

OS Analysis with Nagios



Owen Dubiel

Information Security Professional

www.linkedin.com/in/owendubiel66



Nagios®





Creator: “Ethan Galstad”



Nagios is a powerful awareness tool that allows organizations to detect and respond to problems before issues can occur.



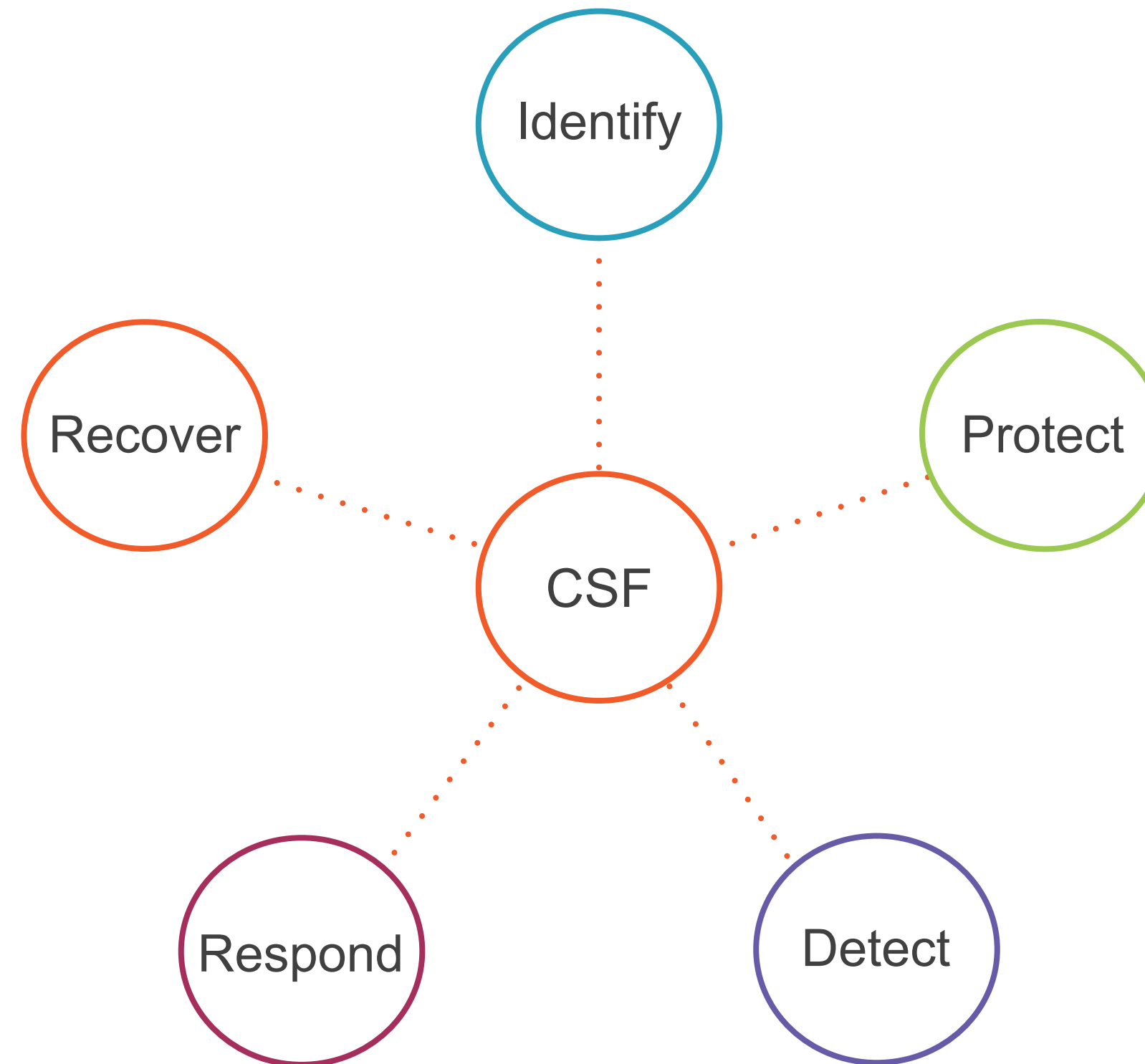
What is it?

Where do I get it?

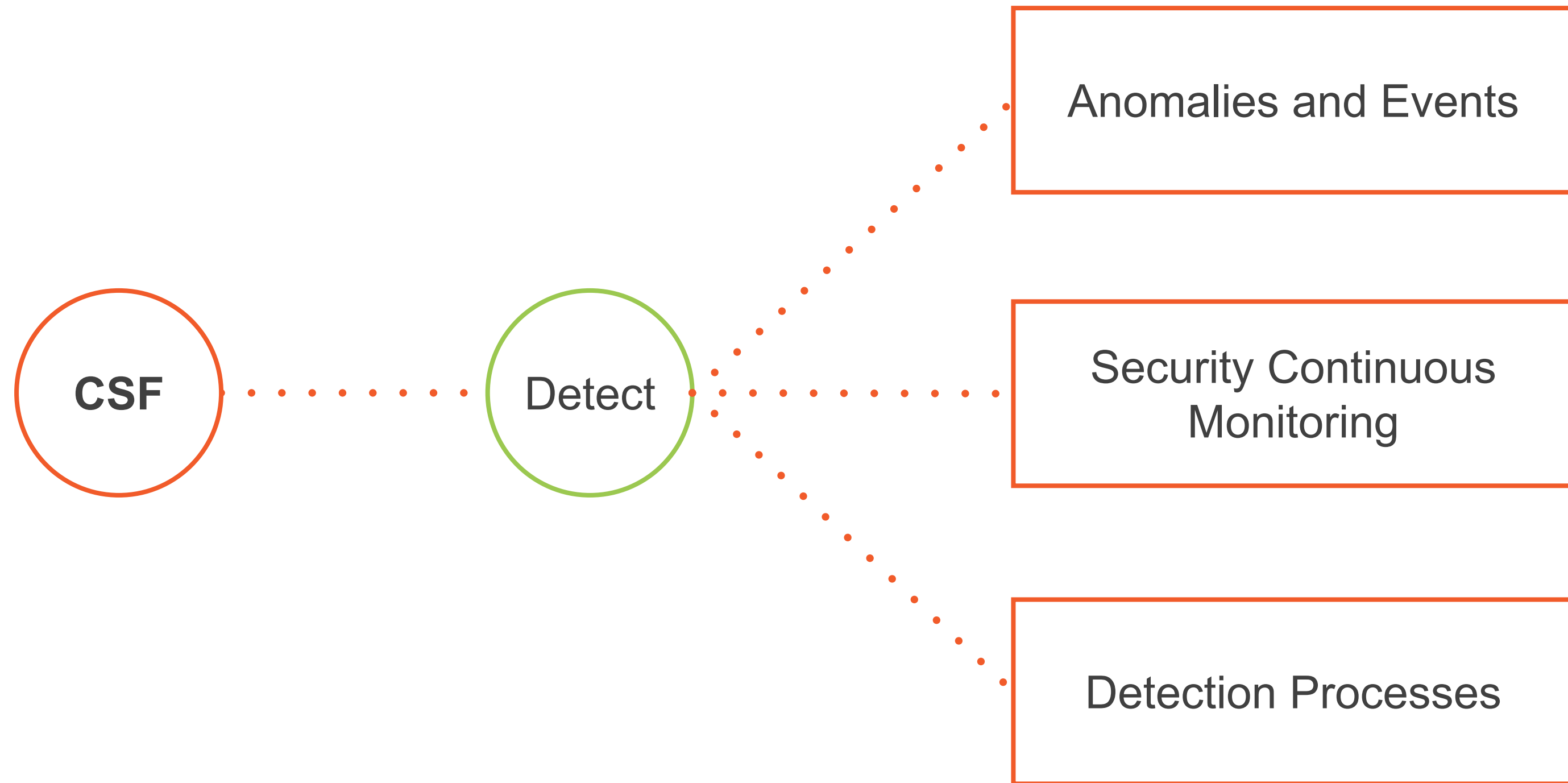
What makes it special; why use this one?



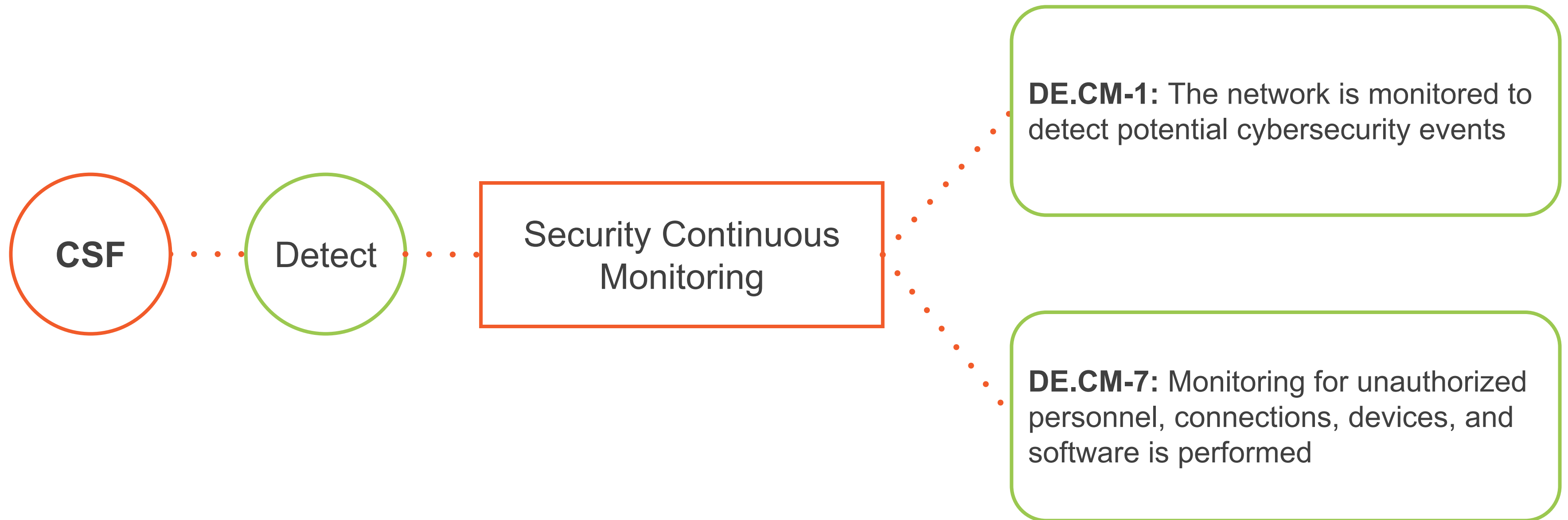
NIST Cybersecurity Framework



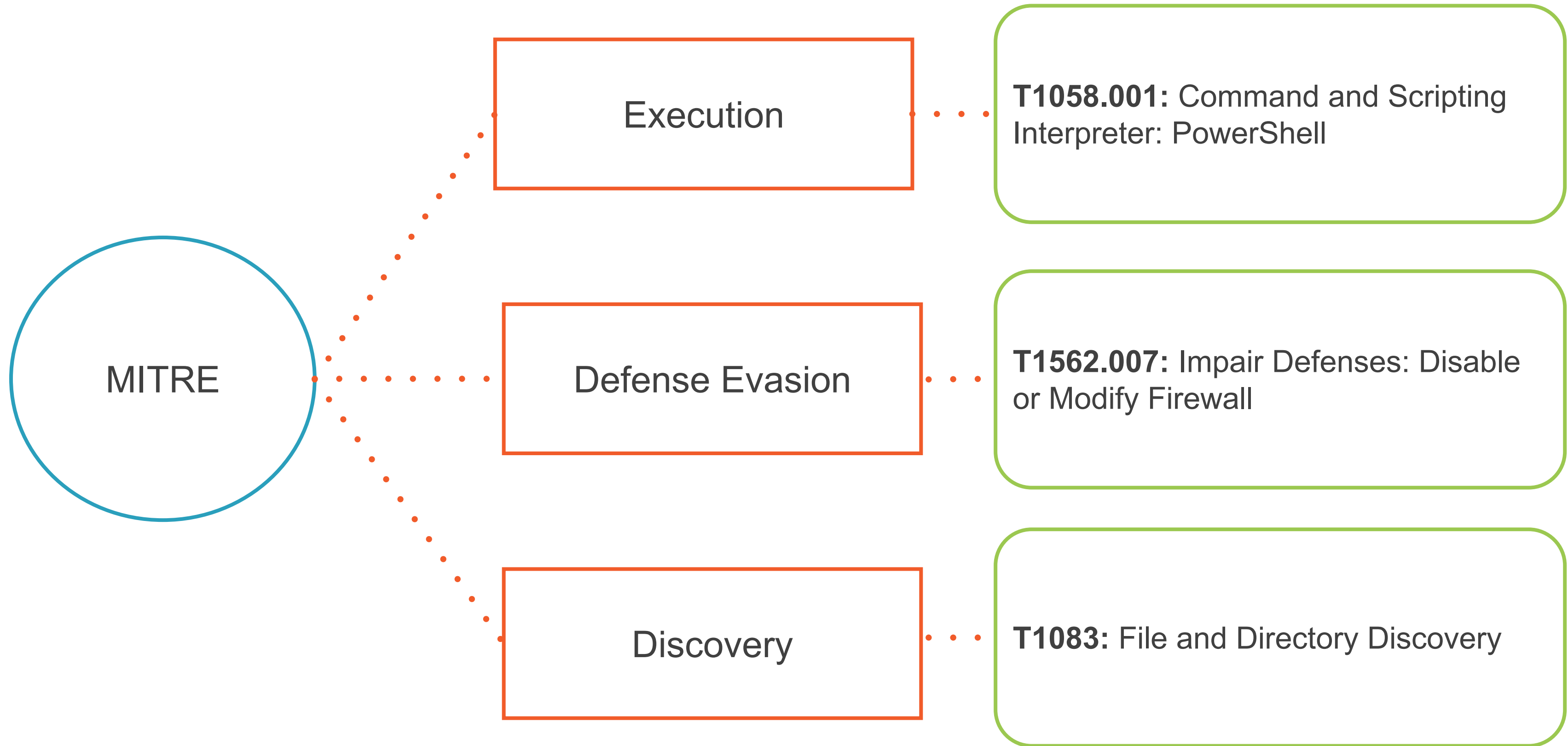
NIST Cybersecurity Framework



NIST Cybersecurity Framework



MITRE ATT@CK Framework TTP



Nagios Demo

1. Enable Free Version
2. Deploy Scanning or Agents
3. Use of Main Features to Identify the Following:
 - T1059.001
 - T1562.007
 - T1083



More Information

Capabilities

Nagios Core

<https://www.nagios.com/products/nagios-core/>

Nagios Network Analyzer

<https://www.nagios.com/products/nagios-network-analyzer/>

Related Information

T1059.001:

<https://attack.mitre.org/techniques/T1059/001/>

T1562.007:

<https://attack.mitre.org/techniques/T1562/007/>

T1083:

<https://attack.mitre.org/techniques/T1083/>

