

#FIRSTCON24



# A Recipe for Improving SecOps Detections

Take Three Security Controls,  
Add a Tablespoon of Threat  
Intelligence and Let it Rise

John Stoner (Google Cloud, US)

# #whoami > John Stoner

SIEM/SecOps space since 2004

- SecOps, Threat Hunting, Detection Engineering, Threat Intelligence

Focus on content development

Build adversary emulations around APT actors

Blog - New to Google SecOps

Enjoy Alt80s "sad-timey" music



Principal Security Strategist  
Google Cloud  
@stonerpsu

# At Inception...

Organizations often start with a set of logs/events

Good intentions to detect badness

Maybe a few use cases



# Over Time, Things Change

Organizations collect more

Good intentions to detect badness

Upkeep of those initial detection use cases and existing rules

Probably want to add new detection use cases and rules

# Can't We Just Keep Adding Use Cases and Rules and Move Along?

Investment from legacy tech – Detections from 5 years and perhaps 2 SIEMs ago

Do the use cases align to my tools?

Are some of those use cases and rules built based on the strengths (or weaknesses) of the previous technology?

Do those use cases still apply to my business processes and risk tolerance?

# Can I Just (Buy | Download) My Use Cases/Rules?

Loads of detection rules exist in the public domain

Businesses are built around building and selling detections

Do they apply to our organization?

- Align with our tooling?
- Align with our risk posture?
- Align to the threats we face?

Use these resources as enablers

# Agenda

Approaches to Emulation

Considerations When Crafting Your Emulation

Building Detections

# Adversary Simulation v Emulation

## Simulation

- Focus on evaluating defenses against general attack patterns & behaviors
- Identify potential vulnerabilities and weaknesses that could be exploited
- Less focused on specific adversaries

## Emulation

- Mimic specific TTPs
- Attempt to replicate the attack lifecycle of an adversary



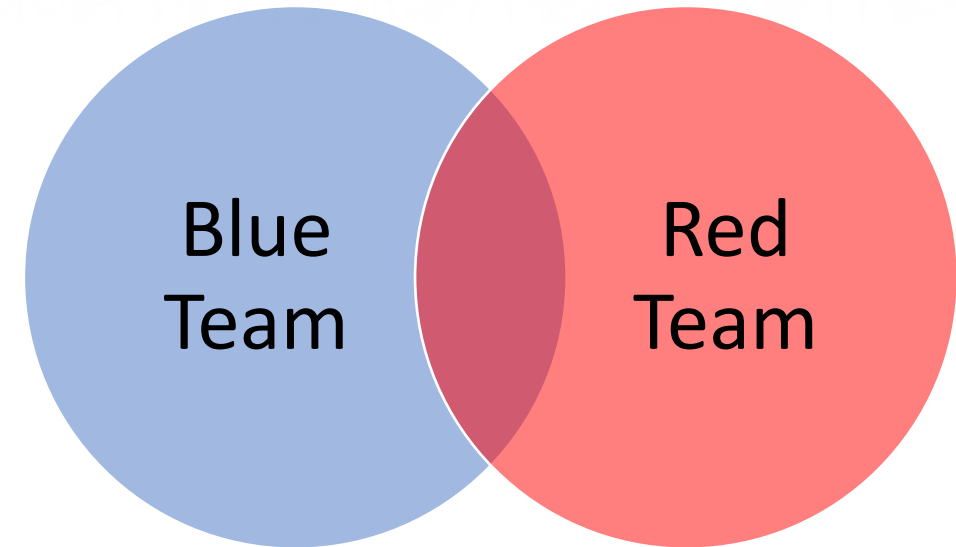
# Methods to Simulate/Emulate

Purple Teams – Fusion of attackers and defenders collaborating

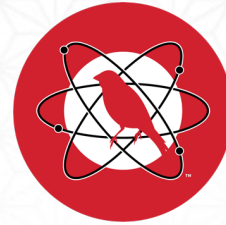
- Focus on the threats we care about
- Can be personnel intensive
- Red team component brings SME and assistance to secure the organization

Automated Red Teams

- Automation can be good
- Do these align to the threats facing the organization?
- Do they help uplevel the defenders once they are complete?



# What Are We Trying To Accomplish?



Atomic  
Detections

Action -> Atomic detection

- Relatively easy to setup and execute
- Specific detection for a specific concern

End to End Scenario

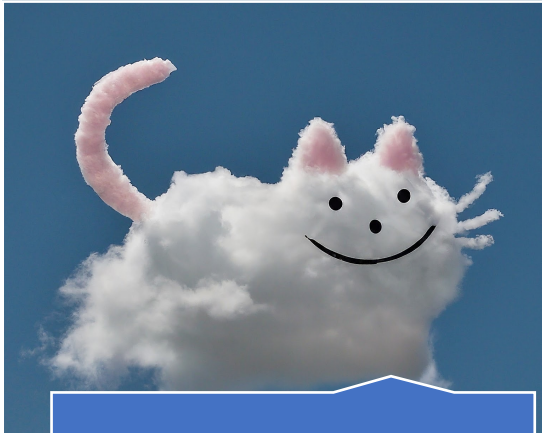
- Can get complex
- Lots to build and test depending on scope
- Loads of potential to better understand a specific adversary
- Detections can be across a broad continuum versus atomic detections
  - Chaining detection X with Z is consequential but not with Y
  - Helpful for analysts to understand threats more broadly

Actions
<b>Group 1 - Initial Access and Execution</b>
Protected Theater - APT34, TWOTONE Execution
<b>Group 2 - Command and Control</b>
Benign Remote Desktop Protocol Traffic
<b>Group 3 - Command and Control, Downloads</b>
Malicious File Transfer - APT34, MANGOPUNCH, Download
Malicious File Transfer - APT34, SEASHARPEE, Download
Malicious File Transfer - APT34, EDGEBENDER, Download
Malicious File Transfer - APT34, TOEMOUSE, Download
Malicious File Transfer - APT34, POWERSTATS, Download
Malicious File Transfer - APT34, NUTSHELL, Download

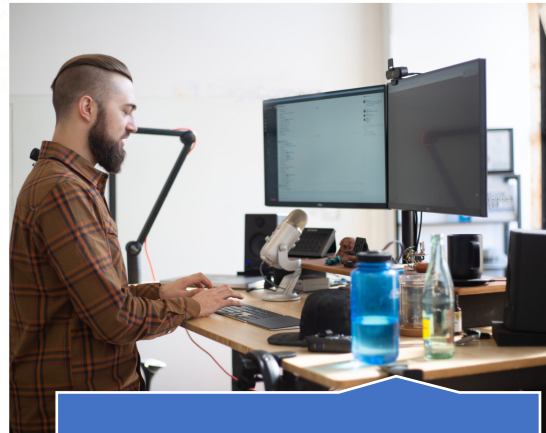
Sequence/  
Unit Tests

End to End  
Scenario

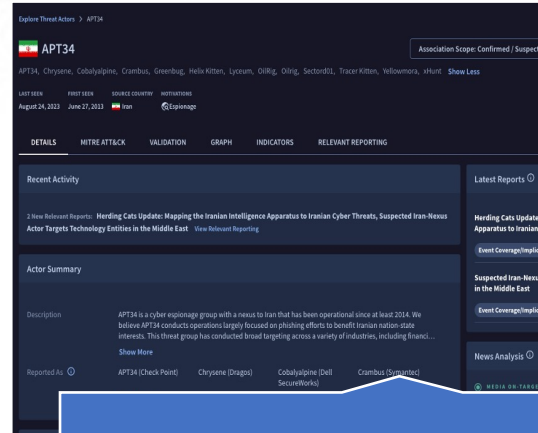
# If You Decide To Build End to End...



Imagination



Experience



Threat Intelligence

Atomic Testing	Micro Emulation	Full Emulation
Single technique	Emulate compound behaviors across 2-3 techniques	Emulate adversary operations
Executable in seconds	Executable in seconds	Executable in minutes
Red test for LSASS Memory	E.g., Fork & Run Process Injection	E.g., FIN6 adversary emulation
Easy to automate	Easy to automate	Difficult to automate
Validate atomic analytics	Validate atomic analytics	Validate atomic analytics
Validate chain analytics	Validate chain analytics	Validate chain analytics
Evaluate SOC against a specific set of TTPs	Evaluate SOC against a specific set of TTPs	Evaluate SOC against a specific set of TTPs
Evaluate SOC holistically	Difficult to evaluate SOC holistically	Evaluate SOC holistically

MITRE CTID Adversary Emulation Plans

# Prioritizing What We Need To Detect

Who is targeting us?

What (platforms | applications | services) are we using that align with things that adversary has exploited previously?

Where do we perceive our detection gaps?



What needs to be defended?

What are our crown jewels?

- Systems/Data
- Users – Executives/R&D/IT?

# Data Generation

Should we generate our data directly in production?

- Accurate depiction of security controls and configs
- How do we ensure that analysts are aware of emulations and any associated detections?
- Malware?

Does our development environment align to production?

- EDR/NDR policies will need to align with reality
- System configurations (Patched in the lab, but not for two years in prod)
- Are the users & systems representative of production?
  - Applications
  - Cloud Policies

# How Threat Intelligence Fits

## Prioritization

Focus on adversaries & techniques we care about

Fodder for detection ideas

## IOCs

- Be careful not to over rotate

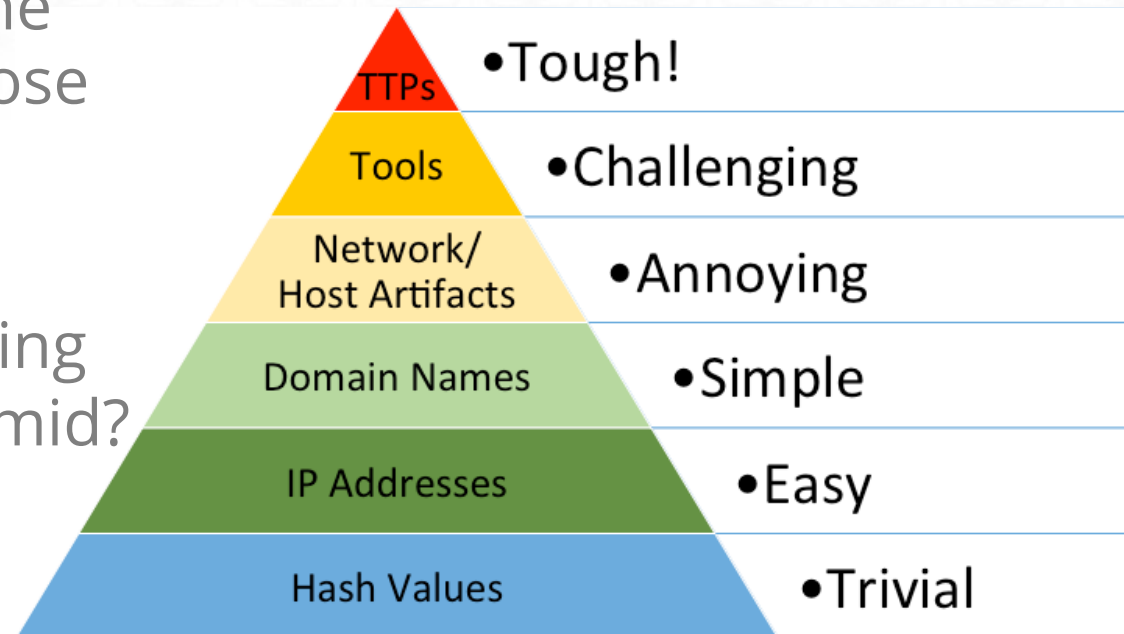
The screenshot shows a threat intelligence dashboard for APT34. At the top, it displays the actor name 'APT34' with an Iranian flag icon, and a table of associated aliases: Chrysene, Cobalyalpine, Crambus, Greenbug, Helix Kitten, Lyceum, OilRig, Oilrig, Sector01, Tracer Kitten, Yellowmora, and xHunt. Below this is a table with columns for 'LAST SEEN', 'FIRST SEEN', 'SOURCE COUNTRY', and 'MOTIVATIONS'. The 'LAST SEEN' entry is 'August 24, 2023', 'FIRST SEEN' is 'June 27, 2013', 'SOURCE COUNTRY' is 'Iran', and 'MOTIVATIONS' is 'Espionage'. The dashboard includes navigation tabs for 'DETAILS', 'MITRE ATT&CK', 'VALIDATION', 'GRAPH', 'INDICATORS', and 'RELEVANT REPORTING'. The 'Recent Activity' section shows '2 New Relevant Reports: Herding Cats Update: Mapping the Iranian Intelligence Apparatus to Iranian Cyber Threats, Suspected Iran-Nexus Actor Targets Technology Entities in the Middle East'. The 'Actor Summary' section provides a description: 'APT34 is a cyber espionage group with a nexus to Iran that has been operational since at least 2014. We believe APT34 conducts operations largely focused on phishing efforts to benefit Iranian nation-state interests. This threat group has conducted broad targeting across a variety of industries, including financi...'. The 'Reported As' section lists 'APT34 (Check Point)', 'Chrysene (Dragos)', 'Cobalyalpine (Dell SecureWorks)', and 'Crambus (Symantec)'. The 'Group Associations' section is partially visible. On the right, there are sections for 'Latest Reports' and 'News Analysis', both featuring reports from 'THE HACKER NEWS' with 'NEW' and 'PLAUSIBLE' tags.

# Threat Intelligence IOCs

Detecting against IOCs is important, but the process around what is done based on those detections is more important

Are we taking those IP and hashes and doing something with them to work up the pyramid?

Detection focus should be the upper end of the pyramid



<https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>

# Attacking/Defending the Cloud

Can you emulate an attack in your cloud infrastructure?

<https://aws.amazon.com/security/penetration-testing/>

<https://support.google.com/cloud/answer/6262505>

<https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement>

Do your homework before you conduct an emulation within the cloud

Links above are not exhaustive



# MITRE CTID Emulation Plan – Nation State Actor

Based on Windows only environment

- Exchange, SQL, Active Directory, Workstation

General Flow

- Workstation compromise leads to a webshell being used on the Exchange server to dump credentials and stage tools followed by lateral movement to the SQL server

Benefit

- Created the ability to exercise controls without being focused on standing up adversary tooling
- Opportunities exist to customize the emulation plan or use it as is

Unit testing of components are required

# Event Creation & Data Review



# Event Creation & Data Review



```
# OilRig has run ipconfig /all on a victim.
```

```
Jan 25 20:33:26 Win 4624/4688/4672 Sysmon 1/10
```

```
curl --http1.1 --ntlm -u 'lunarstiiness\dan.cooper:blue-manatee-2' -k -X  
POST --data "pro=cmd.exe" --data "cmd=ipconfig /all"  
https://23.251.154.146/ews/contact.aspx
```

# Event Creation & Data Review

TIMESTAMP	EVENT	METADAT...	PRINCIPAL.HOST...	PRINCIPAL.PROCESS.COMMAND_LINE	PRINCIPAL.PROCESS.FILE....	TARGET.PROCESS.COMMAN...
2024-01-25T20:33:26.259	PROCESS_LAUNCH cmd.exe launched by w3wp.exe	1	win-helium.lunarstiiiness.com	c:\windows\system32\inetsrv\w3wp.exe -ap "MSEExchangeServicesAppPool" -v "v4.0" -c "C:\Program Files\Microsoft\Exchange Server\V15\bin\GenericAppPoolConfigWithGCServerEnabledFalse.config" -a \\.\pipe\iisipm7df805f7-e790-4266-9aad-3063fc9e1d21 -h "C:\inetpub\temp\appools\MSEExchangeServicesAppPool\MSEExchangeServicesAppPool.config" -w "" -m 0	C:\Windows\System32\inetsrv\w3wp.exe	"cmd.exe" /c ipconfig /all
2024-01-25T20:33:26.257	NETWORK_CONNEC win-helium to win-adfc	dce_rpc	win-helium	[Unknown]	[Unknown]	[Unknown]
2024-01-25T20:33:26.153	NETWORK_CONNEC 34.118.170.49 to win-helium	ssl	[Unknown]	[Unknown]	[Unknown]	[Unknown]
2024-01-25T20:33:26.117	NETWORK_CONNEC 34.118.170.49 to win-helium	conn	[Unknown]	[Unknown]	[Unknown]	[Unknown]
2024-01-25T20:33:26.000	PROCESS_LAUNCH cmd.exe launched by w3wp.exe	4688	win-helium.lunarstiiiness.com	[Unknown]	C:\Windows\System32\inetsrv\w3wp.exe	"cmd.exe" /c ipconfig /all



# How Many Of These Are Detection Opportunities?

Phishing  
Valid Domain Account  
Use of VB/Windows Command  
Scheduled Tasks  
System Services/Execution  
Web Shell  
File Deletion  
Masquerading  
Credential Dumping  
Account Discovery  
Pass The Hash  
Ingress Tool Transfer

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Click to Compromise	Command and Scripting Processor	Account Manipulation	Abuse Desktop Control Mechanism	Abuse Desktop Control Mechanism	Adversary-In-The-Middle	Account Discovery	Enumeration of Remote Services	Adversary-In-The-Middle	Application Layer Protocol	Administrative Exfiltration
Exploit Public-Facing Application	Javacvst	Active Directory	Access Token Manipulation	Access Token Manipulation	Arbitrary File Write	Calendar Access	Active Spanning	Active Collected Data	API	API
External Remote Services	PowerShell	BITS Jobs	BitLocker Local Authentication	BitLocker Local Authentication	BITS Jobs	Email Account	Remote Session Hijacking	Public Catalogs	File Transfer Protocols	Catalogs
Hardware Address	Pylons	Boot or Login Assistant Execution	Boot or Login Assistant Execution	Boot or Login Assistant Execution	Credentials Run Pastward-Status	Local Account	Service Session Hijacking	Automated Collection	Mal Proxies	Mal Proxies
<b>Phishing</b>	Win Shell	Browser Extensions	Credit or Malicious System Process	Credit or Malicious System Process	Desktop Non-Web Browser	Local Account	Service Session Hijacking	Service Session Hijacking	Mal Proxies	Mal Proxies
Spawning Remote Execution	PowerShell	Component Object Model Software Binary	Domain Policy Modification	Domain Policy Modification	Desktop Search	Application Window Discovery	Desktop Component Object Model	Automated Collection	Browser Session Hijacking	Browser Session Hijacking
Unauthorized Logins	PowerShell	Credential Access	Domain Policy Modification	Domain Policy Modification	Desktop Search	Browser Session Discovery	Desktop Component Object Model	Automated Collection	Browser Session Hijacking	Browser Session Hijacking
Unauthorized Logins	PowerShell	Credential Access	Domain Policy Modification	Domain Policy Modification	Desktop Search	Browser Session Discovery	Desktop Component Object Model	Automated Collection	Browser Session Hijacking	Browser Session Hijacking
Unauthorized Logins	PowerShell	Credential Access	Domain Policy Modification	Domain Policy Modification	Desktop Search	Browser Session Discovery	Desktop Component Object Model	Automated Collection	Browser Session Hijacking	Browser Session Hijacking
Unauthorized Logins	PowerShell	Credential Access	Domain Policy Modification	Domain Policy Modification	Desktop Search	Browser Session Discovery	Desktop Component Object Model	Automated Collection	Browser Session Hijacking	Browser Session Hijacking

[https://github.com/center-for-threat-informed-defense/adversary\\_emulation\\_library/blob/master/oilrig/Intelligence\\_Summary/Intelligence\\_Summary.md](https://github.com/center-for-threat-informed-defense/adversary_emulation_library/blob/master/oilrig/Intelligence_Summary/Intelligence_Summary.md)

# Aggregated Events for Discovery Tactics

2024-01-25 00:00:00 - 2024-01-26 00:00:00

## 2 Detections

EXPAND ALL UNWRAP TEXT COLUMNS

Search Rows

TIMESTAMP ↑	DETECTION	EVENT_COUNT...	TARGET_PROCESS_COMMAND_LINE (OUTCOME)
> 2024-01-25T20:03:00.000	<b>DETECTION</b> hostname:wrk-pacman.lunarstiiiness.com	8	C:\Windows\system32\cmd.exe /c whoami & hostname & ipconfig /all & net user /domain 2>&1 & net group /domain 2>&1 & net group "domain admins" /domain 2>&1 & net group "Exchange Trusted Subsystem" /domain 2>&1 & net accounts /domain 2>&1 & net user 2>&1 & net localgroup administrators 2>&1 & netstat -an 2>&1 & tasklist 2>&1 & sc query 2>&1 & systeminfo 2>&1 & reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" 2>&1 2>&1, ipconfig /all, netstat -an, reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default", sc query, systeminfo, tasklist, whoami
> 2024-01-25T20:34:30.000	<b>DETECTION</b> hostname:win-helium.lunarstiiiness.com	14	"C:\Windows\system32\nslookup.exe" -type=A WIN-HELIUM.lunarstiiiness.com. 10.128.0.21, "cmd.exe" /c ipconfig /all, "cmd.exe" /c netstat -an, "cmd.exe" /c whoami, ipconfig /all, netstat -an, whoami

# Compound Rule – Web Shell

Looking for process launches and file creations with corresponding network traffic

- Corelight for Network Traffic
- Sysmon (EDR) for Endpoint Traffic

Without getting into filtering IP addresses and file paths, getting a good detection with both data sources got challenging

- Too much noise or too few detections

Pretty good hunting detection

# Behavioral - Beacon

Similar process launches were seen so frequently

- Tough to separate signal/noise

Task Scheduler presented a method to detect based on frequency analysis

Baselining activity is another option

What kinds of activity accompanied the continual beacon?

- Process launches
- Network connections



# Detection Quality



	Executable Name	Hash Value	Command Strings
	Focus on Behavior Exhibited (lsass.exe access, trailing events on port 445? additional exe run after)		
Recompile	Modify name in code	Hash will change	Obfuscate Command Strings – instead of sekurlsa::pth, why not hatch::peppers?
	Changed from mimikatz.exe to sol.exe	29efd64dd3c7fe1e2b022b7ad73a1ba5	n/a
	mimikatz.exe	29efd64dd3c7fe1e2b022b7ad73a1ba5	n/a

# Malware

Numerous sources to get malware

- The burden of defanging it is on you or running it in isolation and burning down the environment after

CTID Emulation Plans provided “malware” without the mess

- Do the plans align to your adversaries?

What Is Your Focus?

- Broad use of lolbins as well as off the shelf C2 platforms

# Building Out Metrics for Detection

What does our false positive rate look like?

Is the detection better suited to be a hunting rule instead?

- Web Shell

Multiple Behavior Detections

- Task Schedule -> Task & Process -> Task & Process & Network

One additional criteria can skew test results to be careful

Overfitting is real

# Continual Testing & Validation

Engineering a new solution is fun

- Operations & Maintenance - not so much

Impacts to Detections

- What happens when the security controls change?
- What happens when the surrounding architecture changes?
- What happens when the logging format changes?

Goal is to remove potential blind spots due to IT lifecycle that has huge impact to SecOps

# Do I Need An End to End Emulation?

Weigh the pros and cons

What resources exist?

We built our own automated tooling to ingest emulated events

- Use for gamification and instruction

Atomic and smaller unit tests are very valid and a great place to start

# Additional Reading

Detection as Code – David French

<https://www.googlecloudcommunity.com/gc/Community-Blog/Getting-Started-with-Detection-as-Code-and-Chronicle-Security/ba-p/702154>

Practical Threat Detection Engineering – Megan Roddie

<https://www.packtpub.com/product/practical-threat-detection-engineering/9781801076715>

MITRE CTID Adversary Emulation Plans

<https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/adversary-emulation-library/>

Red Canary Atomic Red Team

<https://github.com/redcanaryco/atomic-red-team>

#FIRSTCON24

# Thank You!

John Stoner

<https://www.linkedin.com/in/johnastoner>

@stonerpsu (the other socials)

