RSA®Conference2019
Asia Pacific & Japan

Singapore | 16–18 July | Marina Bay Sands

BETTER.

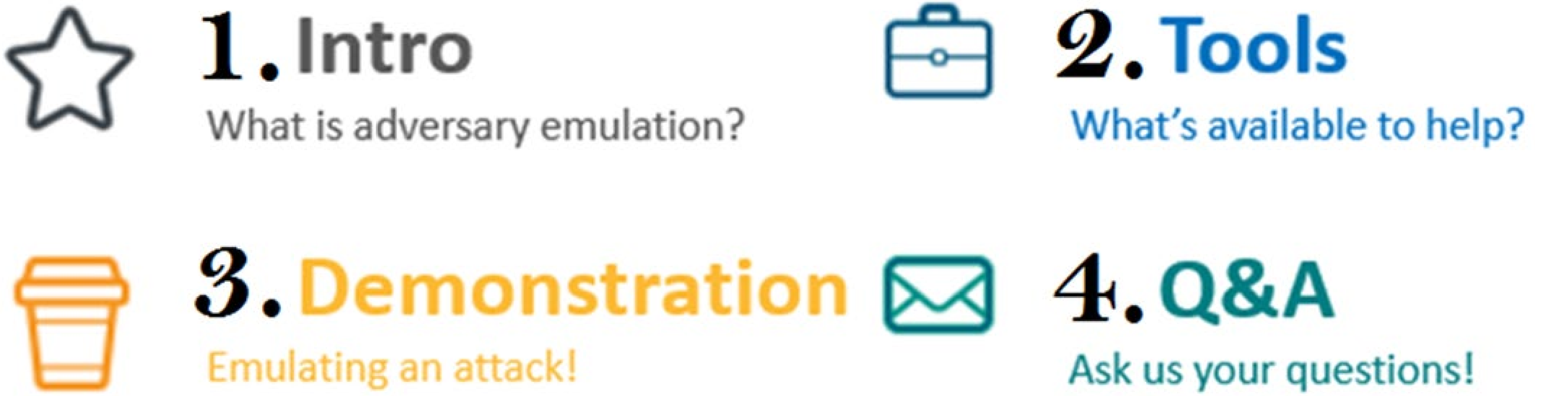
SESSION ID: AIR-R02

Live Adversary Simulation Red and Blue Team Tactics

Stephen Sims

Security Researcher / Fellow / Curriculum Lead
SANS Institute
@Steph3nSims

Agenda



1. **Intro**
   What is adversary emulation?
2. **Tools**
   What's available to help?
3. **Demonstration**
   Emulating an attack!
4. **Q&A**
   Ask us your questions!

RSAConference2019
Asia Pacific & Japan

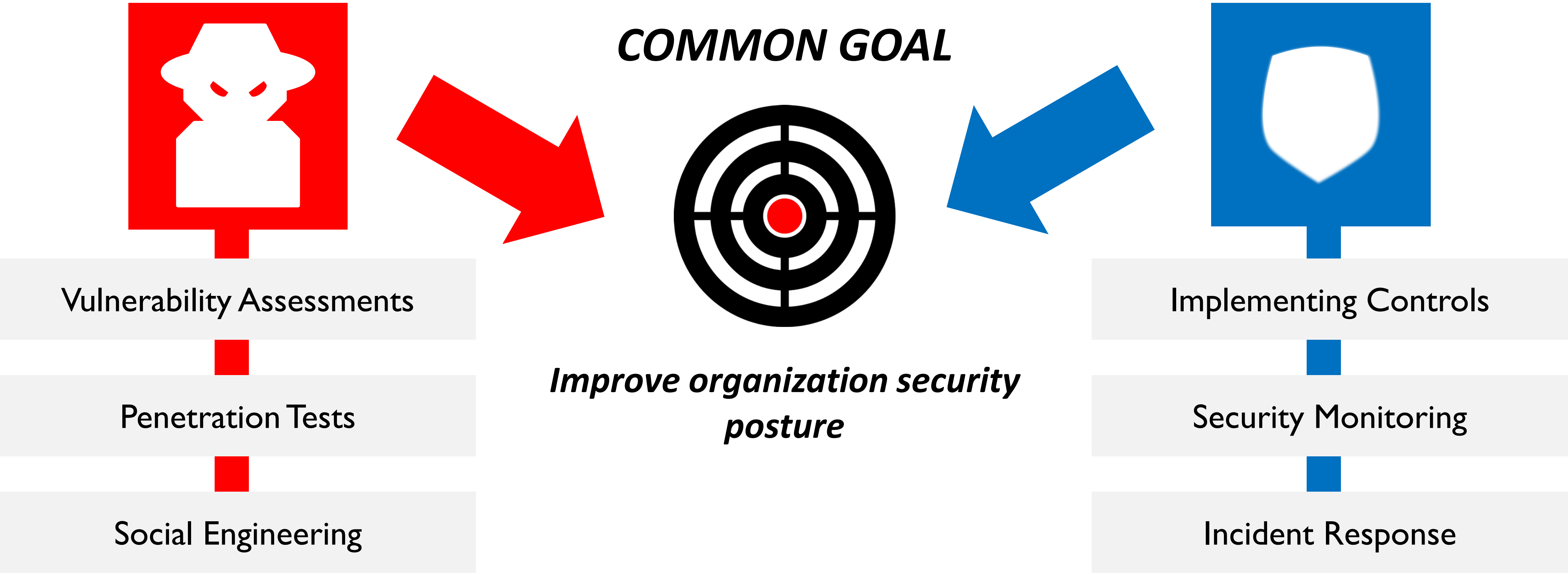
Intro

What is Adversary Emulation

What is “Red Team” & “Blue Team”?

“Offense”

“Defense”



COMMON GOAL

Vulnerability Assessments

Penetration Tests

Social Engineering

Implementing Controls

Security Monitoring

Incident Response

Improve organization security posture

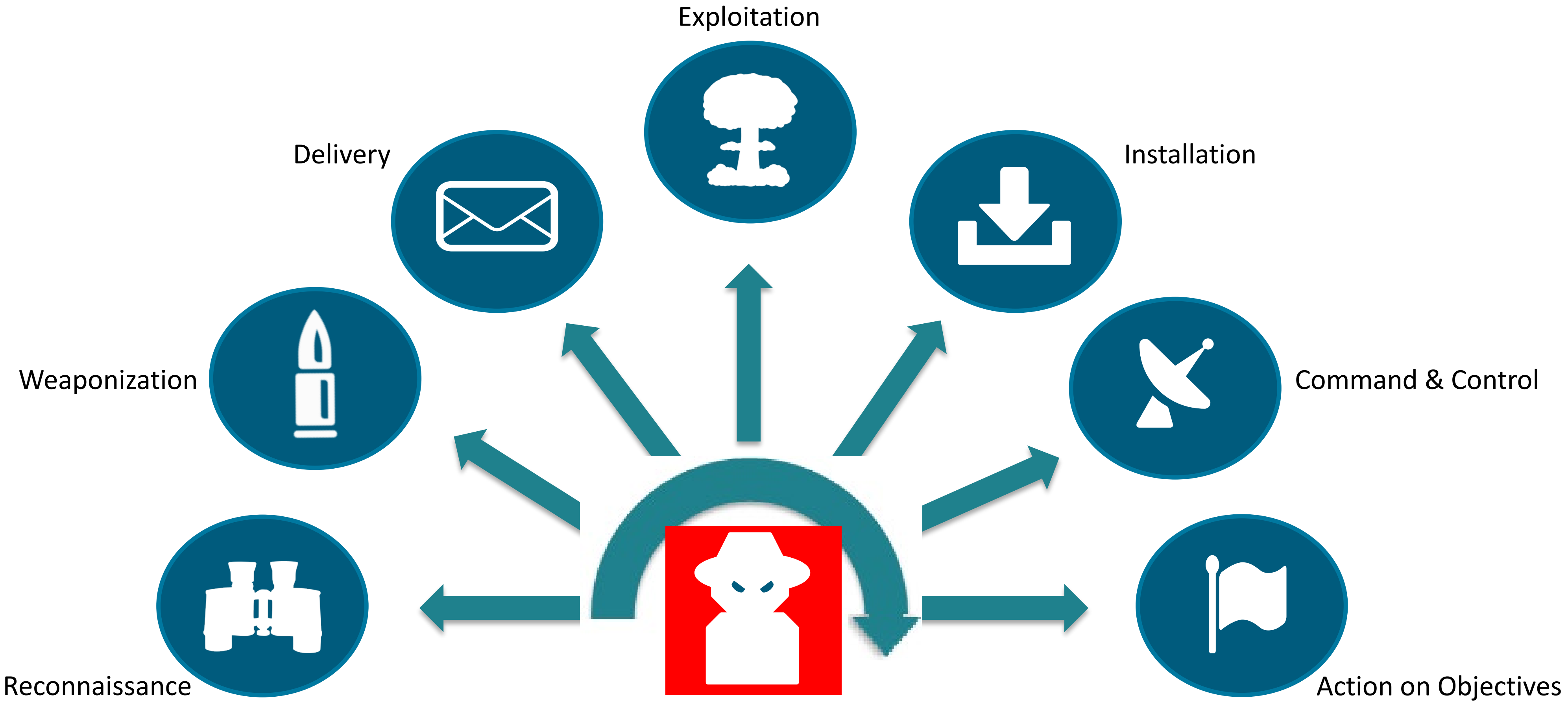
What is “Adversary Emulation”?

Adversary emulation is an activity where security experts emulate how an adversary operates. The ultimate goal of course is to improve how resilient the organization is versus these adversary techniques. Both red and purple teaming can be considered as adversary emulation.

TTP

Adversary activities are described using **TTPs (Tactics, Techniques & Procedures**), possibly described using a **kill chain**. TTPs are not as concrete as for example IOCs, but they describe how the adversary operates at a higher level. Adversary emulation should be based on TTPs. As such, a traditional vulnerability scan or internal penetration test that is not based on TTPs should not be considered adversary emulation.

Adversary Emulation



Why do Adversary Emulation?

Understand your current exposure to a **realistic**, **relevant**, threat

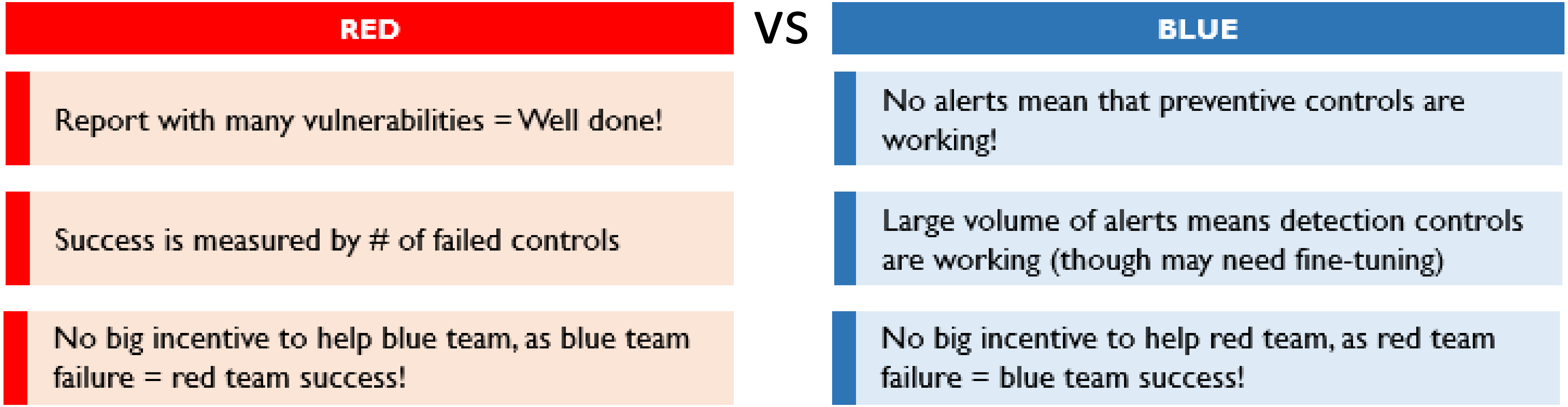
On top of vulnerability identification, assess **detection capability** as well

Also includes testing of the **human reaction** as well

Repeatable, structured process that provides **key areas for improvement**

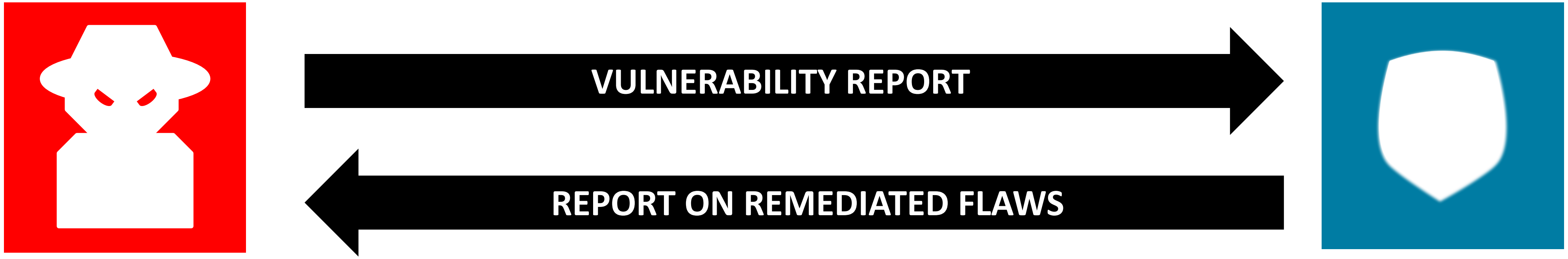
Consider Purple Teaming

- Red and Blue teams typically report within different silos or hierarchies, hurting communication



RED	VS	BLUE
Report with many vulnerabilities = Well done!		No alerts mean that preventive controls are working!
Success is measured by # of failed controls		Large volume of alerts means detection controls are working (though may need fine-tuning)
No big incentive to help blue team, as blue team failure = red team success!		No big incentive to help red team, as red team failure = blue team success!

Feedback Loop



VULNERABILITY REPORT

REPORT ON REMEDIATED FLAWS

- Information should flow in both directions
  - Offense informs the defense about the TTPs of bad actors
  - Defense informs the offense about their controls and monitoring
  - Offense informs the defense about their techniques
  - Defense informs the offense as to how they respond to incidents

Prerequisites for Purple Teaming

If you’re not looking, you can’t really purple team...

We will walk through the kill chain and focus on a variety of different security controls that can help stop (advanced) adversaries in their attempts to penetrate your environment. We should however understand that a “prevent-only” approach is not sufficient, especially when dealing with targeted attacks.

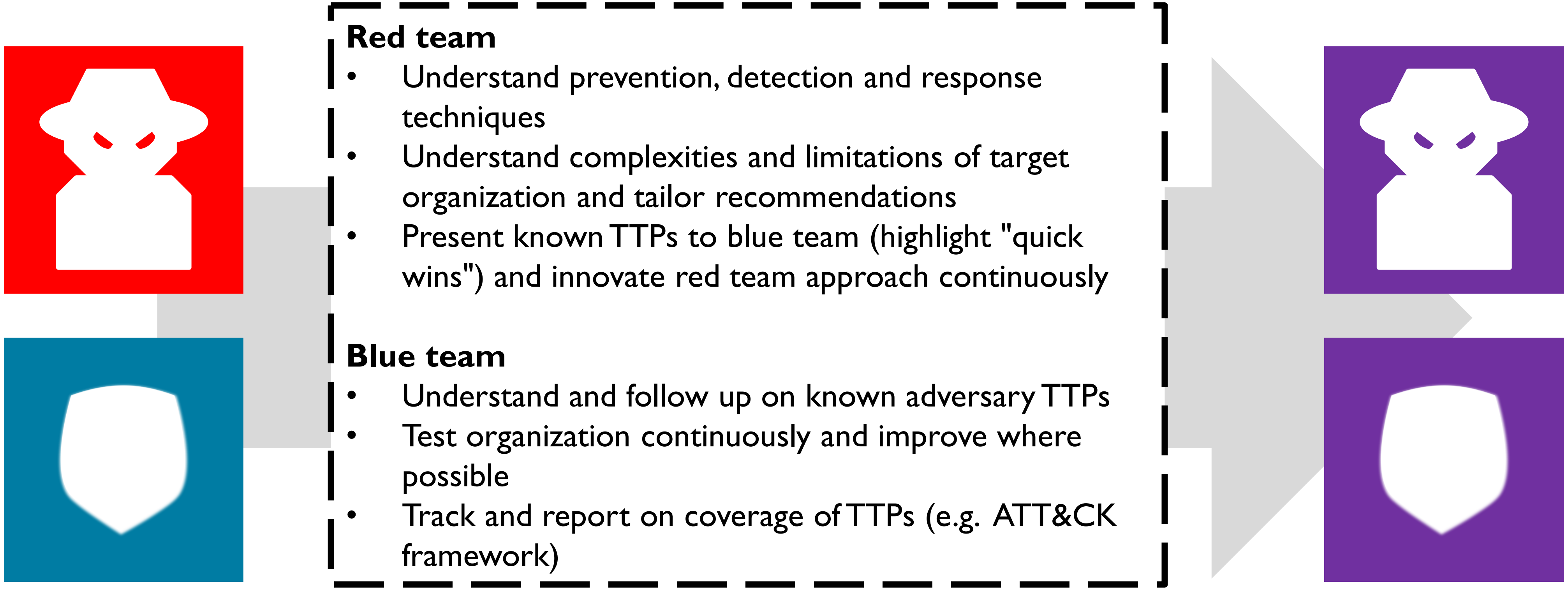
So, what do we require for a proper detection capability?

- A central logging platform that can parse, index and visualize collected information
- Network device logs, key focus areas include DNS, web proxy, firewall, IDS ...
- Endpoint (workstation & server) visibility using real-time log and periodic data collection
- FPC — Optionally, a full packet capture solution that acts as a “flight recorder” for egress & ingress traffic

Depending on your environment, some log sources might be more important than others!

How to Approach This?

Let's make blue more "red" and make "red" more blue:



Red team

- Understand prevention, detection and response techniques
- Understand complexities and limitations of target organization and tailor recommendations
- Present known TTPs to blue team (highlight "quick wins") and innovate red team approach continuously

Blue team

- Understand and follow up on known adversary TTPs
- Test organization continuously and improve where possible
- Track and report on coverage of TTPs (e.g. ATT&CK framework)

So how do we practically do this? What about our yearly red team?

Does this mean "Purple" is better than "Red"? The answer is not that simple. ☺ Depending on your objectives, either could offer value. Here's an idea for a setup:

RED

Organize a yearly **red team to assess** the actual state of security in the organization. Feedback only after the exercise ends, as the exercise is typically meant to be stealth (realistic adversary emulation)…
VALUE: Periodic assessment of organization resilience

PURPL
E

Perform continuous **purple teaming to improve** the state of security in the organization. Blue team members simulate focused attack techniques as part of their operations to immediately test effectiveness of detection and prevention controls.
VALUE: Continuous improvement of organization resilience

Demonstration

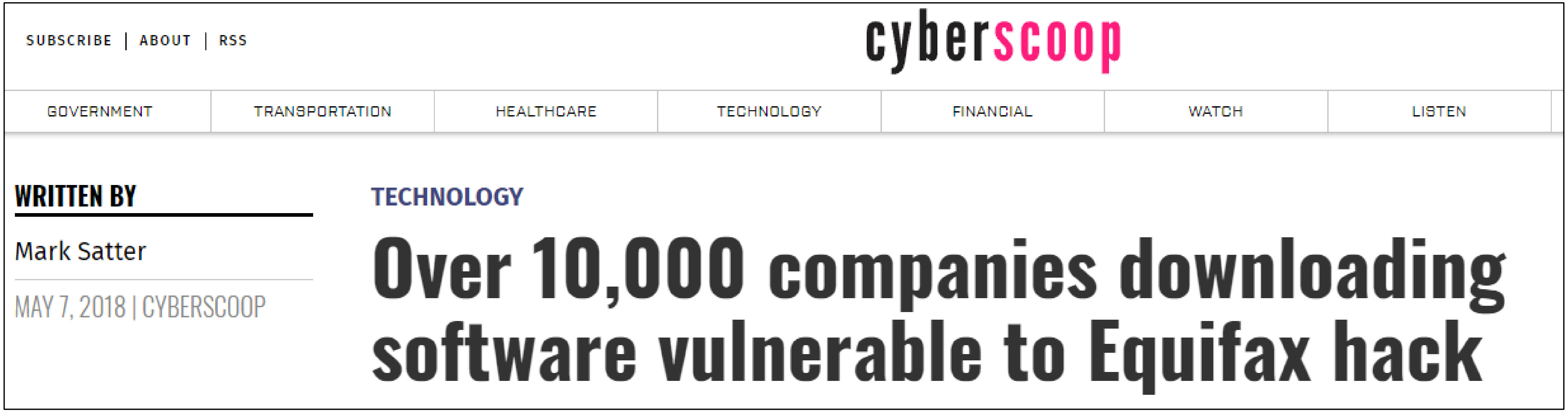
- In 2017, a well-known organization fell victim to an attack against a known Apache Struts2 vulnerability
- Regardless of the lack of patching, the adversarial actions performed were all recorded in the logs…
- Let’s see a demo!

Struts^{2}

What failed?

- A lack of asset or software inventory (Critical Controls #1 & #2)
- A lack of proper patch management
- A lack of log management
- A likely flat network
- How does this map back to the various APT-Lifecycles available?

…and it continues



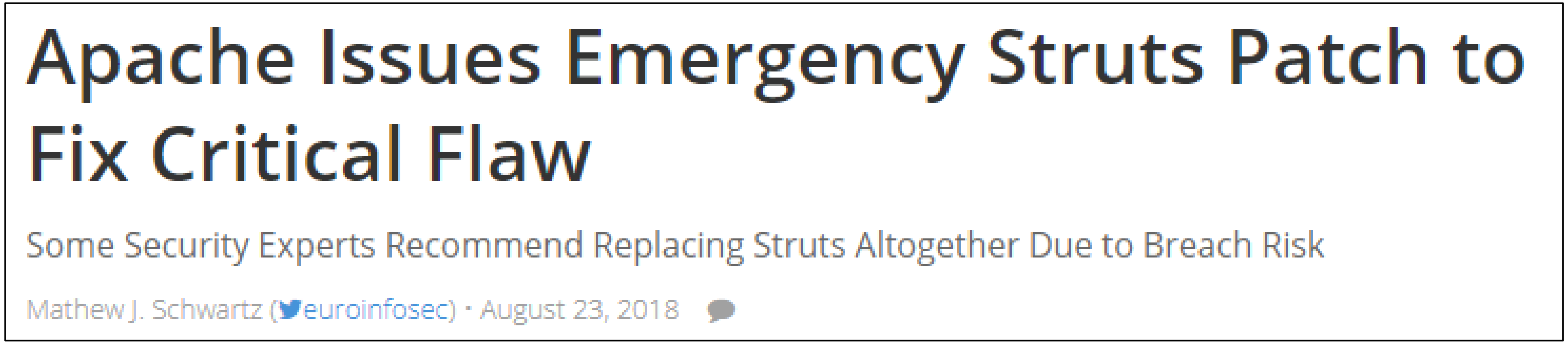
WRITTEN BY

Mark Satter

MAY 7, 2018 | CYBERSCOOP

TECHNOLOGY

Over 10,000 companies downloading software vulnerable to Equifax hack



Apache Issues Emergency Struts Patch to Fix Critical Flaw

Some Security Experts Recommend Replacing Struts Altogether Due to Breach Risk

Mathew J. Schwartz (euroinfosec) • August 23, 2018

RSA®Conference2019
Asia Pacific & Japan

Tools

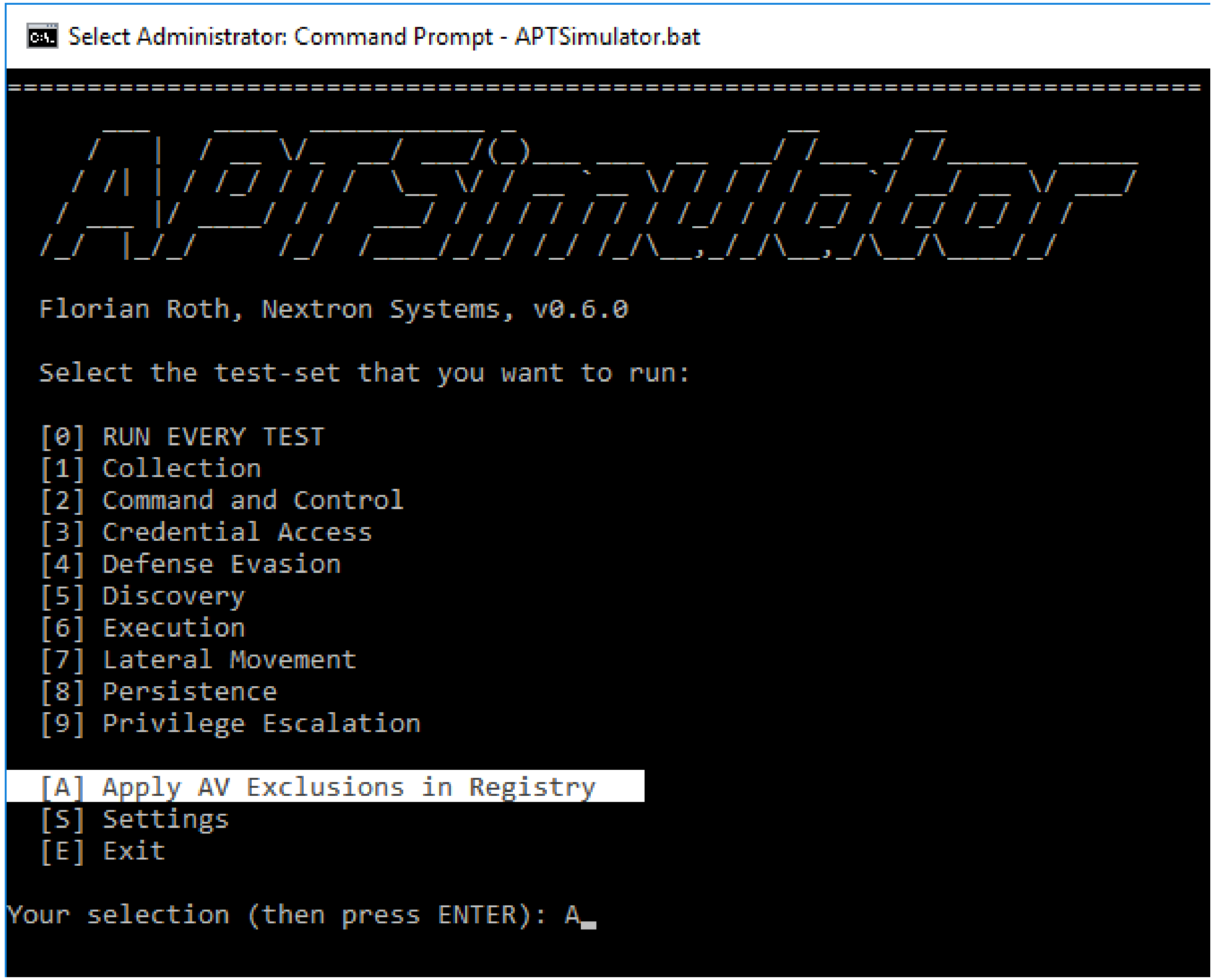
What’s Available to Help?

Typical “Pen Test” and “Red Team” Tools

Metasploit is an exploitation framework used by virtually all penetration testers. It has both a free community edition and a commercial edition available. It’s main focus is on “standardization” of exploit development and usage.

Empire is primarily a post-exploitation tool. It has both Windows support (using a pure PowerShell2.0 agent) and Linux / OS X support (using a pure Python 2.6/2.7 agent). It is the result of the merger of PowerShell Empire and Python EmPyre!

APTSimulator

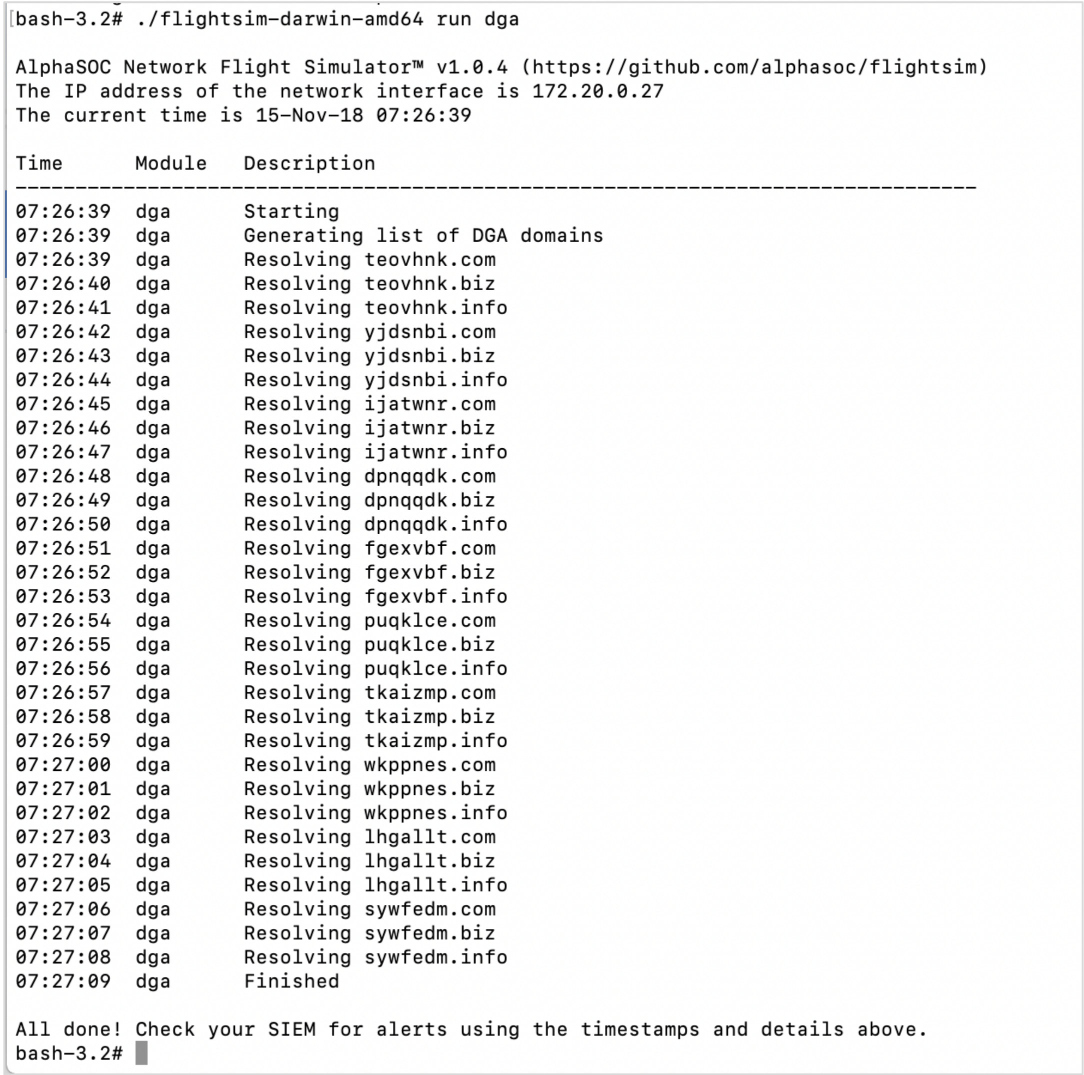


```
==========================================================================

  Florian Roth, Nextron Systems, v0.6.0

  Select the test-set that you want to run:

  [0] RUN EVERY TEST
  [1] Collection
  [2] Command and Control
  [3] Credential Access
  [4] Defense Evasion
  [5] Discovery
  [6] Execution
  [7] Lateral Movement
  [8] Persistence
  [9] Privilege Escalation

  [A] Apply AV Exclusions in Registry
  [S] Settings
  [E] Exit

Your selection (then press ENTER): A_
```

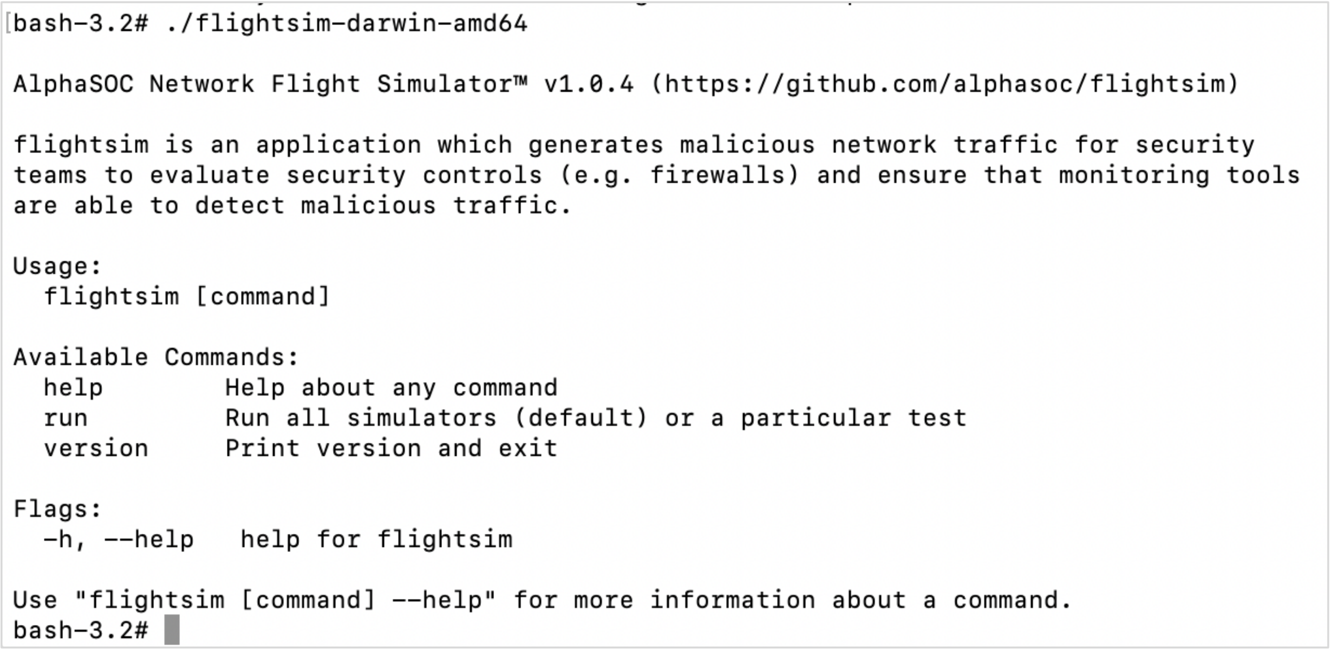
APTSimulator is a Windows-based tool that makes a system look like it was victim of a targeted attack. Key focus is thus on the endpoint)

It supports a wide variety of the ATT&CK tactics, as described in the screenshot to the left.

FlightSim

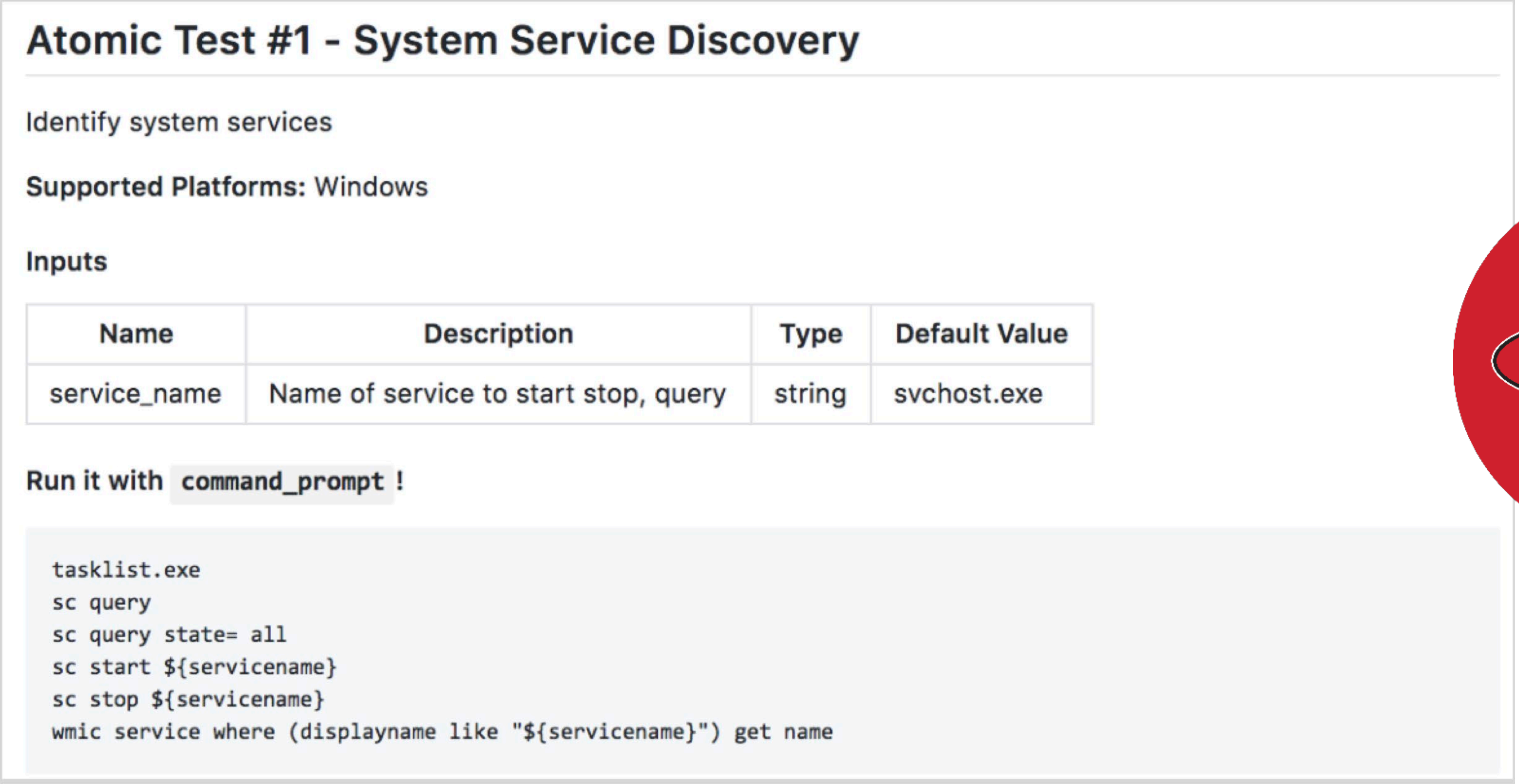


```
bash-3.2# ./flightsim-darwin-amd64 run dga

AlphaSOC Network Flight Simulator™ v1.0.4 (https://github.com/alphasoc/flightsim)
The IP address of the network interface is 172.20.0.27
The current time is 15-Nov-18 07:26:39

Time      Module   Description
--------------------------------------------------------------------------------
07:26:39  dga      Starting
07:26:39  dga      Generating list of DGA domains
07:26:39  dga      Resolving teovhnk.com
07:26:40  dga      Resolving teovhnk.biz
07:26:41  dga      Resolving teovhnk.info
07:26:42  dga      Resolving yjdsnbi.com
07:26:43  dga      Resolving yjdsnbi.biz
07:26:44  dga      Resolving yjdsnbi.info
07:26:45  dga      Resolving ijatwnr.com
07:26:46  dga      Resolving ijatwnr.biz
07:26:47  dga      Resolving ijatwnr.info
07:26:48  dga      Resolving dpnqqdk.com
07:26:49  dga      Resolving dpnqqdk.biz
07:26:50  dga      Resolving dpnqqdk.info
07:26:51  dga      Resolving fgexvbf.com
07:26:52  dga      Resolving fgexvbf.biz
07:26:53  dga      Resolving fgexvbf.info
07:26:54  dga      Resolving puqklce.com
07:26:55  dga      Resolving puqklce.biz
07:26:56  dga      Resolving puqklce.info
07:26:57  dga      Resolving tkaizmp.com
07:26:58  dga      Resolving tkaizmp.biz
07:26:59  dga      Resolving tkaizmp.info
07:27:00  dga      Resolving wkppnes.com
07:27:01  dga      Resolving wkppnes.biz
07:27:02  dga      Resolving wkppnes.info
07:27:03  dga      Resolving lhgallt.com
07:27:04  dga      Resolving lhgallt.biz
07:27:05  dga      Resolving lhgallt.info
07:27:06  dga      Resolving sywfedm.com
07:27:07  dga      Resolving sywfedm.biz
07:27:08  dga      Resolving sywfedm.info
07:27:09  dga      Finished

All done! Check your SIEM for alerts using the timestamps and details above.
bash-3.2#
```



```
bash-3.2# ./flightsim-darwin-amd64

AlphaSOC Network Flight Simulator™ v1.0.4 (https://github.com/alphasoc/flightsim)

flightsim is an application which generates malicious network traffic for security
teams to evaluate security controls (e.g. firewalls) and ensure that monitoring tools
are able to detect malicious traffic.

Usage:
  flightsim [command]

Available Commands:
  help        Help about any command
  run         Run all simulators (default) or a particular test
  version     Print version and exit

Flags:
  -h, --help   help for flightsim

Use "flightsim [command] --help" for more information about a command.
bash-3.2#
```

Atomic Red Team



Atomic Test #1 - System Service Discovery

Identify system services

Supported Platforms: Windows

Inputs

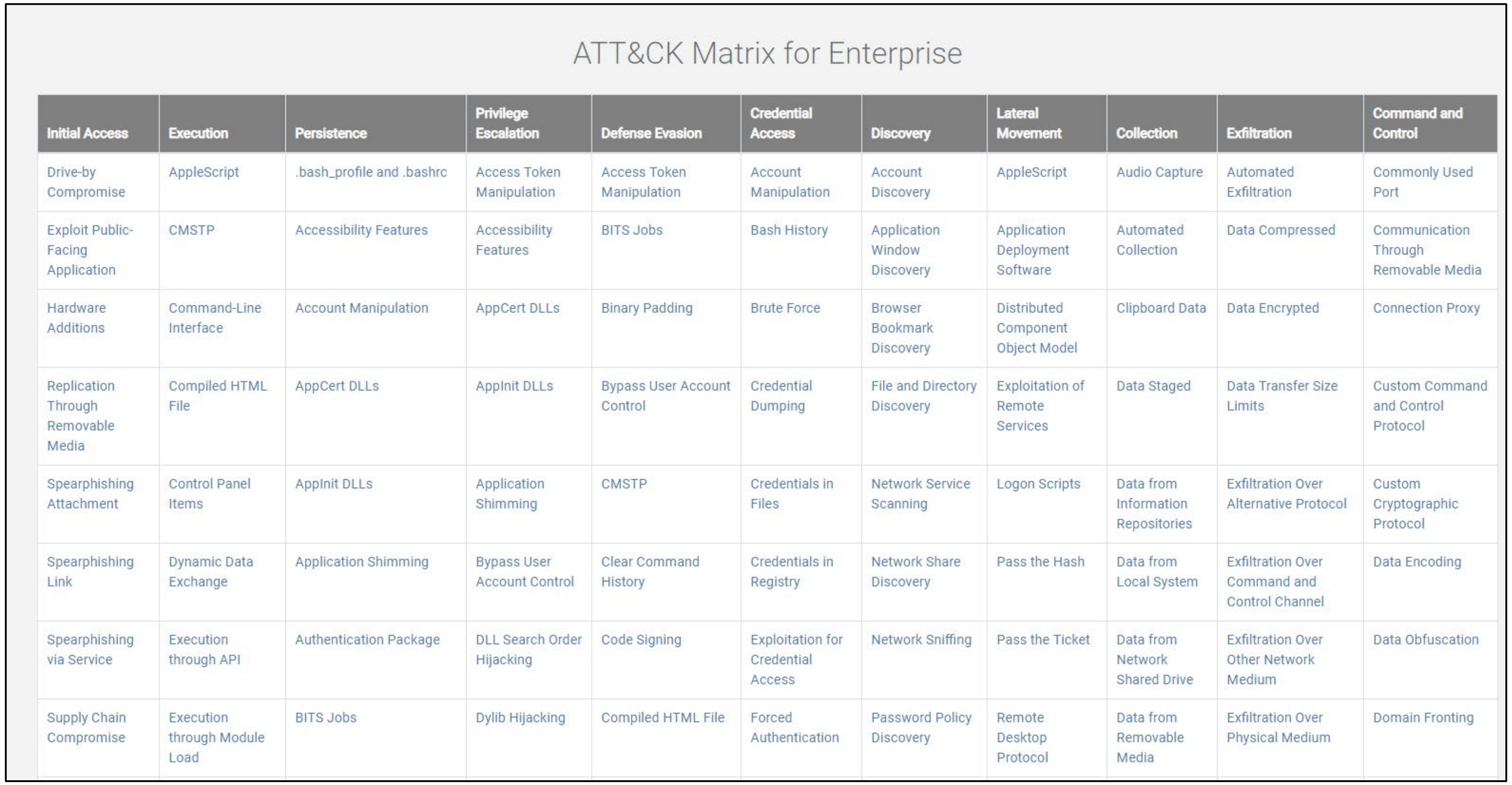
Name	Description	Type	Default Value
service_name	Name of service to start stop, query	string	svchost.exe

Run it with `command_prompt` !

```
tasklist.exe
sc query
sc query state= all
sc start ${servicename}
sc stop ${servicename}
wmic service where (displayname like "${servicename}") get name
```

MITRE ATT&CK

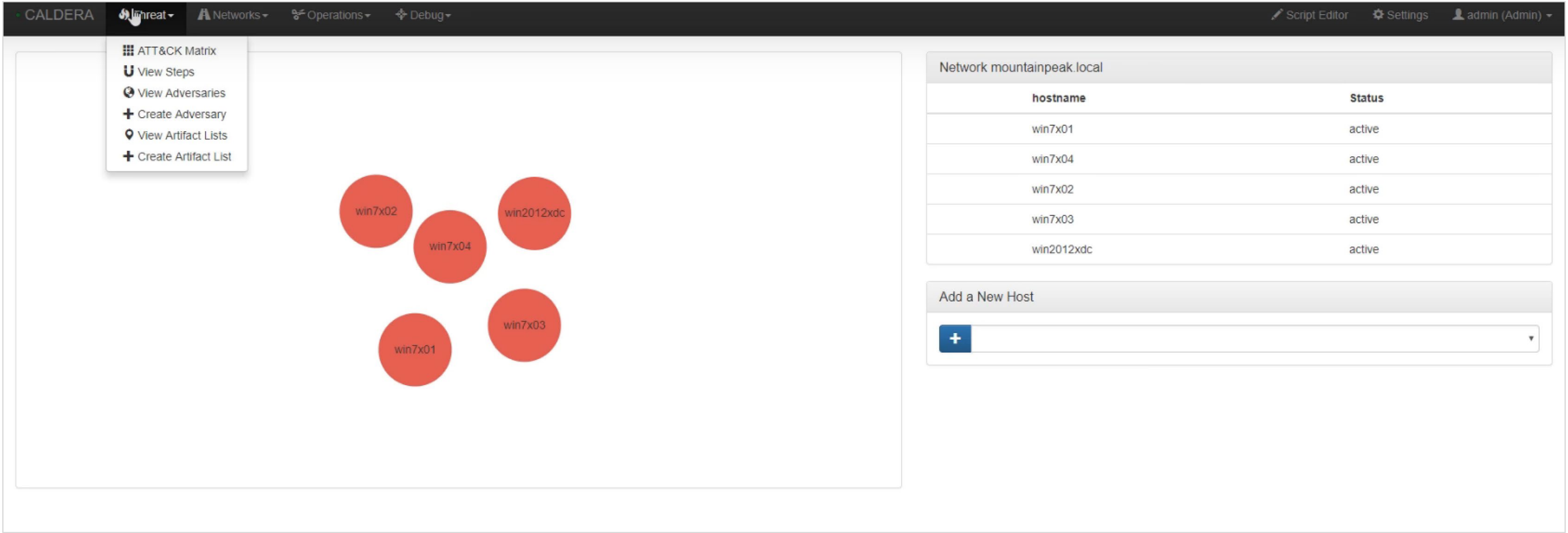
- MITRE ATT&CK "…is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations."



ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting

Caldera

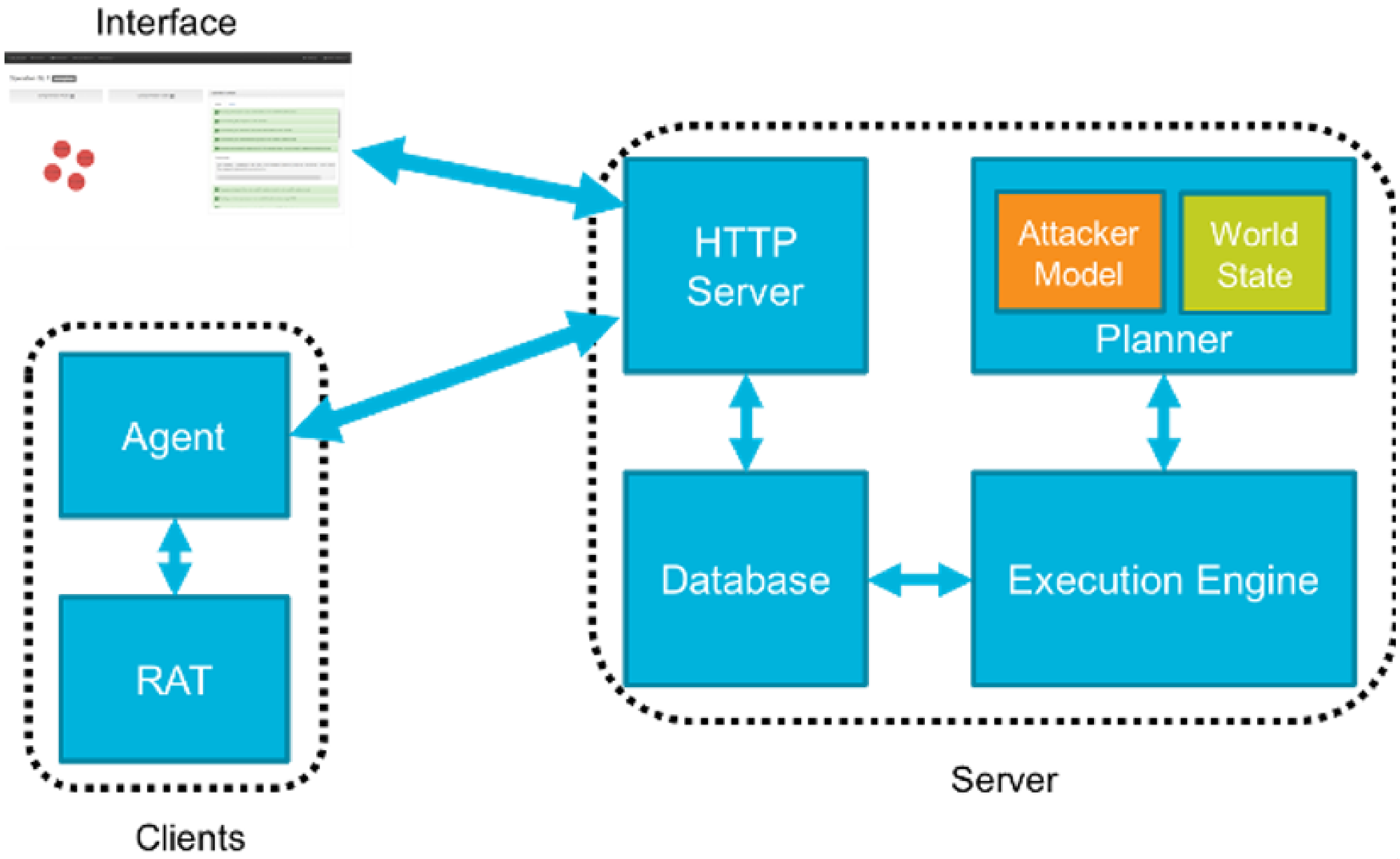


Network mountainpeak.local

hostname	Status
win7x01	active
win7x04	active
win7x02	active
win7x03	active
win2012xdc	active

SANS

Caldera – Architecture

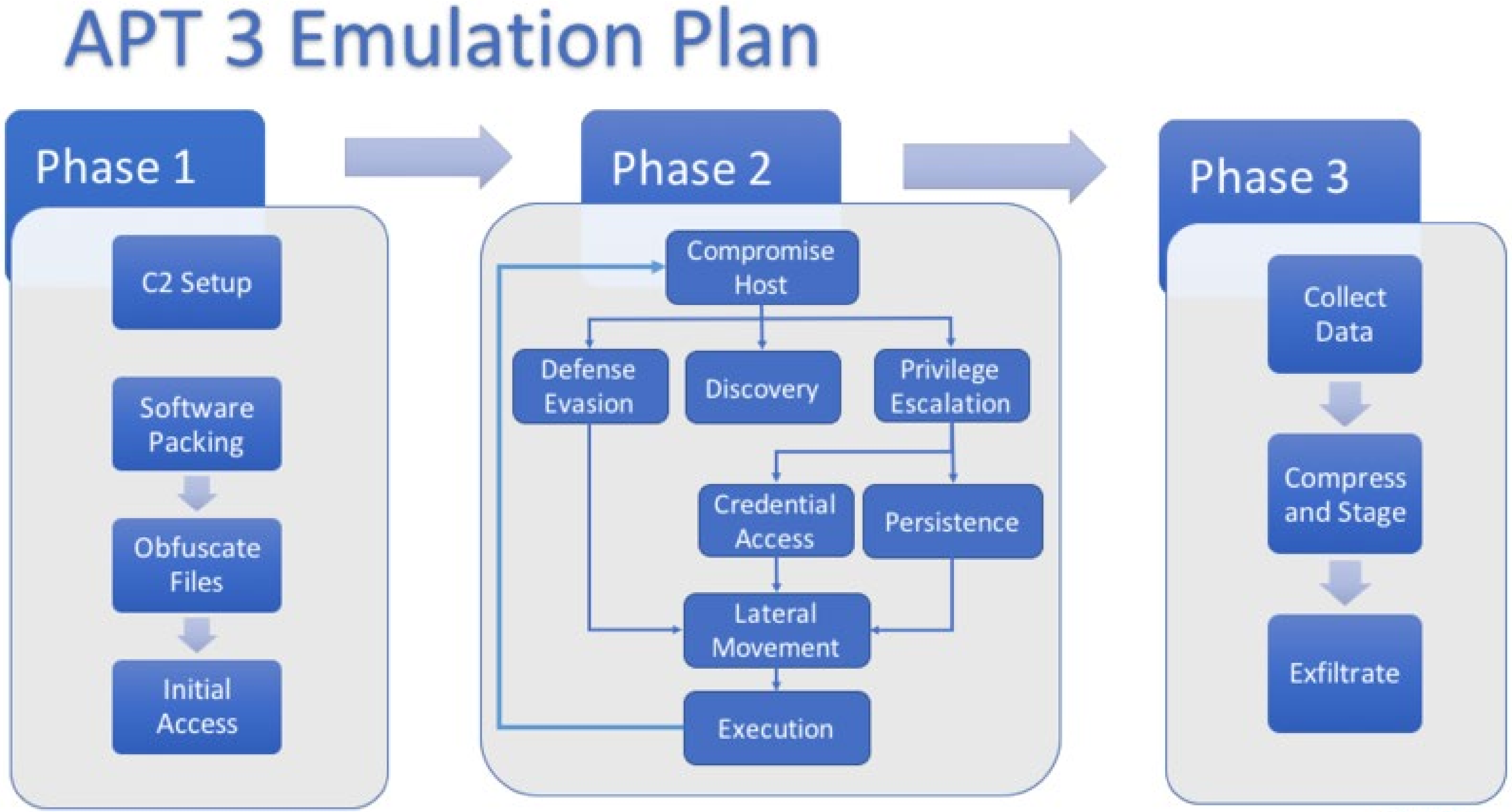


Adversary Emulation Plans

Applying MITRE ATT&CK

Prototype documents of what can be done with publicly available threat reports and ATT&CK

Allow defenders to more effectively test their networks and defenses by enabling red teams to more actively model adversary behavior.



APT 3 Emulation Plan

Phase 1

C2 Setup

Software Packing

Obfuscate Files

Initial Access

Phase 2

Compromise Host

Defense Evasion

Discovery

Privilege Escalation

Credential Access

Persistence

Lateral Movement

Execution

Phase 3

Collect Data

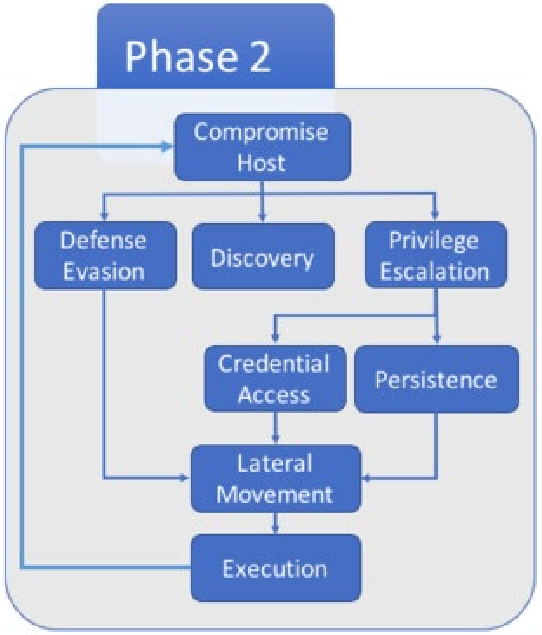
Compress and Stage

Exfiltrate

Approved for Public Release; Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved

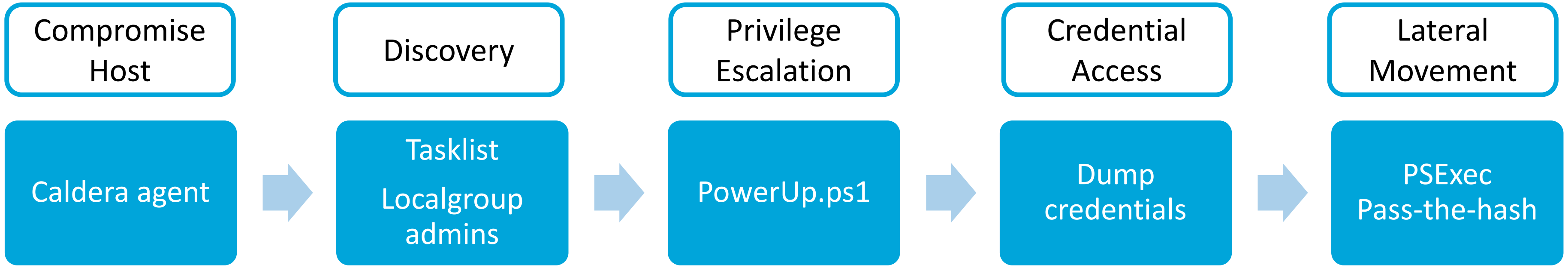
MITRE

Adversary Emulation with Caldera



CALDERA is focused on adversary emulation "post compromise".

As such, CALDERA assumes that an adversary already has an initial foothold on a network.



Commercial Adversary Emulation Tools

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

SCYTHE

ATTACKIQ

SafeBreach

CYMULATE
BREACH & ATTACK SIMULATION

Demonstration

Emulating an Attack Using Caldera!

How to Apply Today’s Subject Matter

- What to take away from this presentation
  - We need to ensure that our “blue” and “red” teams are communicating
  - Validate that we are logging the correct events and information
  - We must also validate that this information is making its way down our pipeline and onto a SOC dashboard
  - Adversary emulation can greatly improve your chances of preventing and detecting a breach

RSA®Conference2019
Asia Pacific & Japan

Thanks!

Stephen Sims

@Steph3nSims