sysdig | aws

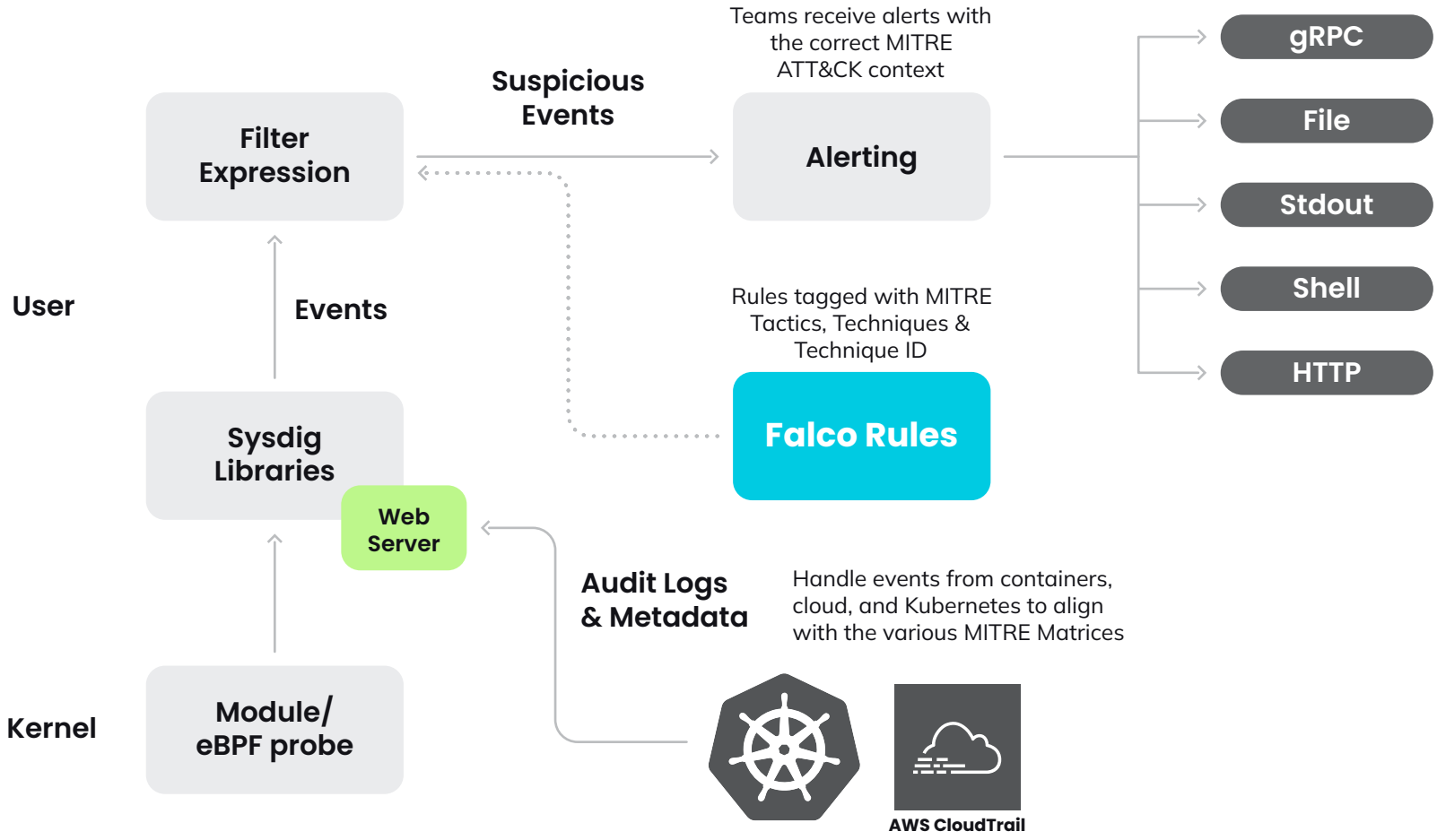
E-BOOK

AWS Cloud Detection and Response Matrix for MITRE ATT&CK

Table of Contents

In today's cloud-driven world, time is the ultimate currency, and every second counts. With attacks capable of compromising systems and tarnishing reputations in as little as 10 minutes, the stakes have never been higher. This reality demands a paradigm shift in how we approach security, requiring new strategies, technologies, and a mindset attuned to the speed of the cloud. The MITRE ATT&CK framework stands as a beacon for cybersecurity professionals, offering a detailed, actionable understanding of attacker behaviors and techniques. It empowers security teams to proactively secure their assets in an ever-evolving landscape of cyber threats.

Falco, the open source standard for real-time threat detection across containers, Kubernetes, and cloud services, ensures comprehensive visibility within your cloud-native environment. It detects threats at runtime, positioning you to act swiftly against potential breaches. This immediacy is crucial, aligning with the "Secure Every Second" ethos that in the cloud, timing is not just critical; it's everything.



Cloud security and compliance represent a shared responsibility between AWS and its customers. AWS secures the cloud infrastructure, offering unparalleled security and compliance adherence. Customers, however, bear the responsibility for securing their data and applications within the cloud. This dual approach underscores the necessity for innovative security solutions that operate at cloud speed.

This eBook demonstrates how Falco's adaptable rules engine maps directly to MITRE ATT&CK tactics and techniques for AWS, providing a robust detection framework. By correlating container workload rules with AWS CloudTrail audit rules, Falco delivers end-to-end security coverage for your AWS cloud environment.

With the included cheatsheet, you'll quickly understand which Falco rules shield you from various attack vectors, enhancing your ability to detect, respond to, and preempt malicious activities. This resource not only aids in thwarting attacks, but also in identifying potential vulnerabilities before they can be exploited.

In the era of cloud computing, understanding that cloud attacks present unique challenges in terms of urgency, complexity, and stakes is vital. This eBook bridges the awareness gap, positioning Sysdig as a top consideration for Cloud Detection & Response (CDR). Now is the time to rethink security strategies to protect business innovation at the speed of the cloud. Let's embrace new thinking and technologies to ensure that the cloud remains a safe environment for advancement and growth.

In the era of cloud computing, understanding that cloud attacks present unique challenges in terms of urgency, complexity, and stakes is vital.

CHAPTER 01

Understanding the Cloud & Container Matrices

This eBook will cover the MITRE ATT&CK Framework for Cloud & Containers. One important note is that the team at MITRE has developed several different matrices to address the unique risks associated with adversaries in the cloud, in containerized workloads as well as on mobile devices. As a result, we will provide our insights through the lens of the two following matrices:

Cloud Matrix

attack.mitre.org/matrices/enterprise/cloud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Drive-by compromise	Serverless Execution	Account Manipulation	Domain Policy Modification	Use Alternate Auth Material	Brute Force	Network Sniffing	Internal Spear Phishing	Data from Information Repositories	Transfer Data to Cloud Account	Account Access Removal
Exploit Public-Facing Application	User Execution	Office Application Startup	Event Triggered Execution	Modify Cloud Compute Resources	Forge Web Credentials	Cloud Service Discovery	Taint Shared Content	Automated Collection		Data Destruction
Phishing		Create Account	Valid Accounts	Impair Defenses	Modify Auth Process	Network Service Discovery	Use Alternate Auth Material	Data from Cloud Storage		Defacement
Trusted Relationship		Event Triggered Execution		Indicator Removal	MFA Request Generation	Cloud Infrastructure Discovery		Data Staged		Data Encrypted for Impact
Valid Accounts		Valid Accounts		Hide Artifacts	Network Sniffing	Password Policy Discovery		Email Collection		Endpoint Denial of Service
		Modify Auth Process		Domain Policy Modification	Unsecured Credentials					Resource Hijacking
		Implant Internal Image		Unused / Unsupported Cloud Regions	Steal App Access Tokens					Network Denial of Service

Container Matrix

attack.mitre.org/matrices/enterprise/containers

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
External Remote Services	Container Administration Command	External Remote Services	Escape to Host	Build Image on Host	Brute Force	Container & Resource Discovery	Use Alternate Auth Material	Endpoint Denial of Service
Exploit Public-Facing Application	User Execution	Implant Internal Image	Exploitation for Privilege Escalation	Deploy Container	Steal Application Access Token	Network Service Discovery		Network Denial of Service
Valid Accounts	Deploy Container	Valid Accounts	Valid Accounts	Use Alternate Auth Method	Unsecured Credentials	Permission Groups Discovery		Resource Hijacking
	Scheduled Task/Job	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal				
				Impair Defenses				
				Masquerading				
				Valid Accounts				

CHAPTER 02

Initial Access

What is it?

The initial access tactic (TA0001) consists of techniques that use various entry vectors to gain a foothold within a network. Techniques include compromising credentials, exploiting bugs on public servers, and leveraging weak configurations.

Why is it a threat?

Initial access by an unauthorized user can lead to other attack tactics, including persistence, privilege escalation, and credential access.

Cloud Rule

T1078 (Valid Accounts) - Console Login Through Assumed Role (GitHub)

Assuming a role involves using a set of temporary security credentials that you can use to access AWS resources that you might not normally have access to. These temporary credentials consist of an access key ID, a secret access key, and a security token.

Container Rule

T1190 (Exploit Public-Facing Application) - DB program spawned process (GitHub)

Falco can detect when a database-server related program spawned a new process other than itself. This shouldn't occur and is a follow up from some SQL injection attacks.

DIG DEEPER

AWS Lambda function - Initial access in cloud attacks

READ THE BLOG →

CHAPTER 03

Execution

What is it?

The execution tactic (TA0002) consists of techniques used by adversaries to run malicious code on a local or remote system to gain access to the infrastructure or accomplish broader attack tactics, like discovery or data exfiltration.

Why is it a threat?

Adversaries could use execution to run malicious code, like cryptominers or backdoors, in your environment. If they gain initial access, detecting execution is critical to stop attacks. For example, malicious container images uploaded to public repositories may be run inadvertently, facilitating threat activities like executing attack code and cryptomining.

Cloud Rule

T1648 (Serverless Execution) - Create Lambda Function (GitHub)

Adversaries may abuse serverless computing, integration, and automation services to execute arbitrary code in cloud environments. AWS Lambda is a serverless, event-driven compute service that lets you run your application code without provisioning or managing servers.

Container Rule

T1610 (Deploy Container) - Launch Excessively Capable Container (GitHub)

Adversaries may deploy a container into an environment to facilitate execution or evade defenses. Falco detects containers that have started with a powerful set of capabilities. Exceptions should only be made for known, trusted images.

DIG DEEPER

Detect the containers' escape capabilities with Falco

READ THE BLOG →

CHAPTER 04

Persistence

What is it?

The persistence tactic (TA0003) consists of techniques that adversaries could use to potentially maintain access across your cloud environment.

Why is it a threat?

Adversaries may use a new user with credentials or create a new container image to use as a backdoor to maintain access to your environment. If persistence is obtained, they are able to autonomously access your cloud environment, or the resource in it, without repeatedly performing the first steps of initial access.

Cloud Rule

T1136 (Create Account) - Create AWS user (GitHub)

If they gain initial access, adversaries may create an account to maintain access to victim systems. With a sufficient level of access, creating such accounts may be used to establish secondary credentialed access that does not require persistent remote access tools to be deployed on the system.

Container Rule

T1053 (Scheduled Task/Job) - Schedule Cron Jobs (GitHub)

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time.

CHAPTER 05

Privilege Escalation

What is it?

The privilege escalation tactic (TA0004) consists of techniques that allow an adversary to potentially obtain a higher level of permissions on your cloud account.

Why is it a threat?

Adversaries could escalate the privilege level in a system by triggering functions in your AWS environment or using credentials found in the system. An adversary could escalate privileges in your cloud account to impersonate roles and find a way to get even more permissions. In some cases, this could lead to host takeover or a compromise of your cloud account.

Cloud Rule

T1546 (Event Triggered Execution) - Update Lambda Function Configuration (GitHub)

Adversaries may elevate privileges using system mechanisms that trigger execution based on specific events. Cloud environments like AWS support various functions and services, such as Lambda or EventBridge, that can be invoked in response to specific cloud events.

Container Rule

T1611 (Escape to Host) - Detect release_agent File Container Escapes (GitHub)

Adversaries may break out of a container to gain access to the underlying host. This could allow an unauthorized user access to other containerized resources from the host level or to the host itself.

DIG DEEPER

Detecting MITRE ATT&CK: Privilege escalation with Falco

READ THE BLOG →

CHAPTER 06

Defense Evasion

What is it?

The defense evasion tactic (TA0005) consists of techniques an adversary may use to bypass the detection mechanisms in place and avoid the other defense mechanisms deployed in the environment.

Why is it a threat?

There are many defensive functions and mechanisms provided by cloud providers, like AWS, that adversaries try to evade. Adversaries may try to turn off or delete log files that track user activity or specifically target access points that are lightly defended. If they evade these built-in defenses, they may be able to perform access and actions undetected.

Cloud Rule

T1535 (Unused/Unsupported Cloud Regions) - Run Instances in Non-approved Region (GitHub)

Adversaries may create cloud instances in unused geographic service regions in order to evade detection. Access is usually obtained through compromising accounts used to manage cloud infrastructure.

Container Rule

T1070 (Indicator Removal) - Clear Log Activities (GitHub)

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions.

DIG DEEPER

Detecting MITRE ATT&CK: Defense evasion techniques with Falco

READ THE BLOG →

CHAPTER 07

Credential Access

What is it?

The credential access tactic (TA0006) consists of techniques that can collect credentials which provide access or control over systems and services within a cloud environment.

Why is it a threat?

Accessing credentials could enable a more aggressive attack, and they can be used for other alignments like lateral movement and privilege escalation. Adversaries can use credentials to impair defenses, compromise data, or carry out activity like cryptomining.

Cloud Rule

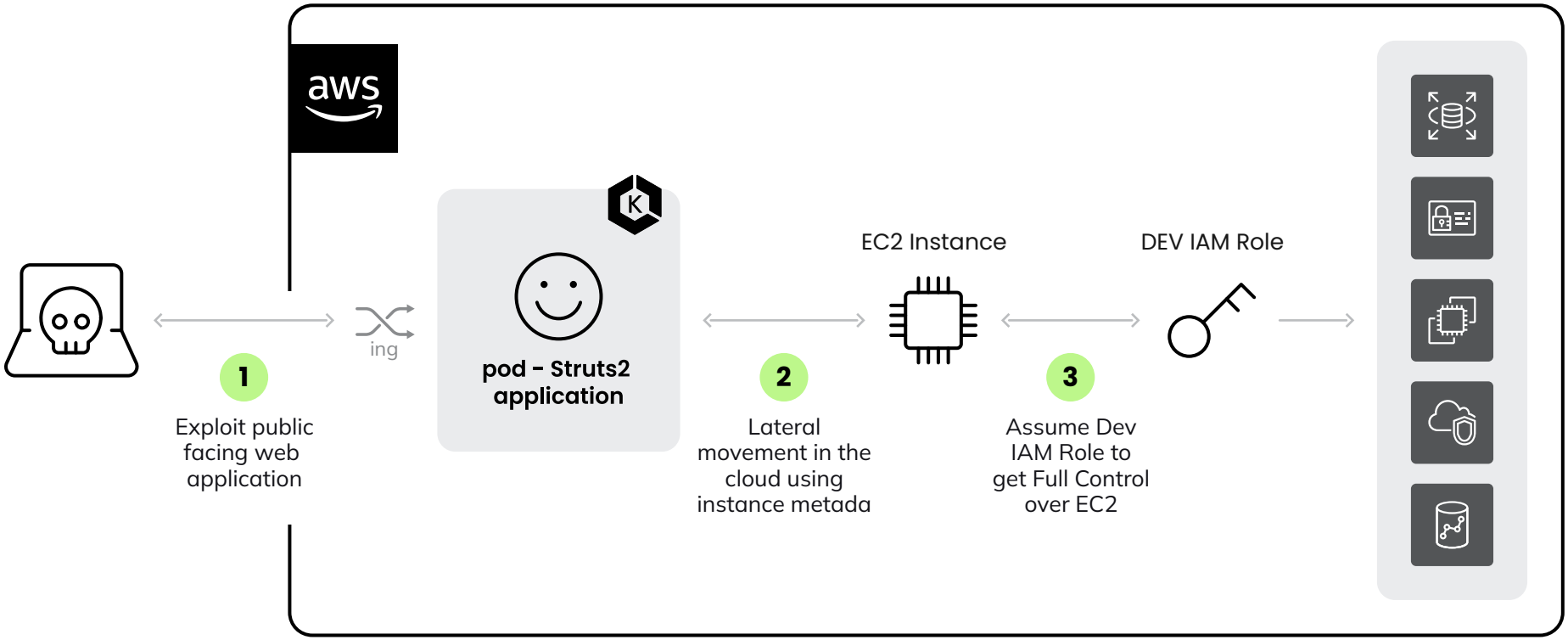
T1556 (Modify Authentication Process) - Deactivate MFA for Root User (GitHub)

Unauthorized users could modify a part of this process to either reveal credentials or bypass authentication mechanisms, such as Multi-Factor Authentication (MFA). Compromised credentials or IAM (Identity & Access Management) permissions may be used to further bypass access controls within the cloud environment.

Container Rule

T1552 (Unsecured Credentials) - Search Private Keys or Passwords (GitHub)

Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g., Bash History), operating system or application-specific repositories (e.g., Credentials in Registry), or other specialized files/artifacts (e.g., Private Keys).



DIG DEEPER

TeamTNT stealing credentials using EC2 Instance Metadata

READ THE BLOG →

CHAPTER 08

Discovery

What is it?

The discovery tactic (TA0007) consists of techniques that allow adversaries to get information and general knowledge about your environments, systems and applications deployed, and available users

Why is it a threat?

Adversaries may gain a deeper understanding of your AWS infrastructure through discovery and see what systems are running. They could use this information to identify vulnerabilities or where to access data and information.

Cloud Rule

T1580 (Cloud Infrastructure Discovery) - List Buckets (GitHub)

An adversary may attempt to discover infrastructure and resources that are available within an infrastructure-as-a-service (IaaS) environment. This includes compute service resources such as instances, virtual machines, and snapshots, as well as resources of other services, including the storage and database services. One way this may be done is by listing public S3 buckets.

Container Rule

T1046 (Network Service Discovery) - Launch Suspicious Network Tool in Container (GitHub)

Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto the host or container.

DIG DEEPER

Proxyjacking Has Entered The Chat

READ THE BLOG →

CHAPTER 09

Lateral Movement

What is it?

The lateral movement tactic (TA0008) consists of techniques adversaries use to move through multiple systems and accounts in your environment and explore your network to find their target.

Why is it a threat?

If your environment is compromised, adversaries may pivot through your systems to find other possible vulnerabilities to exploit. They can use lateral movement to accomplish their objectives even when they do not initially have access to their end goal. By moving within your network, they may search for other areas to exploit in addition to their primary target.

Cloud Rule

T1080 (Taint Shared Content) - Update Lambda Function Code (GitHub)

Adversaries may deliver payloads to remote systems by adding content to shared storage locations, such as an internal code repository. Content stored services may be tainted by adding malicious programs, scripts, or exploit code to otherwise valid Lambda functions. The malicious portion could be executed to run the adversary's code on a remote instance. Adversaries may use tainted shared content to move laterally.

Container Rule

T1550 (Use Alternate Authentication Material) - Read sensitive file untrusted (GitHub)

Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, to move laterally within an environment and bypass normal system access controls. Any attempt to read the above sensitive files should be treated as suspicious behavior where an attacker is attempting to move laterally.

DIG DEEPER

Cloud lateral movement: Breaking in through a vulnerable container

READ THE BLOG →

CHAPTER 10

Collection

What is it?

The collection tactic (TA0009) consists of techniques adversaries use to gather and wrap up information found within compromised systems in your cloud account.

Why is it a threat?

Adversaries may use a variety of collection techniques to target data and information. They often rely on automated techniques for gathering internal data to speed up the operation. Combined with tactics like exfiltration, valuable company assets like files and secrets, sensitive data, and archives can be compromised.

Cloud Rule

T1530 (Data from Cloud Storage) - Put Bucket ACL (GitHub)

Many cloud service providers offer solutions for online data object storage, such as Amazon S3. These solutions differ from other storage solutions (such as SQL or Elasticsearch) in that there is no overarching application. Data from these solutions can be retrieved directly using the cloud provider's APIs.

Falco can detect when an adversary sets the permissions on an existing bucket using Access Control Lists (ACLs). If an adversary managed to make the bucket publicly accessible, they may collect sensitive data from these cloud storage solutions.

DIG DEEPER

SCARLETEEL: Operation leveraging Terraform, Kubernetes, and AWS for data theft

READ THE BLOG →

CHAPTER 11

Exfiltration

What is it?

The exfiltration tactic (TA0010) consists of techniques used by adversaries to potentially access files, backups, and corporate information from a compromised network and send them to a different destination controlled by the attacker.

Why is it a threat?

Adversaries may move the data found in your cloud environment to another cloud account they control on the same service, avoiding typical network-based exfiltration detection. Attackers may then sell this sensitive information or charge the targeted organization a ransom to keep the data secret. Unfortunately, paying the attacker does not always ensure the data and industry secrets are not exposed publicly.

Cloud Rule

T1537 (Transfer Data to Cloud Account) - Interpreted procs outbound network activity (GitHub)

Adversaries may potentially exfiltrate data by transferring it, including backups of cloud environments, to another cloud account they control on the same service to avoid file transfers/ downloads and network-based exfiltration detection.

DIG DEEPER

What is a Data Leak?

LEARN MORE →

CHAPTER 12

Impact

What is it?

The impact tactic (TA0040) consists of techniques that adversaries use to disrupt availability or compromise integrity of your systems and data by manipulating business and operational processes.

Why is it a threat?

Adversaries may use these techniques if they have compromised your account through other tactics. If they have access to your systems, they can encrypt, destroy, or corrupt your data, disrupt the availability of corporate services, or alter business processes to benefit their goals. This may be in conjunction with defense evasion to corrupt and obfuscate their paths and what data they took, or it can be solely with the goal of destruction and damage.

Cloud Rule

T1485 (Data Destruction) - Delete Group (GitHub)

Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives.

Container Rule

T1496 (Resource Hijacking) - Detect cryptominers using the Stratum protocol (GitHub)

Adversaries may leverage the resources of co-opted systems in order to solve resource-intensive problems, such as cryptomining, which may impact system availability.

DIG DEEPER

The Real Cost of Cryptomining: Adversarial Analysis of TeamTNT

READ THE BLOG →

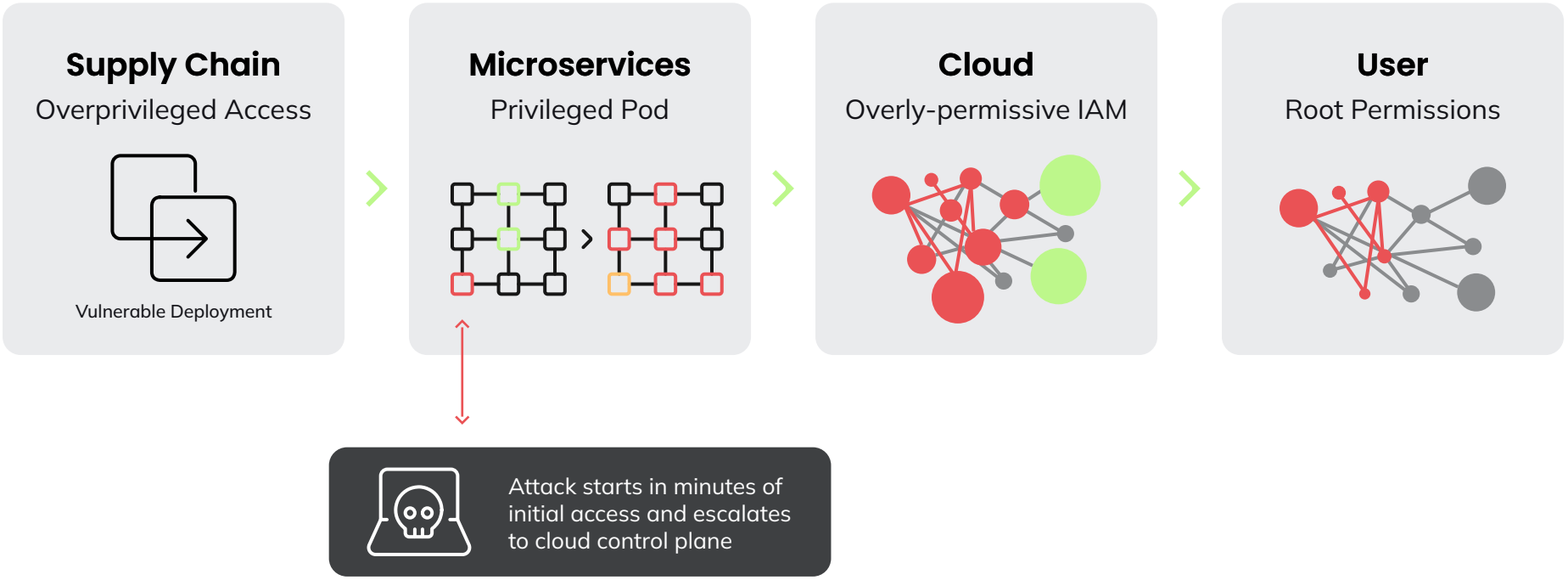
CHAPTER 13

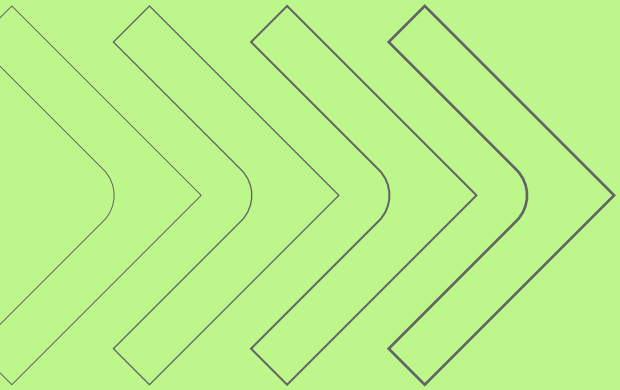
Takeaways

Organizations are rapidly moving their infrastructure and applications to the cloud driven by cost savings, flexibility, and scalability benefits. Adversary tactics and techniques have followed. If an unauthorized user gains access to your cloud environment or container, they can escalate and move to other cloud resources or workloads to exploit further vulnerabilities.

Legacy security solutions not designed to protect cloud-native environments may offer no visibility into cloud and containers, leaving you exposed to threats. A defensive cloud security posture as well as detection and response built for the cloud are critical in stopping and preventing attacks before they cause damage.

By leveraging Falco rules and the MITRE ATT&CK framework, you can detect and respond to threats in your cloud and containers without wasting time. With Falco rules mapped to MITRE ATT&CK tactics, you will have a head start on potential attack vectors and know which rules will best protect you against the most prominent tactics. You and your cybersecurity team can use this guide to manage risk and strengthen the security of your AWS infrastructure, ensuring you will be prepared to face any threat that comes your way.





Additional Resources

Thank you for reading the AWS Cloud Detection and Response Matrix for MITRE ATT&CK eBook! It offers valuable insights into how you can align open source Falco rules with MITRE ATT&CK framework to improve threat response capabilities.

Check out our Sysdig articles for more information on how you can use Falco and MITRE ATT&CK to enhance your security posture, and gain greater visibility into your infrastructure, improve incident response times, and better protect your organization from advanced threats

CHECK OUT THE BLOG →

sysdig

E-BOOK

EBK-006 REV. B 04/24

About Sysdig

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. Sysdig correlates signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

Sysdig. Secure Every Second.