# Community Brand & Identity Guidelines

Looking for our logo? Want to make sure you reference The Falco Project correctly? This handy grouping of information will help you augment your **visual content** and **written content** that can be used publicly.

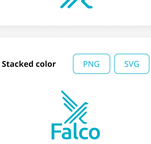
Falco is an open source security project whose brand and identity are governed by the **Cloud Native Computing Foundation**.

## Visual content

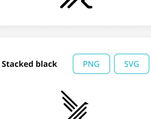
### Project Mark

Wherever possible, the horizontal teal logo is the preferred logo to use. If you need all the logos, **download the logo pac**.

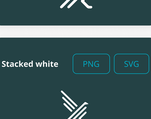
Horizontal color — PNG SVG



Horizontal black — PNG SVG



Horizontal white — PNG SVG



Icon color — PNG SVG



Icon black — PNG SVG



Icon white — PNG SVG



Stacked color — PNG SVG

Stacked black — PNG SVG



Stacked white — PNG SVG



### Project Font & Typestyle

Falco prefers Ubuntu font. When you reference us, please capitalize the first letter of our name, just as you would your own.

✓ Falco, The Falco Project

✗ falco, the falco project, the Falco project

### Project Colors

**Teal**
RGB 0 174 199
PMS 3125

**Cool grey**
RGB 83 86 90
PMS 11

**Black**
RGB 0 0 0

**White**
RGB 255 255 255

### Project Slide Templates

Want to speak about Falco at a meetup or conference? Make it easier by using these templates and/or scripted slides. You can even watch this video as a training tool.

**Empty Falco slide template**
11 SLIDES · LAST MODIFIED MAR 20, 2023 →

**Turnkey, scripted Falco slides**
11 SLIDES · LAST MODIFIED MAR 20, 2023 →

**Example video delivery**
1 VIDEO · LAST MODIFIED MAR 20, 2023 →

### Falco diagrams

Find all the SVG and PNG format diagrams used throughout the Falco website on this repository.

**Diagrams developed in SVG and PNG**
10 DIAGRAMES · LAST MODIFIED MAR 20, 2023 →

## Written content

### Project Facts

As of April, 2023, Falco has:

- 60M+ Downloads in Docker
- 40+ Integrations
- 5,800+ GitHub stars
- 170 contributors

### Project Origin

Falco was created as a cloud native runtime security project by Sysdig. The project was contributed to the CNCF in October 2018. Falco is a CNCF incubating project with more than 170 individual contributors around the world.

### Project Description

Cloud Native Runtime Security

### Project Blurbs

**25-word description**

Falco is the open source standard for threat detection across Kubernetes, containers, hosts and the cloud to detect and stop attacks.

**50-word description**

Falco is the open source standard for threat detection across Kubernetes, containers, hosts and the cloud. Runtime security with Falco provides visibility into unexpected behavior, config changes, intrusions, and data theft in real time, so you can detect and stop attacks. Falco uses state-of-the-art eBPF technology for workload visibility.

**100-word description**

Falco is the open source standard for threat detection across Kubernetes, containers, hosts and the cloud. Runtime security with Falco provides visibility into unexpected behavior, config changes, intrusions, and data theft in real time, so you can detect and stop attacks. Falco uses state-of-the-art eBPF technology to monitor workloads, and can protect cloud services such as AWS CloudTrail, GitHub or Okta. Falco is supported by a global multi-vendor ecosystem, and is hosted by the CNCF, home of the Kubernetes project.

### Project Encouraged Phrasing

The phrases below are effective ways of messaging Falco's value add. Use them when writing or speaking publicly about Falco.

Even when processes are in place for vulnerability scanning and implementing pod security and network policies, not every risk will be addressed. You still need mechanisms to confirm these security barriers are effective, help configure them, and provide with a last line of defense when they fail.

**Falco is the open source standard for threat detection**
This statement refers to Falco as a CNCF incubating project with widespread adoption and broad community leadership.

**Falco is a rules engine that powers runtime security**
This term refers to the concept that Falco is a stateless processing engine. A large amount of data comes into the engine, but meticulously crafted security alerts come out. It reasons about signals coming from a system at runtime, and can alert if a threat is detected.

**Real time threat detection**
This refers to an event that occurs with something unusual, concerning, or odd occurs. We can associate anomalies with unwanted behavior, config changes, intrusions and data theft, and alert in their presence.

**Detection tooling**
Falco does not prevent unwanted behavior. Falco however alerts when unusual behavior occurs. This is commonly referred to as detection or forensics.