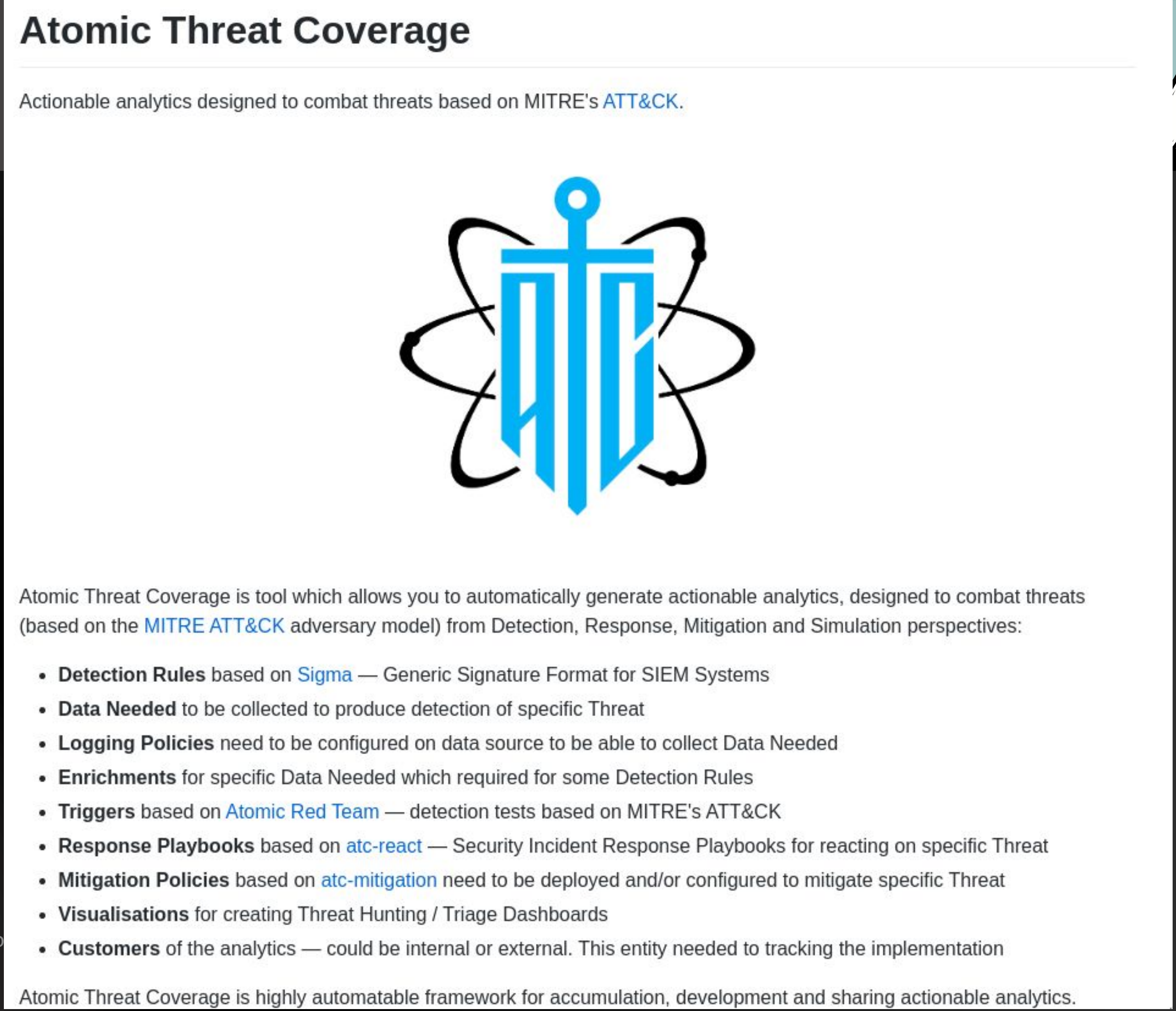
Sigma is for log files what Snort is for network traffic and YARA is for files.

This repository contains:

1. Sigma rule specification in the Wiki
2. Open repository for sigma signatures in the `./rules` subfolder
3. A converter named `sigmac` located in the `./tools/` sub folder that generates search queries for different SIEM systems from Sigma rules

Atomic Threat Coverage





Atomic Threat Coverage

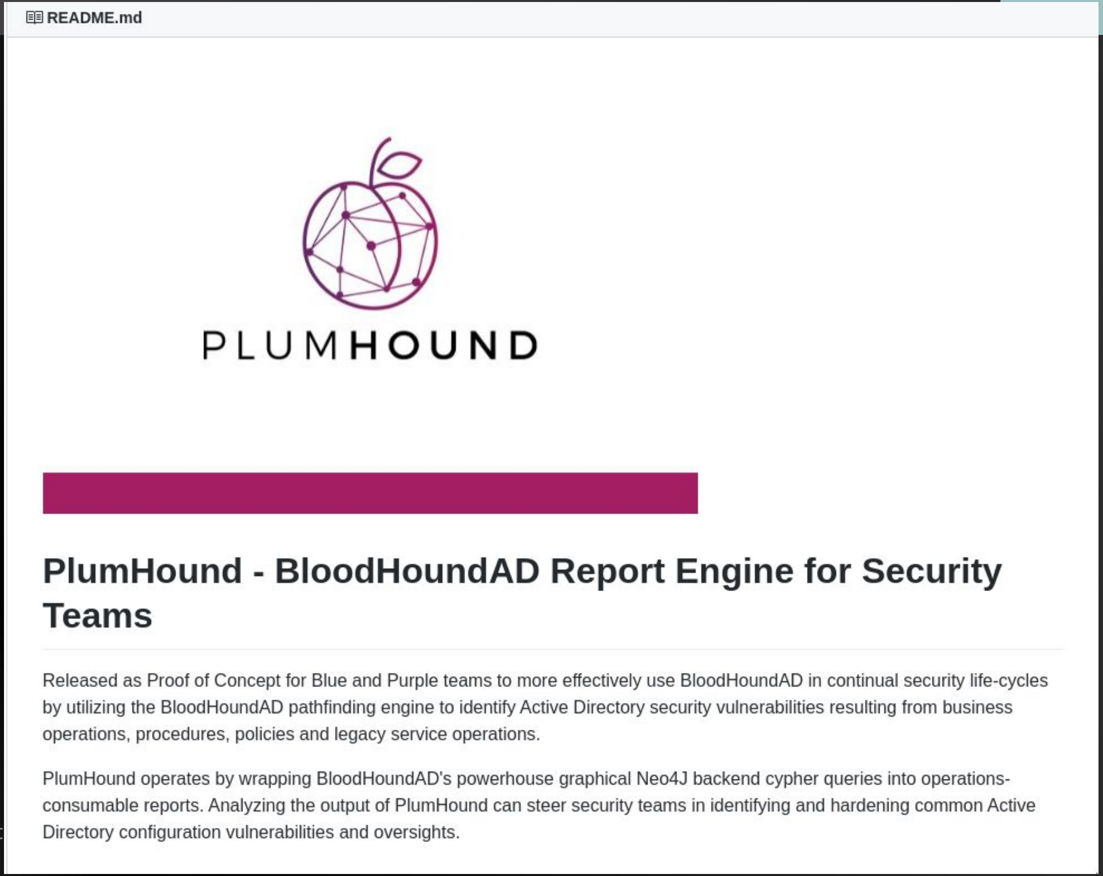
Actionable analytics designed to combat threats based on MITRE's ATT&CK.

Atomic Threat Coverage is tool which allows you to automatically generate actionable analytics, designed to combat threats (based on the MITRE ATT&CK adversary model) from Detection, Response, Mitigation and Simulation perspectives:

- **Detection Rules** based on Sigma — Generic Signature Format for SIEM Systems
- **Data Needed** to be collected to produce detection of specific Threat
- **Logging Policies** need to be configured on data source to be able to collect Data Needed
- **Enrichments** for specific Data Needed which required for some Detection Rules
- **Triggers** based on Atomic Red Team — detection tests based on MITRE's ATT&CK
- **Response Playbooks** based on atc-react — Security Incident Response Playbooks for reacting on specific Threat
- **Mitigation Policies** based on atc-mitigation need to be deployed and/or configured to mitigate specific Threat
- **Visualisations** for creating Threat Hunting / Triage Dashboards
- **Customers** of the analytics — could be internal or external. This entity needed to tracking the implementation

Atomic Threat Coverage is highly automatable framework for accumulation, development and sharing actionable analytics.

PlumHound



README.md

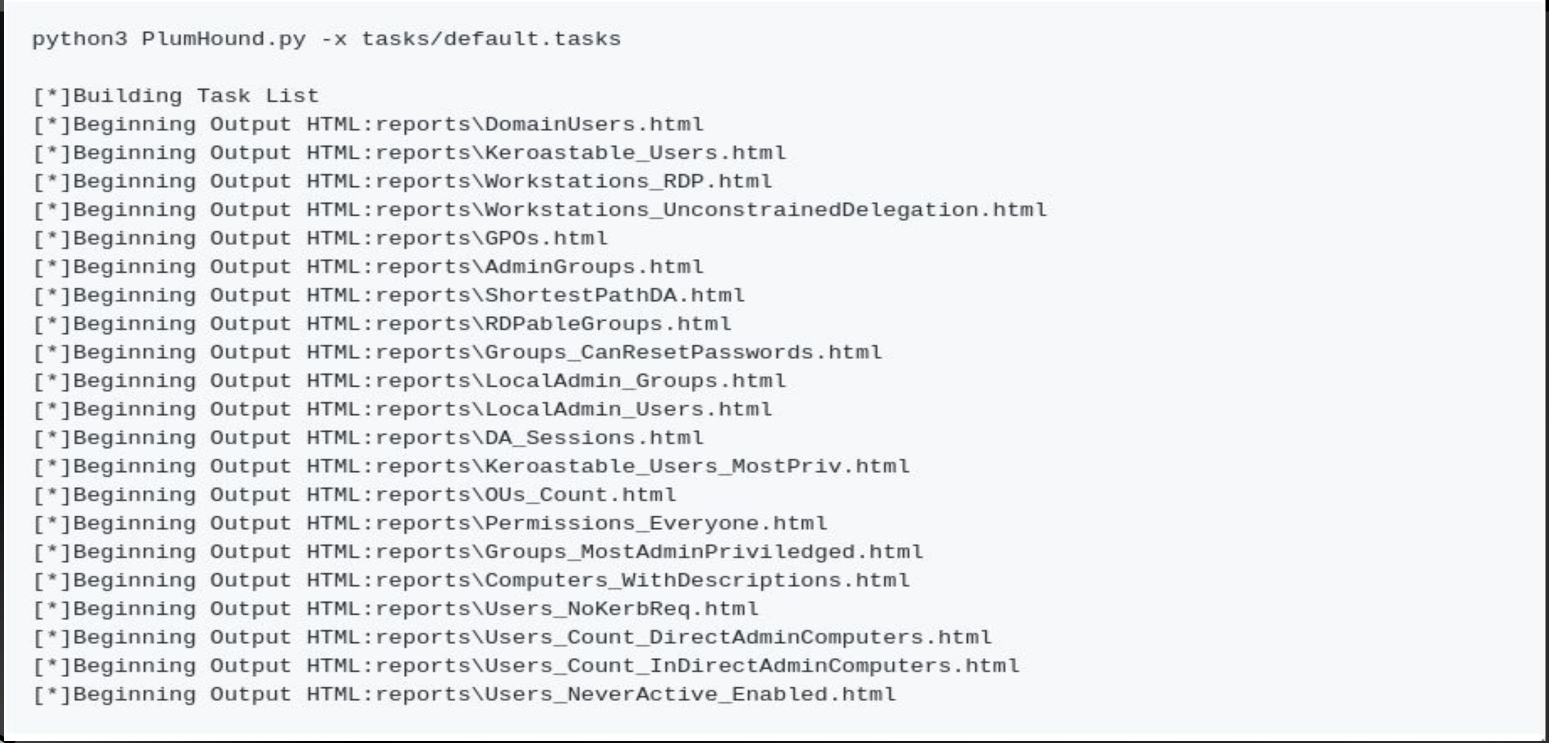
PLUMHOUND

PlumHound - BloodHoundAD Report Engine for Security Teams

Released as Proof of Concept for Blue and Purple teams to more effectively use BloodHoundAD in continual security life-cycles by utilizing the BloodHoundAD pathfinding engine to identify Active Directory security vulnerabilities resulting from business operations, procedures, policies and legacy service operations.

PlumHound operates by wrapping BloodHoundAD's powerhouse graphical Neo4J backend cypher queries into operations-consumable reports. Analyzing the output of PlumHound can steer security teams in identifying and hardening common Active Directory configuration vulnerabilities and oversights.

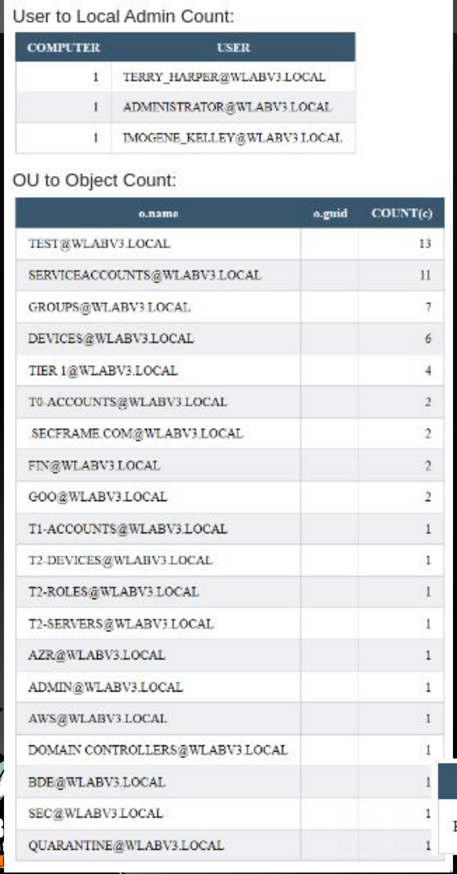
Checks



```
python3 PlumHound.py -x tasks/default.tasks

[*]Building Task List
[*]Beginning Output HTML:reports\DomainUsers.html
[*]Beginning Output HTML:reports\Keroastable_Users.html
[*]Beginning Output HTML:reports\Workstations_RDP.html
[*]Beginning Output HTML:reports\Workstations_UnconstrainedDelegation.html
[*]Beginning Output HTML:reports\GPOs.html
[*]Beginning Output HTML:reports\AdminGroups.html
[*]Beginning Output HTML:reports\ShortestPathDA.html
[*]Beginning Output HTML:reports\RDPableGroups.html
[*]Beginning Output HTML:reports\Groups_CanResetPasswords.html
[*]Beginning Output HTML:reports\LocalAdmin_Groups.html
[*]Beginning Output HTML:reports\LocalAdmin_Users.html
[*]Beginning Output HTML:reports\DA_Sessions.html
[*]Beginning Output HTML:reports\Keroastable_Users_MostPriv.html
[*]Beginning Output HTML:reports\OUs_Count.html
[*]Beginning Output HTML:reports\Permissions_Everyone.html
[*]Beginning Output HTML:reports\Groups_MostAdminPriviledged.html
[*]Beginning Output HTML:reports\Computers_WithDescriptions.html
[*]Beginning Output HTML:reports\Users_NoKerbReq.html
[*]Beginning Output HTML:reports\Users_Count_DirectAdminComputers.html
[*]Beginning Output HTML:reports\Users_Count_InDirectAdminComputers.html
[*]Beginning Output HTML:reports\Users_NeverActive_Enabled.html
```

PlumHound

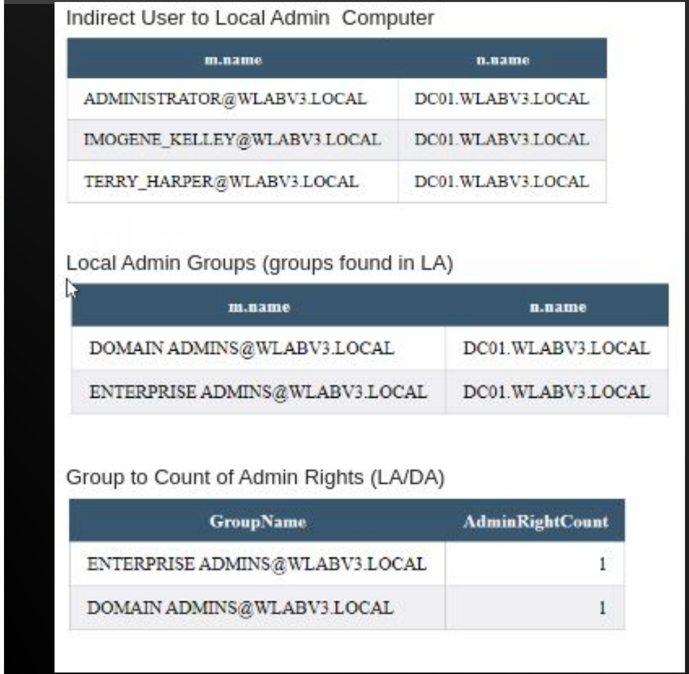


User to Local Admin Count:

COMPUTER	USER
1	TERRY_HARPER@WLABV3.LOCAL
1	ADMINISTRATOR@WLABV3.LOCAL
1	IMOGENE_KELLEY@WLABV3.LOCAL

OU to Object Count:

o.name	o.guid	COUNT(c)
TEST@WLABV3.LOCAL		13
SERVICEACCOUNTS@WLABV3.LOCAL		11
GROUPS@WLABV3.LOCAL		7
DEVICES@WLABV3.LOCAL		6
TIER 1@WLABV3.LOCAL		4
T0-ACCOUNTS@WLABV3.LOCAL		2
SECFRAME.COM@WLABV3.LOCAL		2
FIN@WLABV3.LOCAL		2
GOO@WLABV3.LOCAL		2
T1-ACCOUNTS@WLABV3.LOCAL		1
T2-DEVICES@WLABV3.LOCAL		1
T2-ROLES@WLABV3.LOCAL		1
T2-SERVERS@WLABV3.LOCAL		1
AZR@WLABV3.LOCAL		1
ADMIN@WLABV3.LOCAL		1
AWS@WLABV3.LOCAL		1
DOMAIN CONTROLLERS@WLABV3.LOCAL		1
BDE@WLABV3.LOCAL		1
SEC@WLABV3.LOCAL		1
QUARANTINE@WLABV3.LOCAL		1



Indirect User to Local Admin Computer

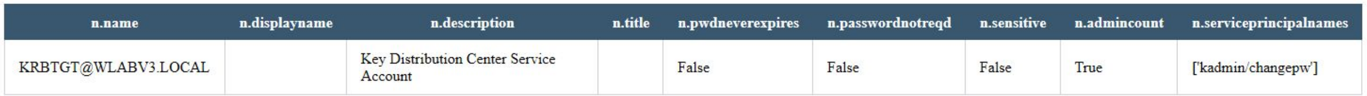
m.name	n.name
ADMINISTRATOR@WLABV3.LOCAL	DC01.WLABV3.LOCAL
IMOGENE_KELLEY@WLABV3.LOCAL	DC01.WLABV3.LOCAL
TERRY_HARPER@WLABV3.LOCAL	DC01.WLABV3.LOCAL

Local Admin Groups (groups found in LA)

m.name	n.name
DOMAIN ADMINS@WLABV3.LOCAL	DC01.WLABV3.LOCAL
ENTERPRISE ADMINS@WLABV3.LOCAL	DC01.WLABV3.LOCAL

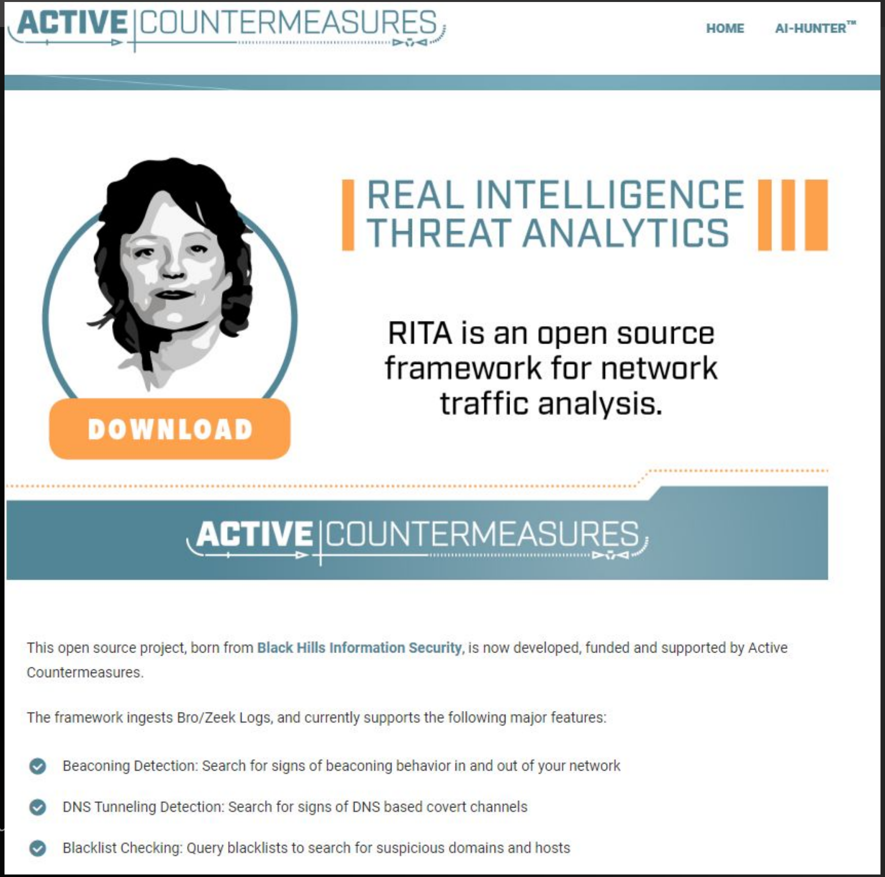
Group to Count of Admin Rights (LA/DA)

GroupName	AdminRightCount
ENTERPRISE ADMINS@WLABV3.LOCAL	1
DOMAIN ADMINS@WLABV3.LOCAL	1



n.name	n.displayname	n.description	n.title	n.pwdneverexpires	n.passwordnotreqd	n.sensitive	n.admincount	n.serviceprincipalnames
KRBTGT@WLABV3.LOCAL		Key Distribution Center Service Account		False	False	False	True	['kadmin/changepw']

RITA



REAL INTELLIGENCE THREAT ANALYTICS

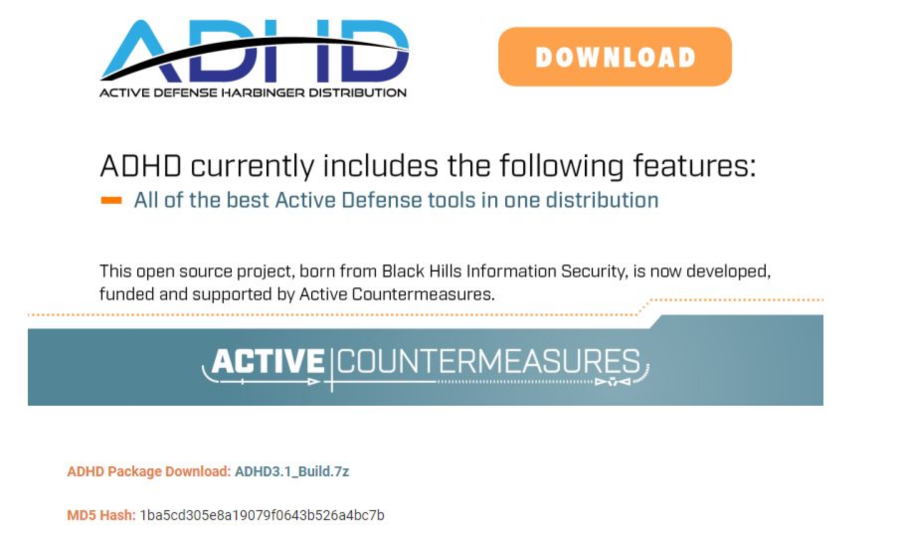
RITA is an open source framework for network traffic analysis.

This open source project, born from **Black Hills Information Security**, is now developed, funded and supported by Active Countermeasures.

The framework ingests Bro/Zeek Logs, and currently supports the following major features:

- ✓ Beaconing Detection: Search for signs of beaconing behavior in and out of your network
- ✓ DNS Tunneling Detection: Search for signs of DNS based covert channels
- ✓ Blacklist Checking: Query blacklists to search for suspicious domains and hosts

A Note on Honeypots



ADHD
ACTIVE DEFENSE HARBINGER DISTRIBUTION

DOWNLOAD

ADHD currently includes the following features:

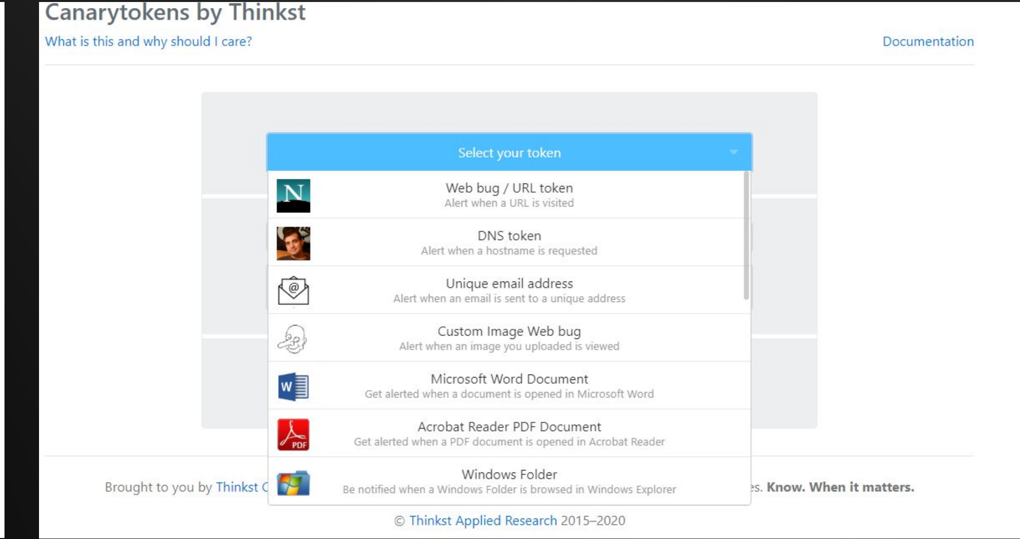
- All of the best Active Defense tools in one distribution

This open source project, born from Black Hills Information Security, is now developed, funded and supported by Active Countermeasures.

ACTIVE | COUNTERMEASURES

ADHD Package Download: ADHD3.1_Build.7z

MD5 Hash: 1ba5cd305e8a19079f0643b526a4bc7b



Canarytokens by Thinkst

What is this and why should I care?

Documentation

Select your token

Web bug / URL token
Alert when a URL is visited

DNS token
Alert when a hostname is requested

Unique email address
Alert when an email is sent to a unique address

Custom Image Web bug
Alert when an image you uploaded is viewed

Microsoft Word Document
Get alerted when a document is opened in Microsoft Word

Acrobat Reader PDF Document
Get alerted when a PDF document is opened in Acrobat Reader

Windows Folder
Be notified when a Windows Folder is browsed in Windows Explorer

Brought to you by Thinkst C

s. Know. When it matters.

© Thinkst Applied Research 2015–2020

Questions?

BLACK HILLS
Information Security
• 2008 •

PENETRATION TESTING

RED TEAMING

THREAT HUNTING

WEBCASTS

OPEN-SOURCE TOOLS

BLOGS

bhis.co

AI HUNTER™

Network Threat Hunting Solution

ANALYZE
Network Traffic

IDENTIFY
Compromised Systems

HUNT
Menacing Threats

- BEACONS MODULE
- LONG CONNECTIONS MODULE
- DEEP DIVE MODULE
- ALERTING

acm.re