Updates from the MITRE ATT&CK® Team

Adam Pennington
ATT&CK Lead

MITRE

ATT&CK 2021

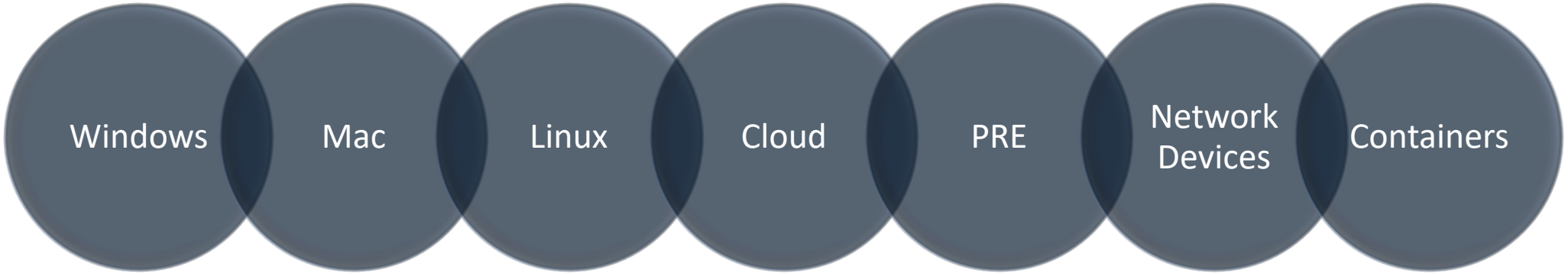
April 29, 2021
Release v9

October 2021
Release v10

You are here

MITRE

ATT&CK for Enterprise

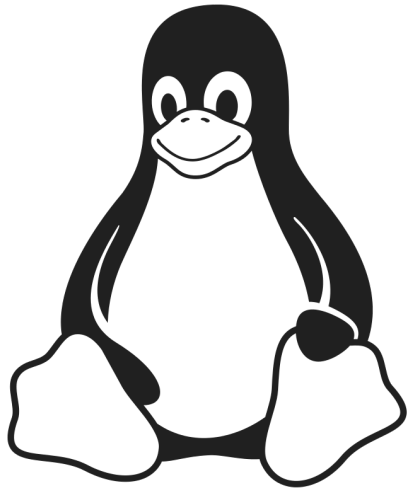


- A period of stability
  - No changes as big as PRE or subs on our roadmap
- Work on backlog for October

MITRE

ATT&CK for Enterprise (Mac/Linux)

- Ongoing effort to improve and expand coverage
  - Much less focus historically than Windows techniques
- Several macOS updates in our April release
  - More than 50% updated, more in October
- Linux updates targeted for October release



MITRE

ATT&CK for Enterprise (Data Sources)

Hijack Execution Flow: COR_PROFILER

- Was a list of text strings
- No details beyond the name
- No descriptions behind them

ID: T1574.012

Sub-technique of: T1574

Tactics: Persistence, Privilege Escalation, Defense Evasion

Platforms: Windows

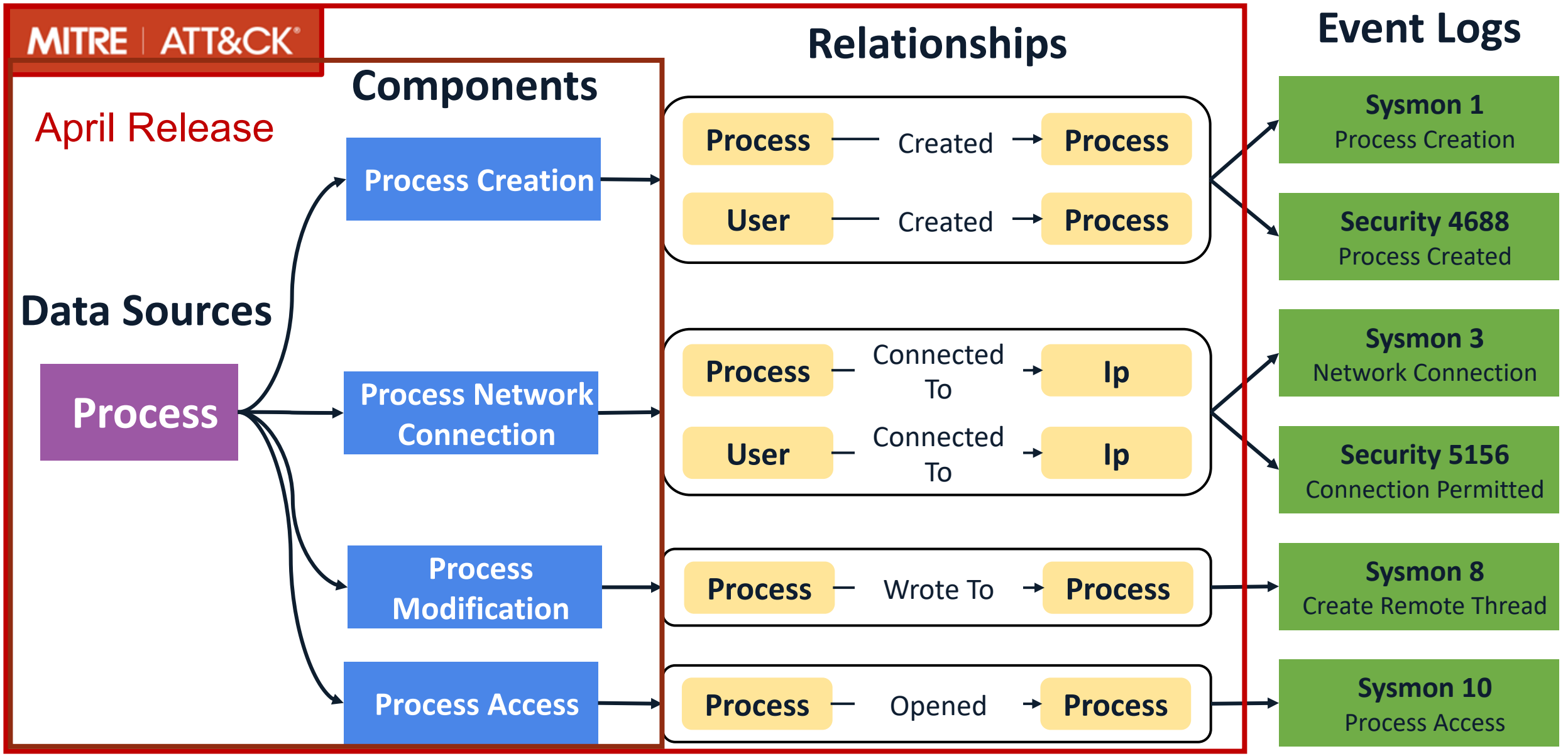
Permissions Required: Administrator, User

Data Sources: File monitoring, Process command-line parameters, Process monitoring, Windows Registry

Contributors: Jesse Brown, Red Canary

MITRE

Adding metadata to ATT&CK data sources



Data Sources for ATT&CK v9

- Data sources list/metadata in GitHub

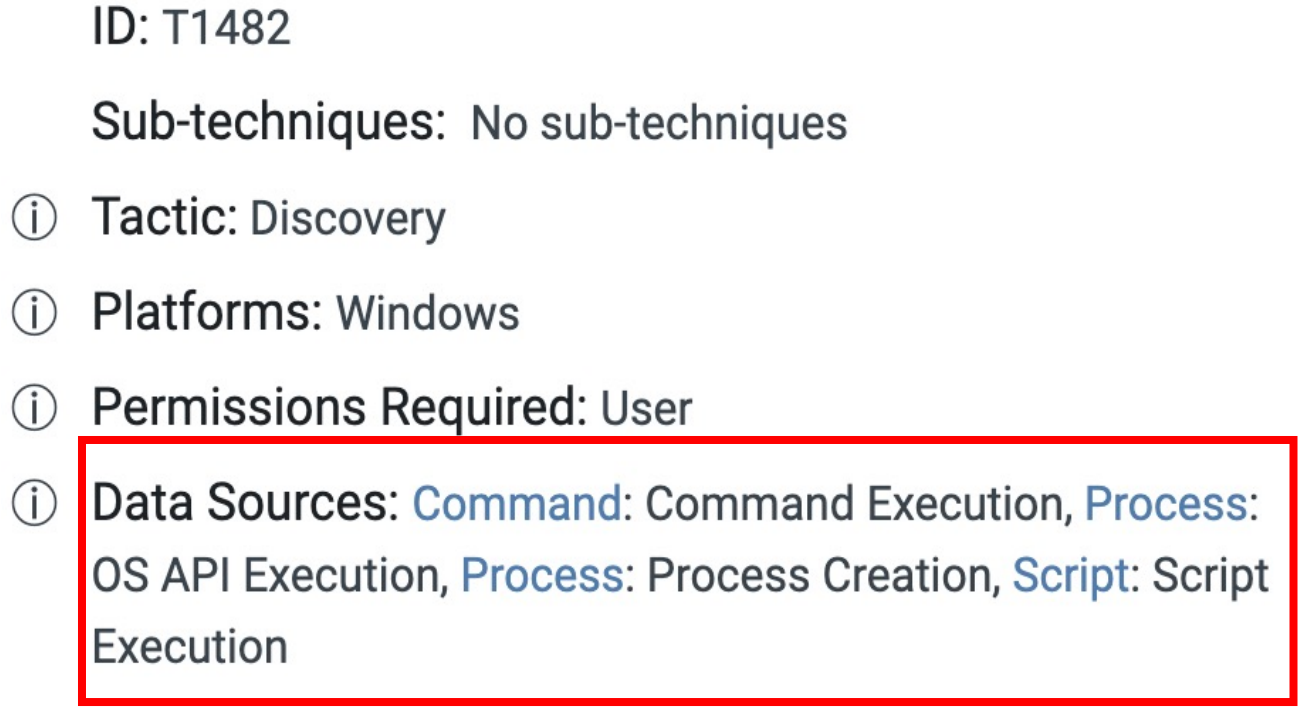
  https://github.com/mitre-attack/attack-datasources

```yaml
- name: Active Directory
  definition: Information associated with the Active Directory service or objects
    (Such as a user, a group, or a workstation) and activity around them.
  collection_layers:
  - host
  - cloud
  platforms:
  - Windows
  - Azure AD
  contributors:
  - ATT&CK
  - CTID
  data_components:
  - name: active directory object creation
    description: An active directory object was created.
    type: activity
    relationships:
    - source_data_element: user
      relationship: created
      target_data_element: ad object
```


MITRE

Data Sources in ATT&CK v9

- No objects yet (pushed to October)
- Updating all data sources to new format
  - Data Source: Component



MITRE

Data Sources as an Object

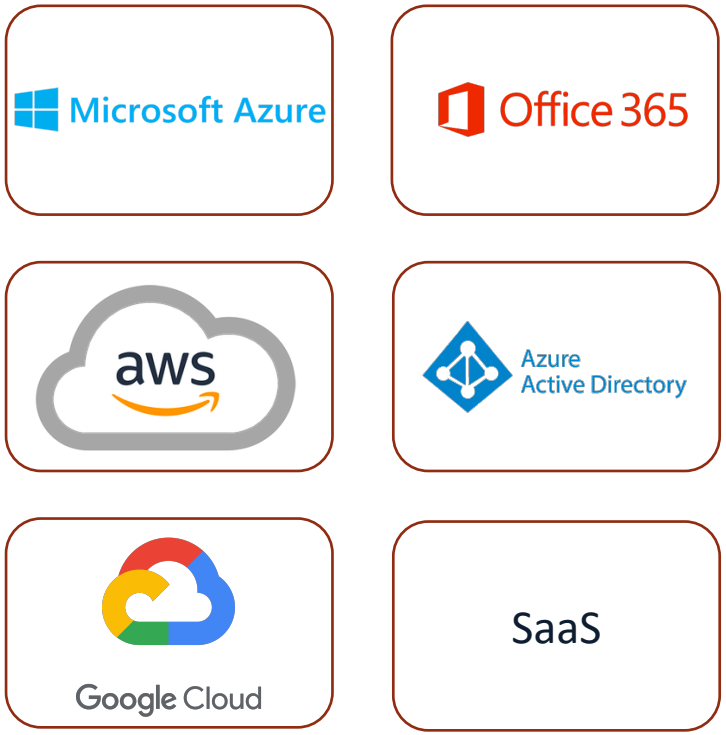
- Slated for Enterprise in October ATT&CK release
- Should flow to other parts of ATT&CK over time
- Will dramatically improve ATT&CK data sources

Field	Data Type	Description
Name	String	The name of the data source based on the main data elements from the recommended telemetry.
Definition	String	A general description of the data source, including all the data elements and their relationships.
Collection Layers	List	A description of data collection locations. This is a key element to start identifying the main physical sources of data.
Platforms	List	The operating system or application where data can be collected within an environment.
Data Components	List of Dictionaries	Group(s) of relationships identified among data elements that define a data source. This information also includes the relationships hence the list of dictionaries.
Contributors	List	Name(s) of the contributor(s) that defined or improved the ATT&CK data source.
References	List	Citation of sources leveraged, or sources that may contribute to an enhanced understanding of a data source.

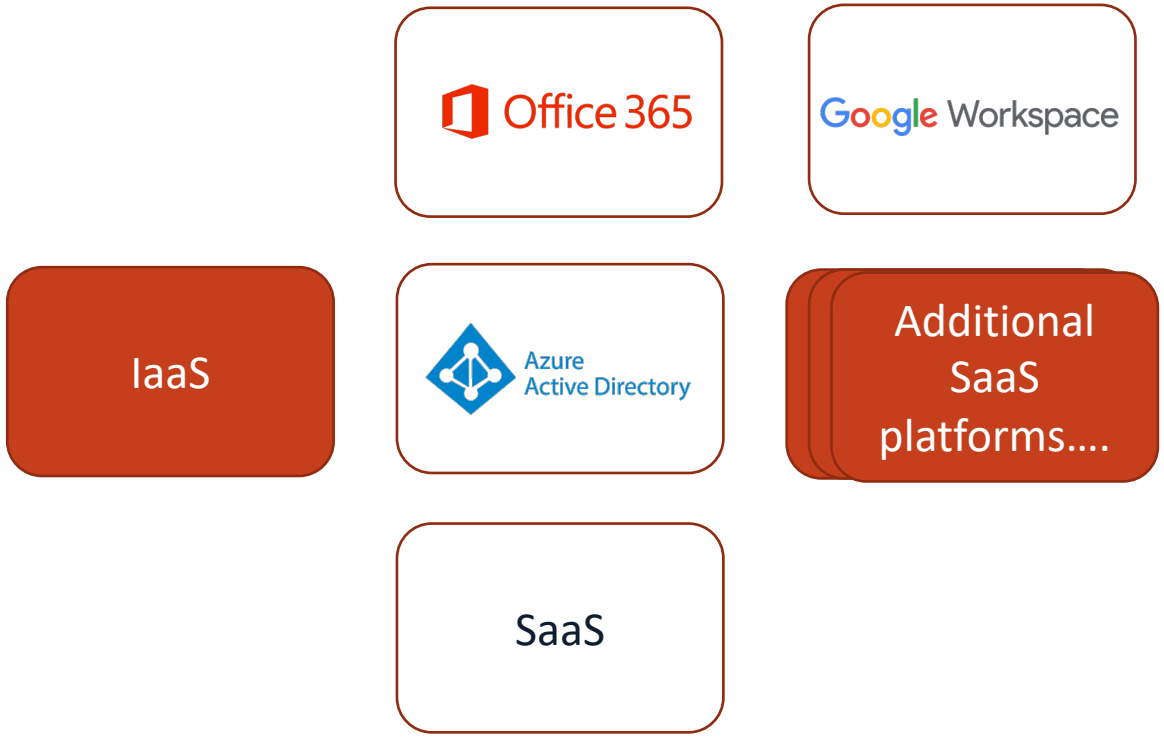
MITRE

ATT&CK for Enterprise (Cloud)

ATT&CK v8

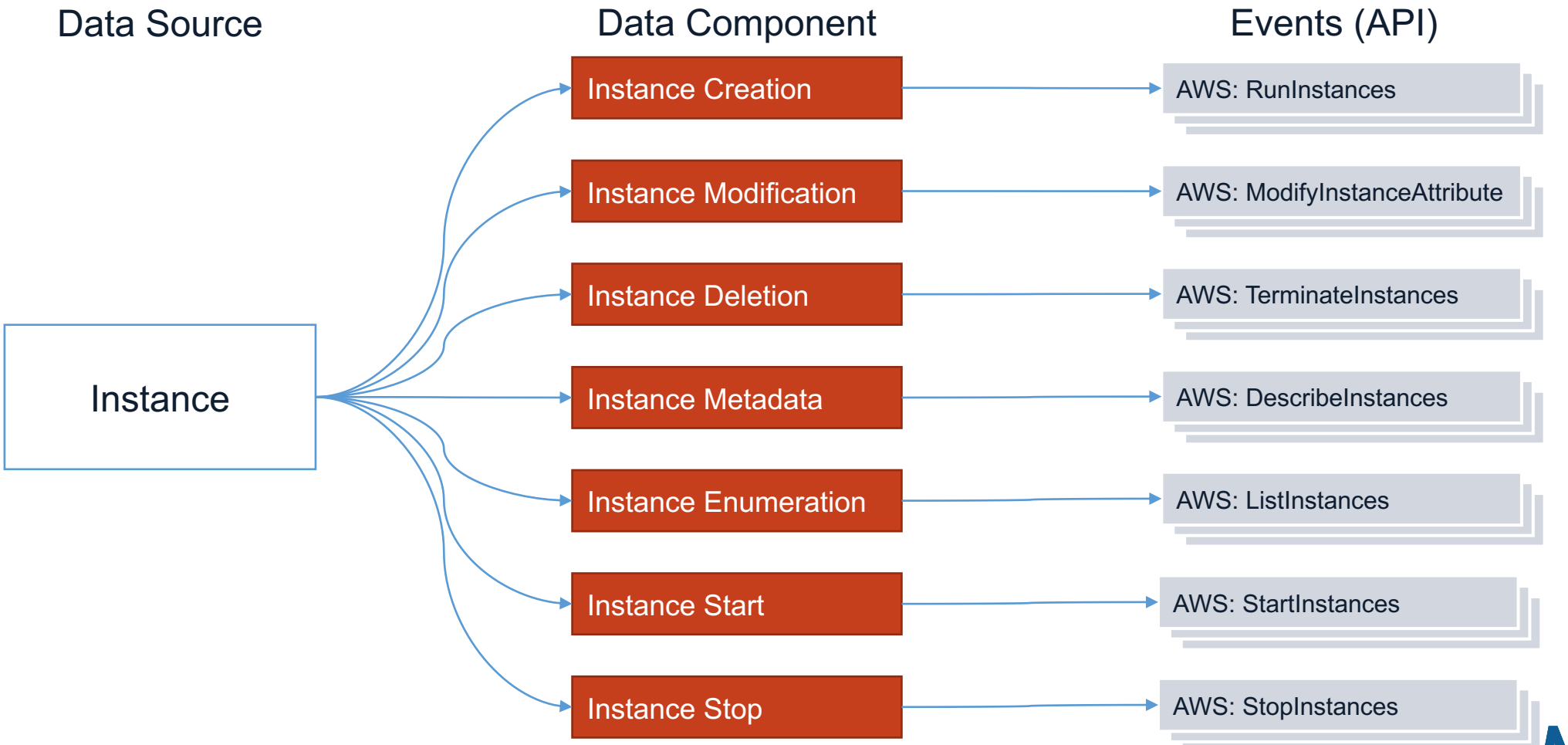


ATT&CK v9



MITRE

Cloud Example Data Source



MITRE

ATT&CK for Enterprise (Containers)

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Using Cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access the K8S API server	Access cloud resources	Data Destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account	Resource Hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Access container service account	Network mapping	Cluster internal networking	Denial of service
Application vulnerability	Application exploit (RCE)		Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access Kubernetes dashboard	Applications credentials in configuration files	
Exposed Dashboard	SSH server running inside container					Instance Metadata API	Writable volume mounts on the host	
							Access Kubernetes dashboard	
							Access tiller endpoint	

Microsoft's ATT&CK-like "Threat Matrix for Kubernetes"

MITRE

ATT&CK for Containers in v9

Containers Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering techniques against container technologies. The Matrix contains information for the Containers platform.

View on the ATT&CK® Navigator

layouts | show sub-techniques | hide sub-techniques | help

Initial Access 3 techniques	Execution 4 techniques	Persistence 4 techniques	Privilege Escalation 4 techniques	Defense Evasion 6 techniques	Credential Access 2 techniques	Discovery 2 techniques	Impact 3 techniques
Exploit Public-Facing Application	Container Administration Command	External Remote Services	Escape to Host	Build Image on Host	Brute Force (3)	Container and Resource Discovery	Endpoint Denial of Service
External Remote Services	Deploy Container	Implant Internal Image	Exploitation for Privilege Escalation	Deploy Container	Password Guessing	Network Service Scanning	Network Denial of Service
Valid Accounts (2)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Impair Defenses (1)	Password Spraying		Resource Hijacking
Default Accounts	Container Orchestration Job	Container Orchestration Job	Container Orchestration Job	Disable or Modify Tools	Credential Stuffing		
Local Accounts	User Execution (1)	Valid Accounts (2)	Valid Accounts (2)	Indicator Removal on Host	Unsecured Credentials (2)		
	Malicious Image	Default Accounts	Default Accounts	Masquerading (1)	Credentials In Files		
		Local Accounts	Local Accounts	Match Legitimate Name or Location	Container API		
				Valid Accounts (2)			
				Default Accounts			
				Local Accounts			

Published at https://medium.com/mitre-engenuity/update-help-shape-att-ck-for-containers-bfcd24515df5

MITRE

ATT&CK for Mobile & ICS

Mobile ATT&CK
Enterprise ATT&CK
ICS ATT&CK

It's just ATT&CK®

- Working towards feature equity with Enterprise
- **ICS** – STIX release timed with Enterprise
  - Cross Domain Groups in October
- **Mobile** – Full release timed with Enterprise
  - Working on sub-techniques

MITRE

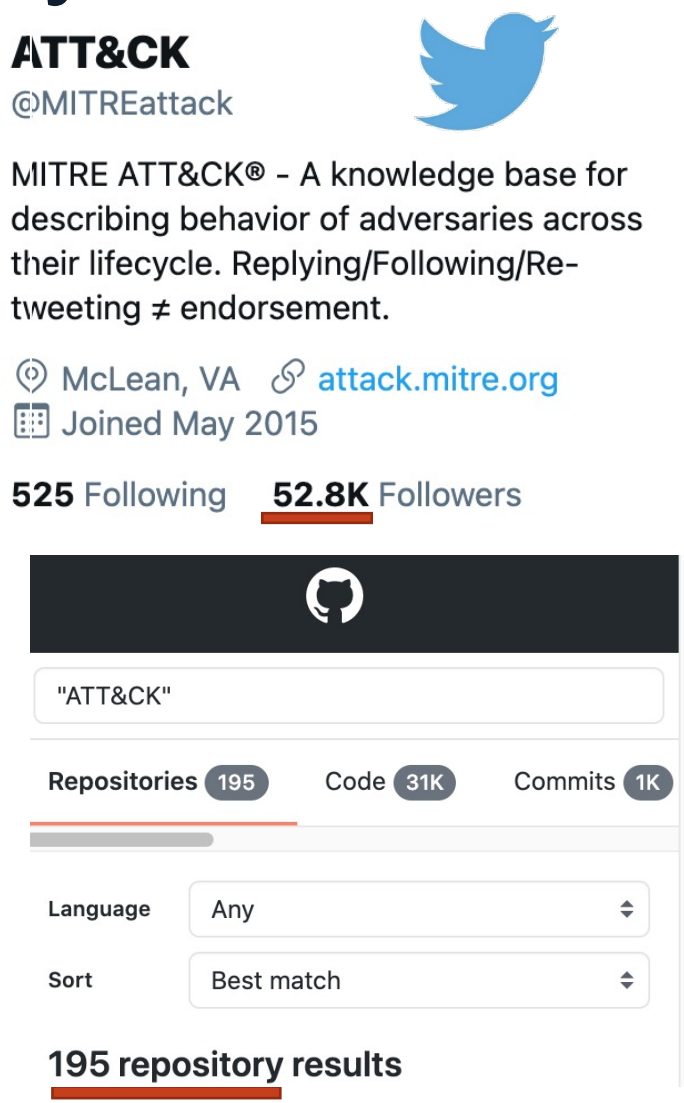
ATT&CKcon 2021

MITRE

Thank you ATT&CK Community!

Individuals + orgs contributing to ATT&CK!

- Christoffer Strömblad
- Alain Homewood, Insomnia Security
- Alan Neville, @abnev
- Alex Hinchliffe, Palo Alto Networks
- Alfredo Abarca
- Allen DeRyke, ICE
- Anastasios Pingios
- Andrew Smith, @jakx_
- Arie Olshtein, Check Point
- AttackIQ
- Aviran Hazum, Check Point
- Avneet Singh
- Barry Shteiman, Exabeam
- Bart Parys
- Bartosz Jerzman
- Brian Prange
- Brian Wiltse @evalstrings
- Bryan Lee
- Carlos Borges, @huntingneo, CIP
- Casey Smith
- Center for Threat-Informed Defense (CTID)
- Chen Erlich, @chen_erlich, enSilo
- Chris Roffe
- Christiaan Beek, @ChristiaanBeek
- Christopher Glyer, FireEye, @cglyer
- Cody Thomas, SpecterOps
- Craig Aitchison
- CrowdStrike Falcon OverWatch
- Cybereason Nocturnus, @nocturnus
- Dan Nutting, @KerberToast
- Daniel Oakley
- Daniil Yugoslavskiy, @yugoslavskiy, Atomic Threat Coverage project
- Daniyal Naeem, @Mrdaniyalnaeem
- Darren Spruell
- Dave Westgard
- David Ferguson, CyberSponse
- David Lu, Tripwire
- David Routin
- Deloitte Threat Library Team
- Diogo Fernandes
- Doron Karmi, @DoronKarmi
- Drew Church, Splunk
- Ed Williams, Trustwave, SpiderLabs
- Edward Millington
- Elastic
- Elger Vinicius S. Rodrigues, @elgervinicius, CYBINT Centre
- Elia Florio, Microsoft
- Elly Searle, CrowdStrike — contributed to tactic definitions
- Emile Kenning, Sophos
- Emily Ratliff, IBM
- Eric Kuehn, Secure Ideas
- Erika Noerenberg, @gutterchurl, Carbon Black
- Erye Hernandez, Palo Alto Networks
- ESET
- Expel
- Felipe Espósito, @Pr0teus
- Filip Kafka, ESET
- FS-ISAC
- George Allen, VMware Carbon Black
- Hans Christoffer Gaardløs
- Heather Linn
- Ibrahim Ali Khan
- Itamar Mizrahi, Cymptom
- Itzik Kotler, SafeBreach
- Ivan Sinyakov
- Jacob Wilkin, Trustwave, SpiderLabs
- Jacques Pluviose, @Jacqueswildy_IT
- James Dunn, @jamdunnDFW, EY
- Jan Miller, CrowdStrike
- Jan Petrov, Citi
- Janantha Marasinghe
- Jannie Li, Microsoft Threat Intelligence Center (MSTIC)
- Jared Atkinson, @jaredcatkinson
- Jean-Ian Boutin, ESET
- Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services)
- Jeremy Galloway
- Jesse Brown, Red Canary
- Jimmy Astle, @AstleJimmy, Carbon Black
- Johann Rehberger
- John Lambert, Microsoft Threat Intelligence Center
- John Strand
- Jon Sternstein, Stern Security
- Jonathan Shimonovich, Check Point
- Jose Luis Sánchez Martinez
- Josh Abraham
- Josh Campbell, Cyborg Security, @cyb0rgsecur1ty
- Josh Day, Gigamon
- Justin Warner, ICEBRG
- Jörg Abraham, EclecticIQ
- Kaspersky
- Kobi Eisenkraft, Check Point
- Lab52 by S2 Grupo
- Lee Christensen, SpecterOps
- Leo Loobeek, @leoloobeek
- Leo Zhang, Trend Micro
- Loic Jaquemet
- Lorin Wu, Trend Micro
- Lucas da Silva Pereira, @vulcanunsec, CIP
- Lukáš Štefanko, ESET
- Marc-Etienne M.Léveillé, ESET
- Mark Wee
- Martin Jirkal, ESET
- Martin Smolár, ESET
- Mathieu Tartare, ESET
- Matias Nicolas Porolli, ESET
- Matt Graeber, @mattifestation, SpecterOps
- Matt Kelly, @breakersall
- Matt Snyder, VMware
- Matthew Demaske, Adaptforward
- Matthew Molyett, @s1air, Cisco Talos
- Matthieu Faou, ESET
- McAfee
- Menachem Shafran, XM Cyber
- Michael Cox
- Michal Dida, ESET
- Microsoft Threat Intelligence Center (MSTIC)
- Mike Kemmerer
- Milos Stojadinovic
- Mnemonic
- Netskope
- Nick Carr, FireEye
- Nik Seetharaman, Palantir
- Nishan Maharjan, @loki248
- Oddvar Moe, @oddvarmoe
- Ofir Almkias, Cybereason
- Ohad Mana, Check Point
- Oleg Kolesnikov, Securonix
- Oleg Skulkin, Group-IB
- Oleksiy Gayda
- Omkar Gudhate
- Patrick Campbell, @pjcampbe11
- Paul Speulstra, AECOM Global Security Operations Center
- Pedro Harrison
- Phil Stokes, SentinelOne
- Praetorian
- Prashant Verma, Paladion
- Rahmat Nurfauzi, @infosecn1nja, PT Xynexis International
- Red Canary
- RedHuntLabs, @redhuntlabs
- Ricardo Dias
- Richard Gold, Digital Shadows
- Richie Cyrus, SpecterOps
- Rick Cole, FireEye
- Rob Smith
- Robby Winchester, @robwinchester3
- Robert Falcone
- Robert Simmons, @MalwareUtkonos
- Rodrigo Garcia, Red Canary
- Romain Dumont, ESET
- Ryan Becwar
- Ryan Benson, Exabeam
- Sahar Shukrun
- Saisha Agrawal, Microsoft Threat Intelligent Center (MSTIC)
- SarathKumar Rajendran, Trimble Inc
- Scott Knight, @sdotknight, VMware Carbon Black
- Scott Lundgren, @5twenty9, Carbon Black
- Sebastian Salla, McAfee
- Sekhar Sarukkai; Prasad Somasamudram; Syed Ummar Farooqh (McAfee)
- Sergey Persikov, Check Point
- Shailesh Tiwary (Indian Army)
- Shane Tully, @securitygypsy
- Stefan Kanthak
- Steven Du, Trend Micro
- Sudhanshu Chauhan, @Sudhanshu_C
- Sunny Neo
- Suzy Schapperle - Microsoft Azure Red Team
- Swapnil Kumbhar
- Swetha Prabakaran, Microsoft Threat Intelligence Center (MSTIC)
- Sylvain Gil, Exabeam
- Sébastien Ruel, CGI
- Tatsuya Daitoku, Cyber Defense Institute, Inc.
- Teodor Cimpoesu
- Tim MalcomVetter
- Toby Kohlenberg
- Tom Ueltschi @c_APT_ure
- Tony Lambert, Red Canary
- Travis Smith, Tripwire
- Trend Micro Incorporated
- Tristan Bennett, Seamless Intelligence
- Valerii Marchuk, Cybersecurity Help s.r.o.
- Veeral Patel
- Vikas Singh, Sophos
- Vinayak Wadhwa, Lucideus
- Vincent Le Toux
- Walker Johnson
- Wayne Silva, F-Secure Countercept
- Wes Hurd
- Ye Yint Min Thu Htut, Offensive Security Team, DBS Bank
- Yonatan Gotlib, Deep Instinct



Adam Pennington
@_whatshisface

ATT&CK®

attack@mitre.org
@MITREattack

MITRE