

# Detecting Anomalies and Events with Packetbeat

---

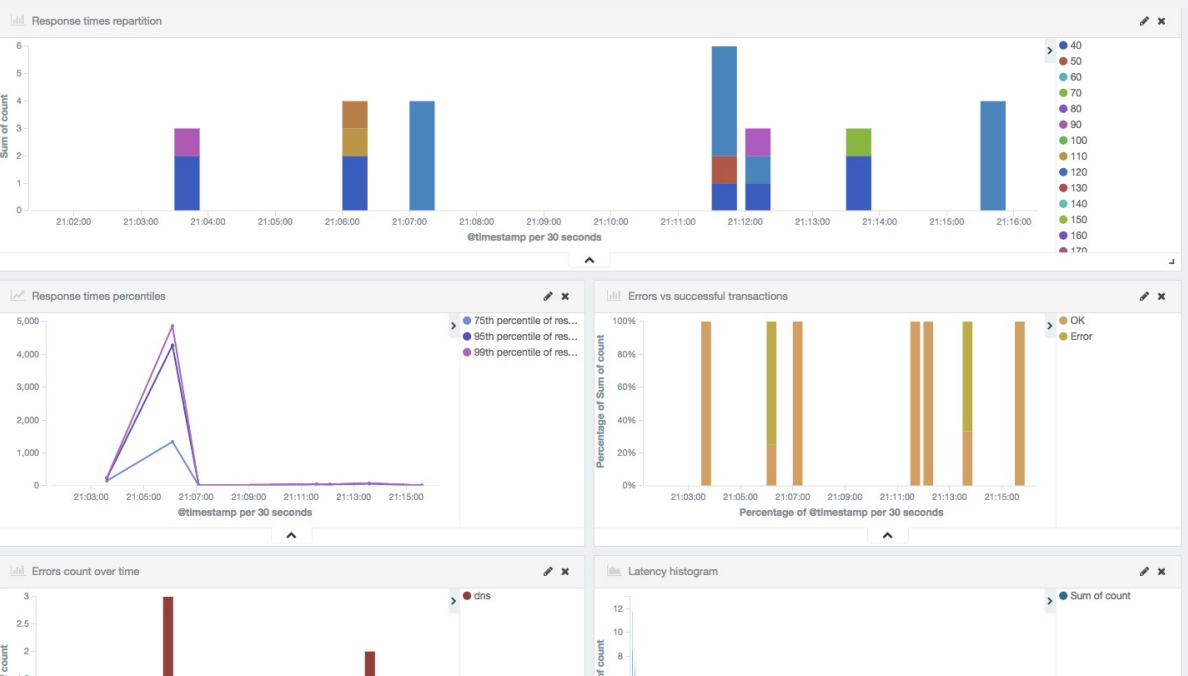


**Owen Dubiel**

Information Security Professional







[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

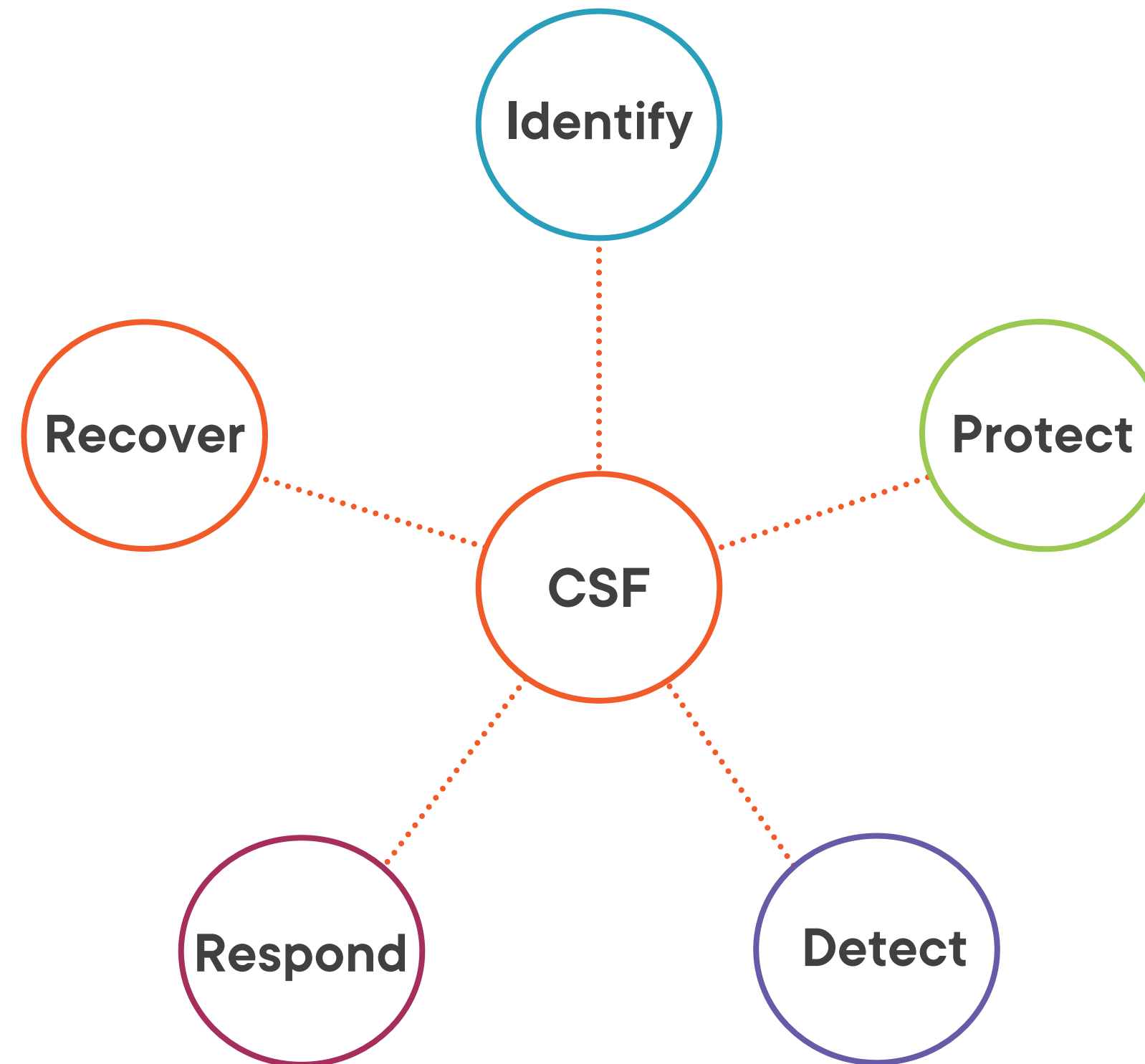
What is it?

What makes it special?

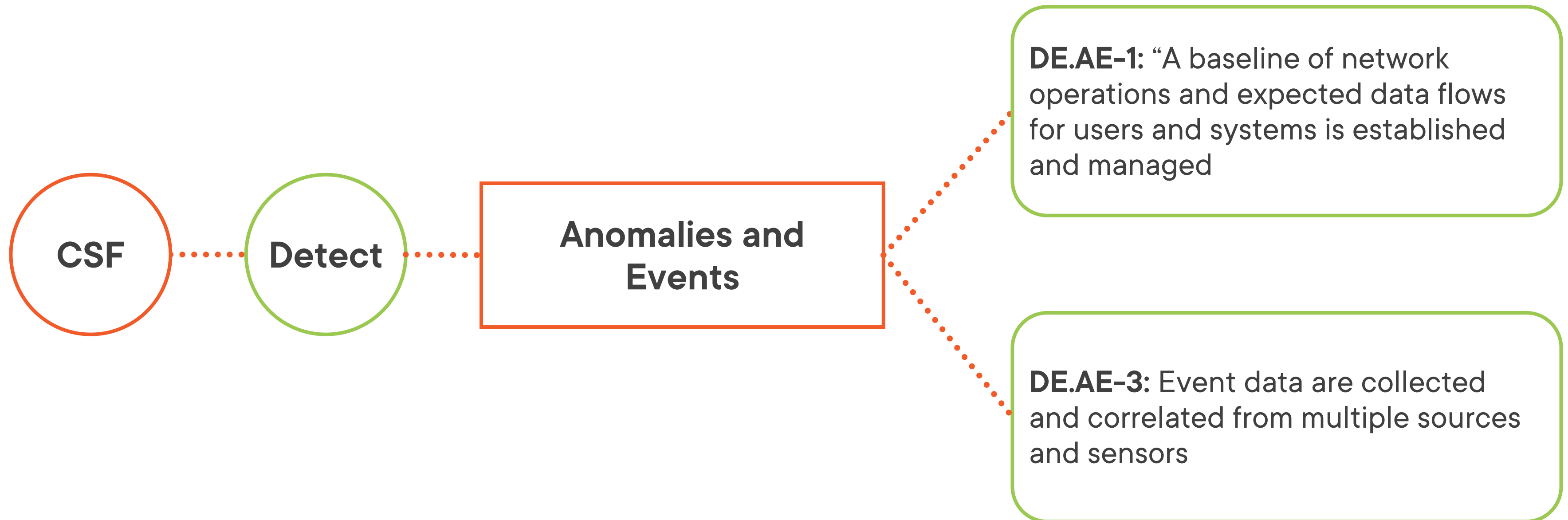
Where do I get it?



# NIST Cybersecurity Framework



# NIST Cybersecurity Framework



# Demo: Set up Packetbeat

1. Prep and Download
2. Configure and Test
3. Setup and Start



# Demo: Networking Use Cases

1. Review Network Tab
2. Discuss Use cases scenerios
3. Verify Packetbeat Events



# Demo: Security Use Case/Custom Alerts

1. Review Hosts tab
2. Discuss Security Use Cases
3. Review Custom Alerts





# More Information

## Capabilities

Capability not covered

<https://link-to-more-into.net/>

Capability 2 covered

<https://yet-another-link.net/>

## Related Information

Info about specific tactic category

<https://totally-relevant-link.net/>

List of subjects in the area

- Similar thing
- Other thing
- Last thing

