Control Validation Compass

Intelligence for Improved Security Validation

Disclaimer

All content contained in this presentation is solely the view of the presenter, and does not represent the opinions, beliefs, experiences, policy, or operating agreements of any organizations the speaker currently works for or has worked for in the past.

Scott Small

Senior Analyst - Adversary Emulation & Threat Modeling
Major US Retailer

twitter.com/IntelScott

github.com/TropChaud

Why does Control Compass exist?

- MITRE ATT&CK© is valuable for bridging threats <-> controls
- Organizations struggle to operationalize CTI
- Defense prioritization is hard (few models/frameworks)
- Industry-based threat modeling is difficult (& time consuming!)

(But don't take my word for it)

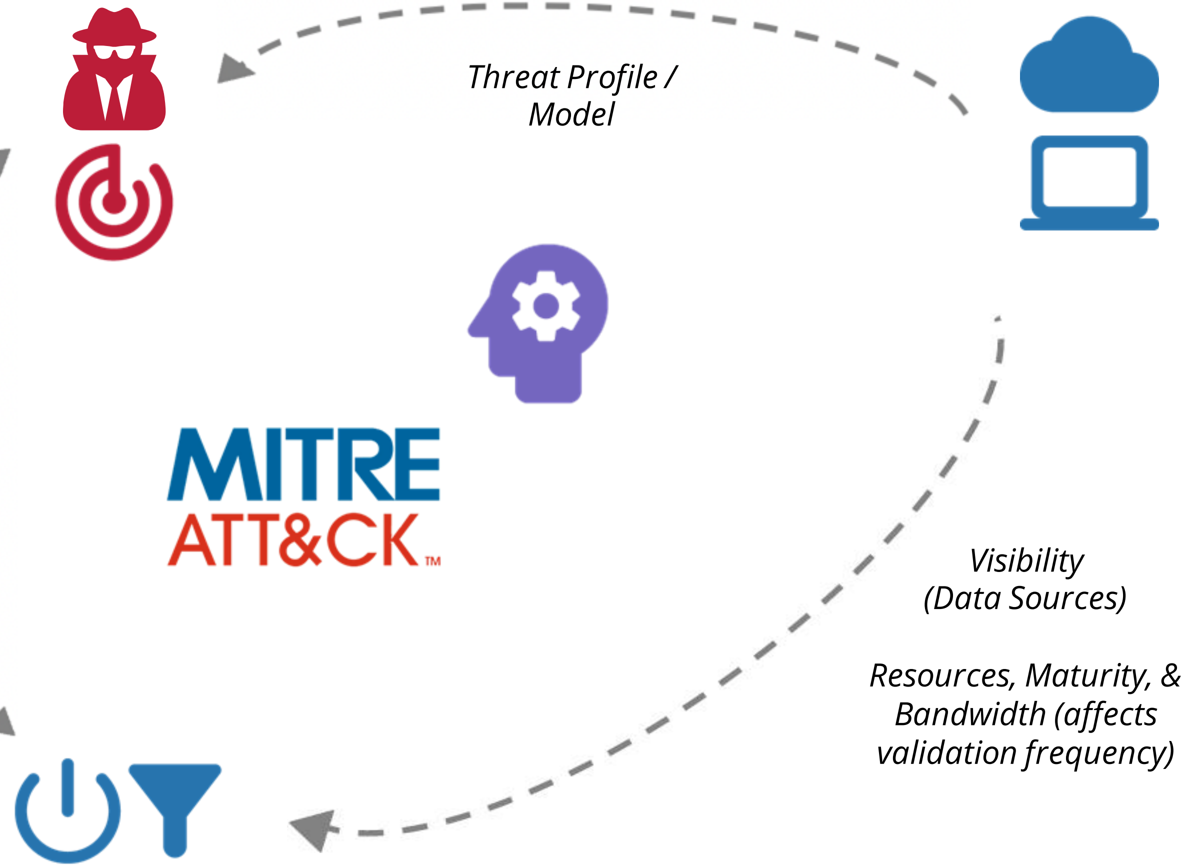
Resistance Isn't Futile: A Practical Approach to Prioritizing Defenses with Threat Modeling

Katie Nickels

Hunting for Post-Exploitation Stage Attacks with Elastic Stack and the MITRE ATT&CK Framework

- John Hubbard

Prioritizing Detections: Risk Profiling



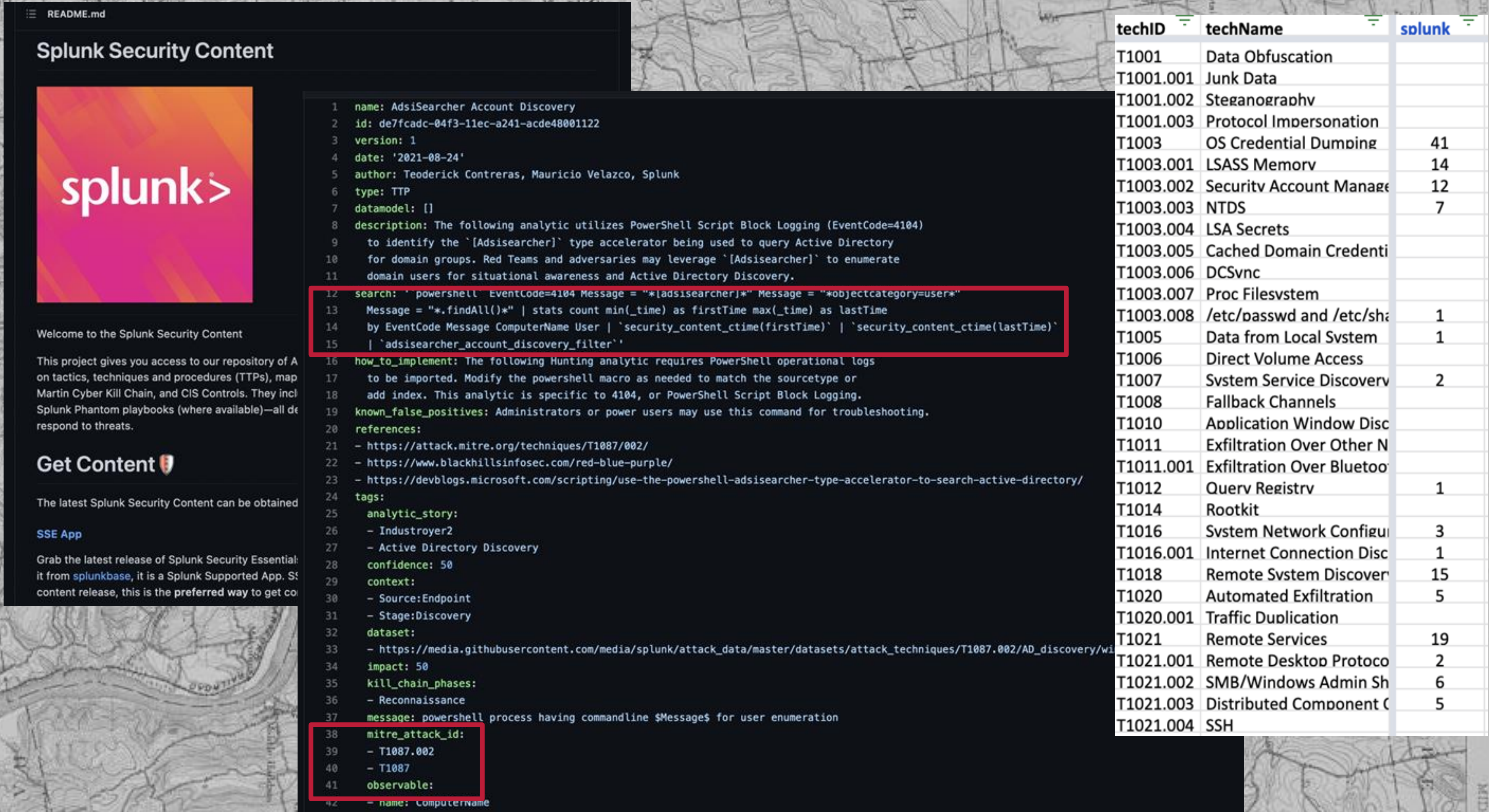
Threat Profile /
Model

Threat Profile /
Model

Actual Control
Coverage

Visibility
(Data Sources)

Resources, Maturity, &
Bandwidth (affects
validation frequency)



README.md

Splunk Security Content

Welcome to the Splunk Security Content

This project gives you access to our repository of A
on tactics, techniques and procedures (TTPs), map
Martin Cyber Kill Chain, and CIS Controls. They incl
Splunk Phantom playbooks (where available)—all de
respond to threats.

Get Content 🛡

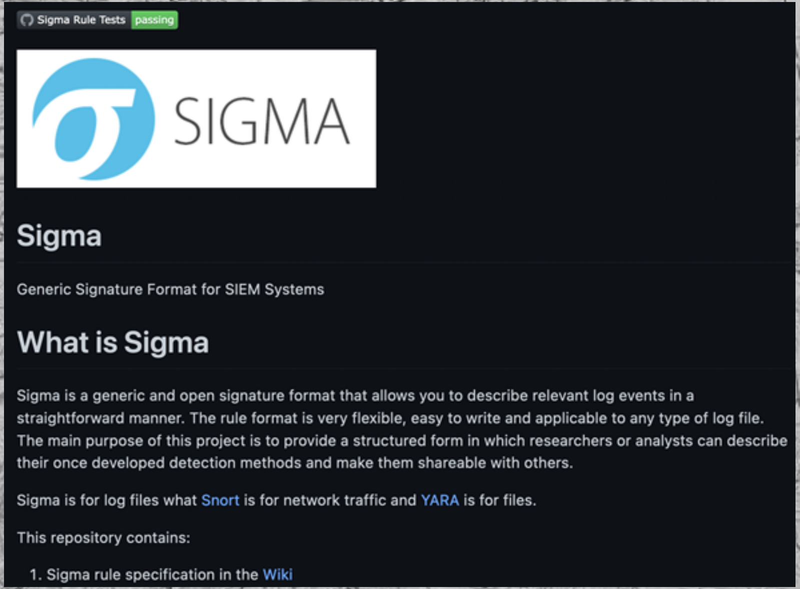
The latest Splunk Security Content can be obtained

SSE App

Grab the latest release of Splunk Security Essential
it from splunkbase, it is a Splunk Supported App. S
content release, this is the **preferred way** to get co

```
name: AdsiSearcher Account Discovery
id: de7fcadc-04f3-11ec-a241-acde48001122
version: 1
date: '2021-08-24'
author: Teoderick Contreras, Mauricio Velazco, Splunk
type: TTP
datamodel: []
description: The following analytic utilizes PowerShell Script Block Logging (EventCode=4104)
  to identify the `[Adsisearcher]` type accelerator being used to query Active Directory
  for domain groups. Red Teams and adversaries may leverage `[Adsisearcher]` to enumerate
  domain users for situational awareness and Active Directory Discovery.
search: '`powershell` EventCode=4104 Message = "*[adsisearcher]*" Message = "*objectcategory=user*"
  Message = "*.findAll()*" | stats count min(_time) as firstTime max(_time) as lastTime
  by EventCode Message ComputerName User | `security_content_ctime(firstTime)` | `security_content_ctime(lastTime)`
  | `adsisearcher_account_discovery_filter`'
how_to_implement: The following Hunting analytic requires PowerShell operational logs
  to be imported. Modify the powershell macro as needed to match the sourcetype or
  add index. This analytic is specific to 4104, or PowerShell Script Block Logging.
known_false_positives: Administrators or power users may use this command for troubleshooting.
references:
- https://attack.mitre.org/techniques/T1087/002/
- https://www.blackhillsinfosec.com/red-blue-purple/
- https://devblogs.microsoft.com/scripting/use-the-powershell-adsisearcher-type-accelerator-to-search-active-directory/
tags:
  analytic_story:
  - Industroyer2
  - Active Directory Discovery
  confidence: 50
  context:
  - Source:Endpoint
  - Stage:Discovery
  dataset:
  - https://media.githubusercontent.com/media/splunk/attack_data/master/datasets/attack_techniques/T1087.002/AD_discovery/wi
  impact: 50
  kill_chain_phases:
  - Reconnaissance
  message: powershell process having commandline $Message$ for user enumeration
  mitre_attack_id:
  - T1087.002
  - T1087
  observable:
  - name: ComputerName
```

techID	techName	splunk
T1001	Data Obfuscation	
T1001.001	Junk Data	
T1001.002	Steganography	
T1001.003	Protocol Impersonation	
T1003	OS Credential Dumping	41
T1003.001	LSASS Memory	14
T1003.002	Security Account Manage	12
T1003.003	NTDS	7
T1003.004	LSA Secrets	
T1003.005	Cached Domain Credenti	
T1003.006	DCSync	
T1003.007	Proc Filesystem	
T1003.008	/etc/passwd and /etc/sha	1
T1005	Data from Local System	1
T1006	Direct Volume Access	
T1007	System Service Discovery	2
T1008	Fallback Channels	
T1010	Application Window Disc	
T1011	Exfiltration Over Other N	
T1011.001	Exfiltration Over Blueto	
T1012	Query Registry	1
T1014	Rootkit	
T1016	System Network Configu	3
T1016.001	Internet Connection Disc	1
T1018	Remote System Discover	15
T1020	Automated Exfiltration	5
T1020.001	Traffic Duplication	
T1021	Remote Services	19
T1021.001	Remote Desktop Protoco	2
T1021.002	SMB/Windows Admin Sh	6
T1021.003	Distributed Component (	5
T1021.004	SSH	



Sigma Rule Tests passing

SIGMA

Sigma

Generic Signature Format for SIEM Systems

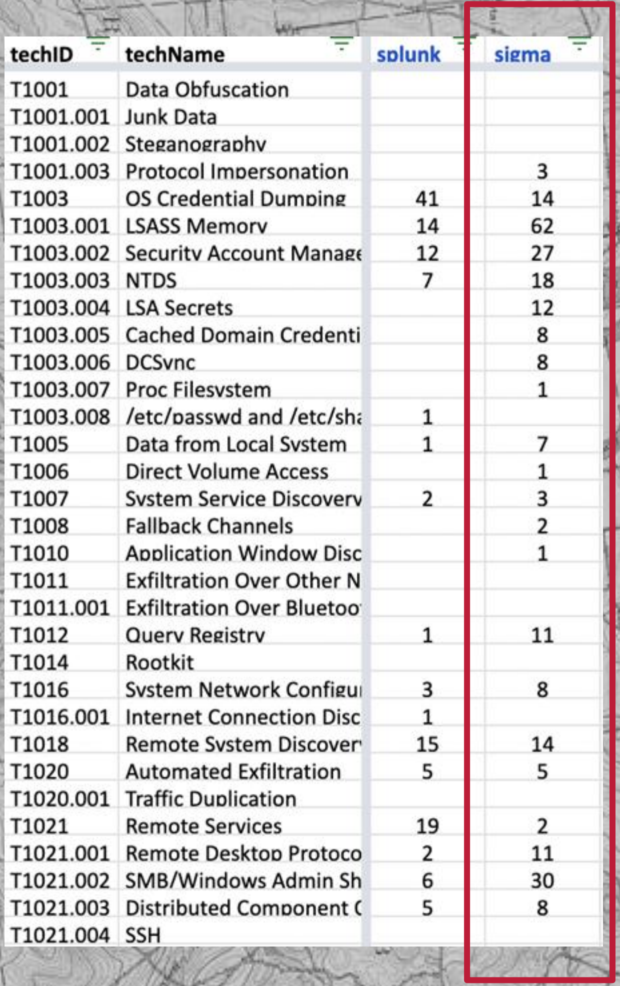
What is Sigma

Sigma is a generic and open signature format that allows you to describe relevant log events in a straightforward 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.

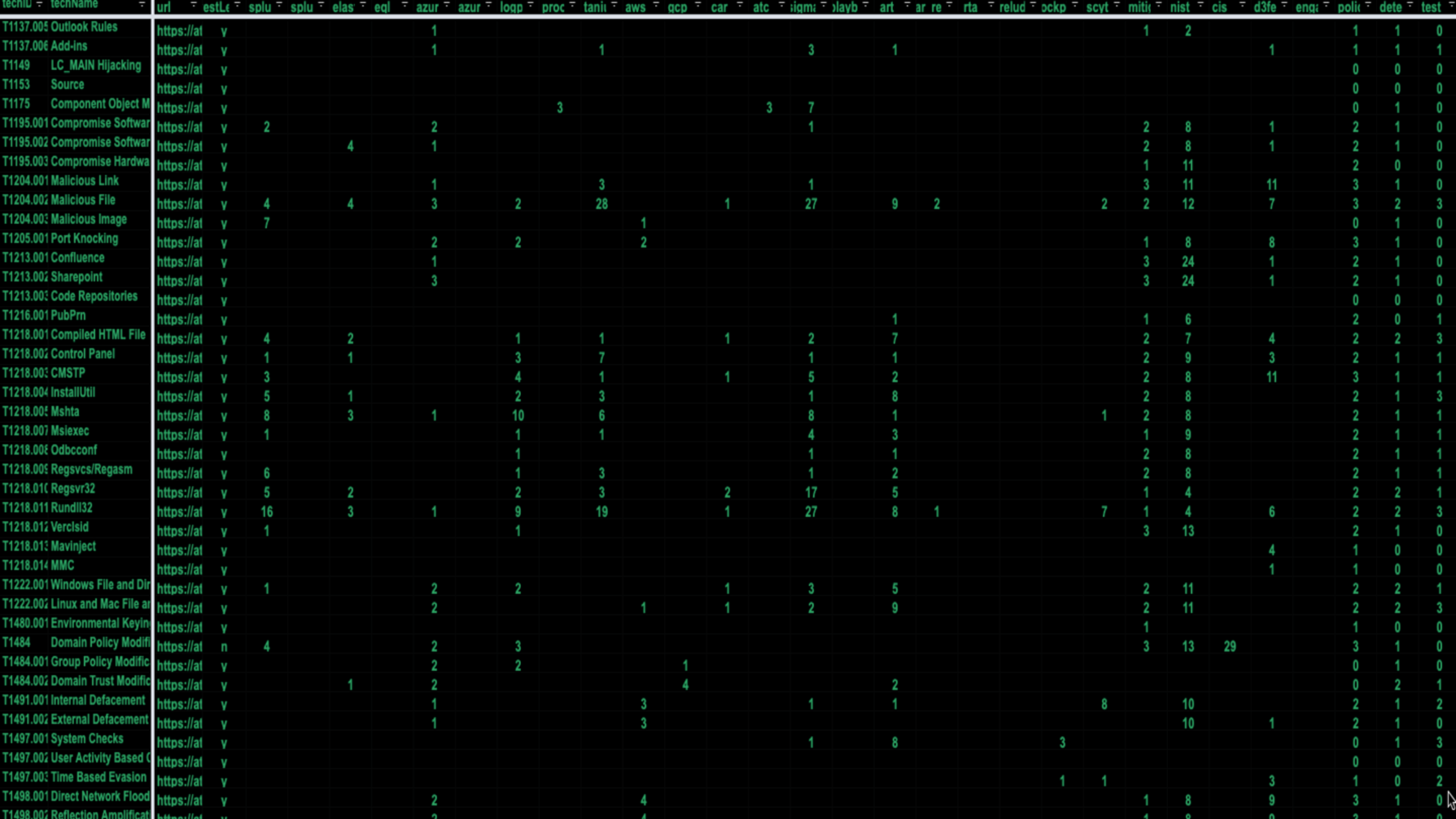
Sigma is for log files what Snort is for network traffic and YARA is for files.

This repository contains:

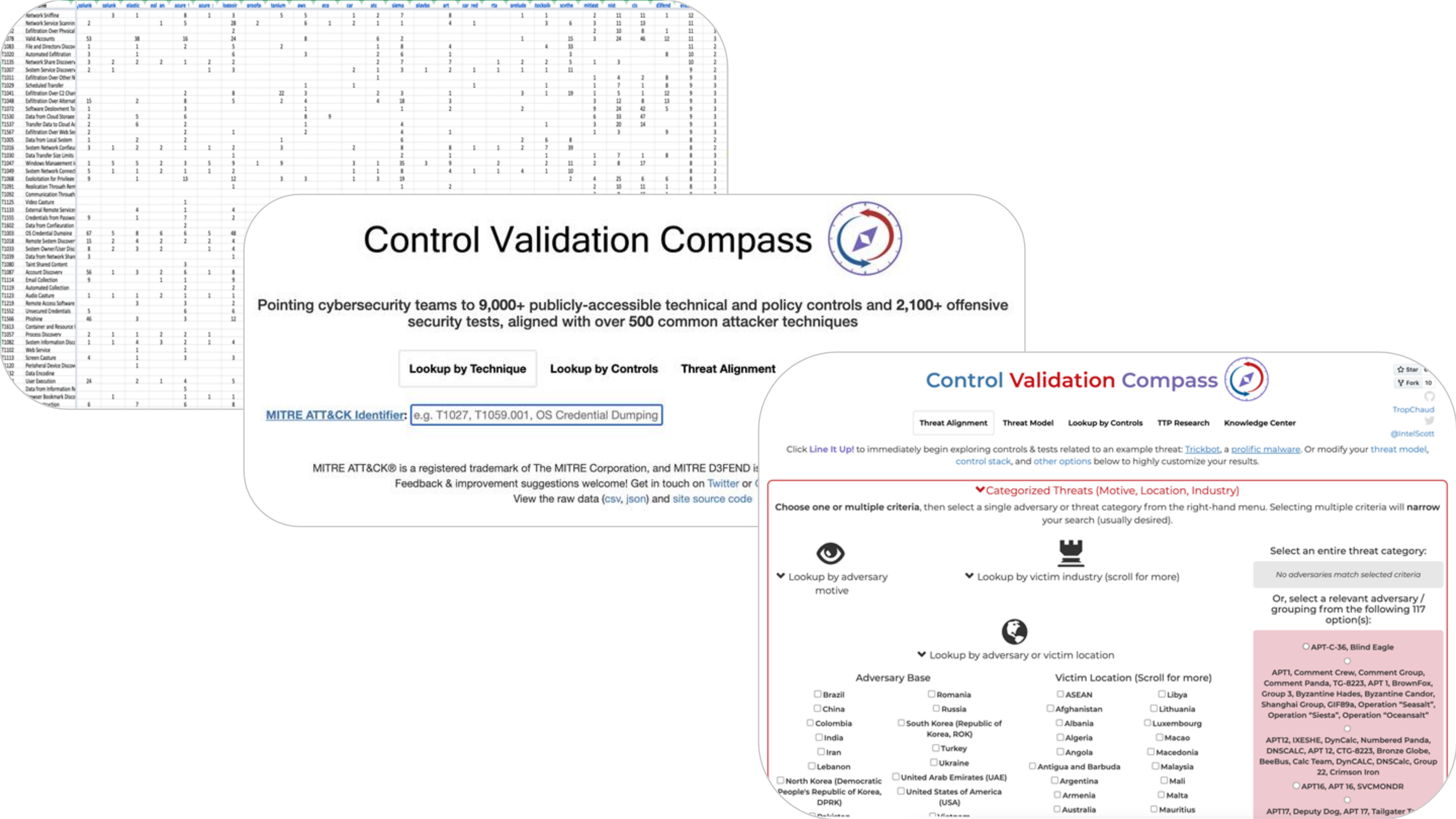
1. Sigma rule specification in the Wiki



techID	techName	splunk	sigma
T1001	Data Obfuscation		
T1001.001	Junk Data		
T1001.002	Steganography		
T1001.003	Protocol Impersonation		3
T1003	OS Credential Dumping	41	14
T1003.001	LSASS Memory	14	62
T1003.002	Security Account Manage	12	27
T1003.003	NTDS	7	18
T1003.004	LSA Secrets		12
T1003.005	Cached Domain Credenti		8
T1003.006	DCSync		8
T1003.007	Proc Filesystem		1
T1003.008	/etc/passwd and /etc/sha	1	
T1005	Data from Local System	1	7
T1006	Direct Volume Access		1
T1007	System Service Discovery	2	3
T1008	Fallback Channels		2
T1010	Application Window Disc		1
T1011	Exfiltration Over Other N		
T1011.001	Exfiltration Over Bluetoo		
T1012	Query Registry	1	11
T1014	Rootkit		
T1016	System Network Configu	3	8
T1016.001	Internet Connection Disc	1	
T1018	Remote System Discover	15	14
T1020	Automated Exfiltration	5	5
T1020.001	Traffic Duplication		
T1021	Remote Services	19	2
T1021.001	Remote Desktop Protoco	2	11
T1021.002	SMB/Windows Admin Sh	6	30
T1021.003	Distributed Component (	5	8
T1021.004	SSH		



techID	techName	url	estLe	splu	splu	elas	eql	azur	azur	logp	proc	tani	aws	gcp	car	atc	igma	layb	art	ar	re	rta	relud	ockp	scyt	mitig	nist	cis	d3fe	enga	polic	dete	test
T1137.005	Outlook Rules	https://at	y					1																		1	2				1	1	0
T1137.006	Add-ins	https://at	y					1				1					3		1										1		1	1	1
T1149	LC_MAIN Hijacking	https://at	y																												0	0	0
T1153	Source	https://at	y																												0	0	0
T1175	Component Object M	https://at	y								3					3	7														0	1	0
T1195.001	Compromise Softwar	https://at	y	2				2									1									2	8		1		2	1	0
T1195.002	Compromise Softwar	https://at	y			4		1																		2	8		1		2	1	0
T1195.003	Compromise Hardwa	https://at	y																							1	11				2	0	0
T1204.001	Malicious Link	https://at	y					1				3					1									3	11		11		3	1	0
T1204.002	Malicious File	https://at	y	4		4		3		2		28			1		27		9		2				2	2	12		7		3	2	3
T1204.003	Malicious Image	https://at	y	7									1																		0	1	0
T1205.001	Port Knocking	https://at	y					2		2			2													1	8		8		3	1	0
T1213.001	Confluence	https://at	y					1																		3	24		1		2	1	0
T1213.002	Sharepoint	https://at	y					3																		3	24		1		2	1	0
T1213.003	Code Repositories	https://at	y																												0	0	0
T1216.001	PubPrn	https://at	y																1							1	6				2	0	1
T1218.001	Compiled HTML File	https://at	y	4		2				1		1			1		2		7							2	7		4		2	2	3
T1218.002	Control Panel	https://at	y	1		1				3		7					1		1							2	9		3		2	1	1
T1218.003	CMSTP	https://at	y	3						4		1			1		5		2							2	8		11		3	1	1
T1218.004	InstallUtil	https://at	y	5		1				2		3					1		8							2	8				2	1	3
T1218.005	Mshta	https://at	y	8		3		1		10		6					8		1						1	2	8				2	1	1
T1218.007	Msiexec	https://at	y	1						1		1					4		3							1	9				2	1	1
T1218.008	Odbcconf	https://at	y							1							1		1							2	8				2	1	1
T1218.009	Regsvcs/Regasm	https://at	y	6						1		3					1		2							2	8				2	1	1
T1218.010	Regsvr32	https://at	y	5		2				2		3			2		17		5							1	4				2	2	1
T1218.011	Rundll32	https://at	y	16		3		1		9		19			1		27		8		1				7	1	4		6		2	2	3
T1218.012	Verclsid	https://at	y	1						1																3	13				2	1	0
T1218.013	Mavinject	https://at	y																										4		1	0	0
T1218.014	MMC	https://at	y																										1		1	0	0
T1222.001	Windows File and Dir	https://at	y	1				2		2					1		3		5							2	11				2	2	1
T1222.002	Linux and Mac File ar	https://at	y					2					1		1		2		9							2	11				2	2	3
T1480.001	Environmental Keying	https://at	y																							1					1	0	0
T1484	Domain Policy Modifi	https://at	n	4				2		3																3	13	29			3	1	0
T1484.001	Group Policy Modific	https://at	y					2		2				1																	0	1	0
T1484.002	Domain Trust Modific	https://at	y			1		2						4					2												0	2	1
T1491.001	Internal Defacement	https://at	y					1					3				1		1						8		10				2	1	2
T1491.002	External Defacement	https://at	y					1					3														10		1		2	1	0
T1497.001	System Checks	https://at	y														1		8					3							0	1	3
T1497.002	User Activity Based (	https://at	y																												0	0	0
T1497.003	Time Based Evasion	https://at	y																					1	1				3		1	0	2
T1498.001	Direct Network Flood	https://at	y					2					4													1	8		9		3	1	0
T1498.002	Reflection Amplificat	https://at	y					2					4													1	8		9		[illegible]	[illegible]	[illegible]



	ame	splunk	splunk	elastic	eql an	azure !	azure :	loesoir	proofp	tanium	aws	eca	car	atc	siema	plavbo	art	car red	rta	prelude	rockolk	scythe	mitlast	nist	cis	d3fend	em	
	Network Sniffing		3	1		8	1	3		5	5		1	2	7		8			1	1		2	11	11	1	12	
	Network Service Scannin	2			1	5		28	2		6	1	2	1	1		4	1			3	6	3	11	13		11	
2	Exfiltration Over Physical							2															2	10	8	1	11	3
078	Valid Accounts	53		38		16		24			8			6	2					1		15	3	24	46	12	11	3
1083	File and Directory Discov	1		1		2		5		2				1	8		4				4	33					11	2
T1020	Automated Exfiltration	3		1				6			3			2	6		1					3				8	10	2
T1135	Network Share Discovery	3	2	2	2	1	2	2						2	7		7		1	2	2	5	1	3			10	2
T1007	System Service Discovery	2	1				1	3					2	1	3	1	2	1	1	1	1	11					9	2
T1011	Exfiltration Over Other N													1									1	4	2	8	9	3
T1029	Scheduled Transfer										1		1					1			1		1	7	1	8	9	3
T1041	Exfiltration Over C2 Chan					2		8		22	3			2	3		1			3	1	19	1	5	1	12	9	3
T1048	Exfiltration Over Alternat	15		2		8		5		2	4			4	18		3						3	12	8	13	9	3
T1072	Software Deployment To	1				3					1				1		2			2			9	24	42	5	9	3
T1530	Data from Cloud Storage	2		5		6					8	9											6	33	47		9	3
T1537	Transfer Data to Cloud Ac	2		6		2					1				4						1		3	20	14		9	3
T1567	Exfiltration Over Web Ser	2				2		1			2				4		1						1	3		9	9	3
T1005	Data from Local System	1		2		2				1					6					2	6	8					8	2
T1016	System Network Configu	3	1	2	2	1	1	2		3			2		8		8	1	1	2	7	39					8	2
T1030	Data Transfer Size Limits							1							2		1				1		1	7	1	8	8	3
T1047	Windows Management I	1	5	5	2	3	5	9	1	9			3	1	35	3	9		2		2	11	2	8	17		8	3
T1049	System Network Connect	5	1	1	2	1	1	2					1	1	8		4	1	1	4	1	10					8	2
T1068	Exploitation for Privilege	9		1		13		12		3	3		1	3	19							2	4	25	6	6	8	3
T1091	Replication Through Rem							1							1		2						2	10	11	1	8	3
T1092	Communication Through																											
T1125	Video Capture					1																						
T1133	External Remote Service			4		1		4																				
T1555	Credentials from Passwo	9		1		7		2																				
T1602	Data from Configuration					2																						
T1003	OS Credential Dumping	67	5	8	6	6	5	48																				
T1018	Remote System Discover	15	2	4	2	2	2	4																				
T1033	System Owner/User Disc	8	2	3	2		1	4																				
T1039	Data from Network Shar	3						1																				
T1080	Taint Shared Content					3																						
T1087	Account Discovery	56	1	3	2	6	1	8																				
T1114	Email Collection	9			1	1		9																				
T1119	Automated Collection					2		2																				
T1123	Audio Capture	1	1	1	2	1	1	1																				
T1219	Remote Access Software			3		3		2																				
T1552	Unsecured Credentials	5				6		6																				
T1566	Phishing	46		3		3		12																				
T1613	Container and Resource I																											
T1057	Process Discovery	2	1	1	2	2	1																					
T1082	System Information Disc	1	1	4	3	2	1	4																				
T1102	Web Service			1		1																						
T1113	Screen Capture	4		1		3		3																				
1120	Peripheral Device Discov			1																								
32	Data Encoding																											
	User Execution	24		2	1	4		5																				
	Data from Information R					5																						
	owser Bookmark Disco		1			1	1	1																				
	uction	6		7		6		8																				

Control Validation Compass

Pointing cybersecurity teams to **9,000+** publicly-accessible technical and policy controls and **2,100+** offensive security tests, aligned with over **500** common attacker techniques

Lookup by Technique **Lookup by Controls** **Threat Alignment**

MITRE ATT&CK Identifier: e.g. T1027, T1059.001, OS Credential Dumping

MITRE ATT&CK® is a registered trademark of The MITRE Corporation, and MITRE D3FEND is

Feedback & improvement suggestions welcome! Get in touch on Twitter or

View the raw data (csv, json) and site source code

Control Validation Compass

Threat Alignment Threat Model Lookup by Controls TTP Research Knowledge Center

Click **Line It Up!** to immediately begin exploring controls & tests related to an example threat: Trickbot, a prolific malware. Or modify your threat model, control stack, and other options below to highly customize your results.

Categorized Threats (Motive, Location, Industry)

Choose one or multiple criteria, then select a single adversary or threat category from the right-hand menu. Selecting multiple criteria will **narrow** your search (usually desired).

Lookup by adversary motive

Lookup by victim industry (scroll for more)

Lookup by adversary or victim location

Adversary Base

□ Brazil
□ China
□ Colombia
□ India
□ Iran
□ Lebanon
□ North Korea (Democratic People's Republic of Korea, DPRK)
□ Romania
□ Russia
□ South Korea (Republic of Korea, ROK)
□ Turkey
□ Ukraine
□ United Arab Emirates (UAE)
□ United States of America (USA)

Victim Location (Scroll for more)

□ ASEAN
□ Afghanistan
□ Albania
□ Algeria
□ Angola
□ Antigua and Barbuda
□ Argentina
□ Armenia
□ Australia
□ Libya
□ Lithuania
□ Luxembourg
□ Macao
□ Macedonia
□ Malaysia
□ Mali
□ Malta
□ Mauritius

Select an entire threat category:

No adversaries match selected criteria

Or, select a relevant adversary / grouping from the following 117 option(s):

○ APT-C-36, Blind Eagle

○ APT1, Comment Crew, Comment Group, Comment Panda, TG-8223, APT 1, BrownFox, Group 3, Byzantine Hades, Byzantine Candor, Shanghai Group, GIF89a, Operation "Seasalt", Operation "Siesta", Operation "Oceansalt"

○ APT12, IXESHE, DynCalc, Numbered Panda, DNSCALC, APT 12, CTG-8223, Bronze Globe, BeeBus, Calc Team, DynCALC, DNSCalc, Group 22, Crimson Iron

○ APT16, APT 16, SVCMONDR

○ APT17, Deputy Dog, APT 17, Tailgater T

Control Validation Compass

controlcompass.github.io

Threat modeling aide & purple team content repository, pointing security & intelligence teams to **10,000+** publicly-accessible technical and policy controls and **2,100+** offensive security tests, aligned with nearly **600** common attacker techniques