

# OS Analysis with Wazuh

---



**Zach Roof**

LEAD SECURITY ENGINEER

@zachroofsec [www.zachroofsec.com](http://www.zachroofsec.com)







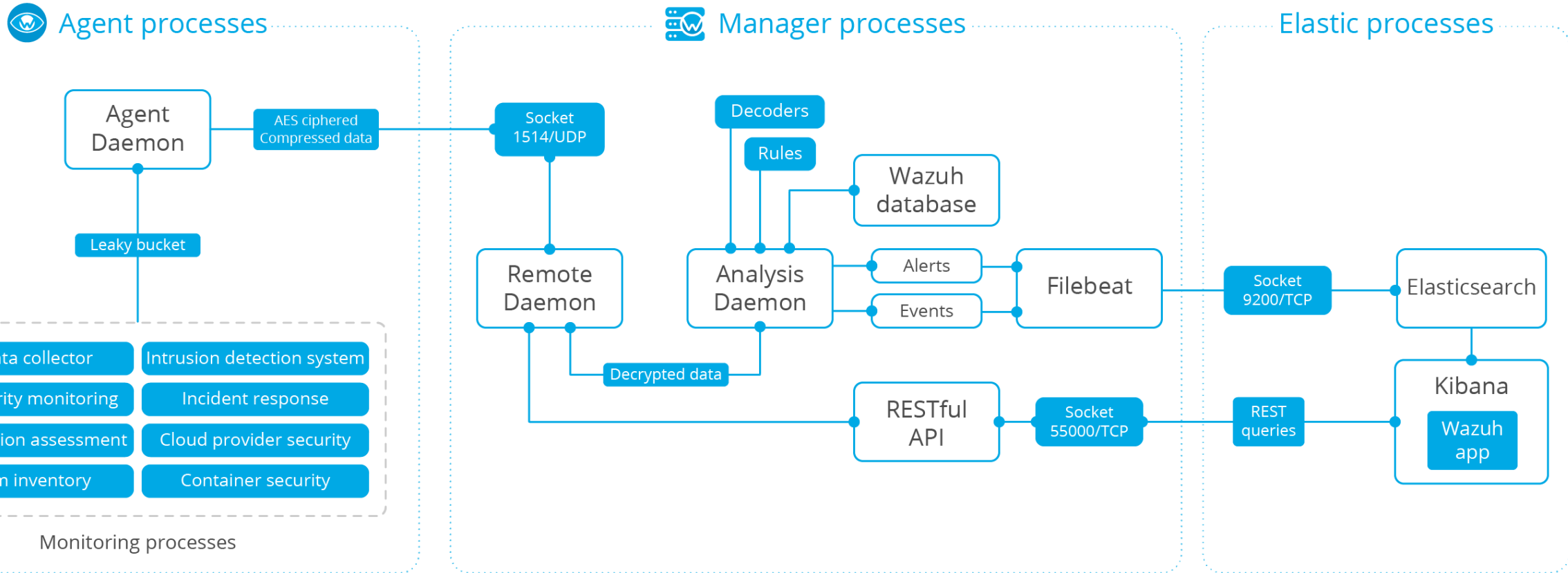
Creator: Santiago Bassett



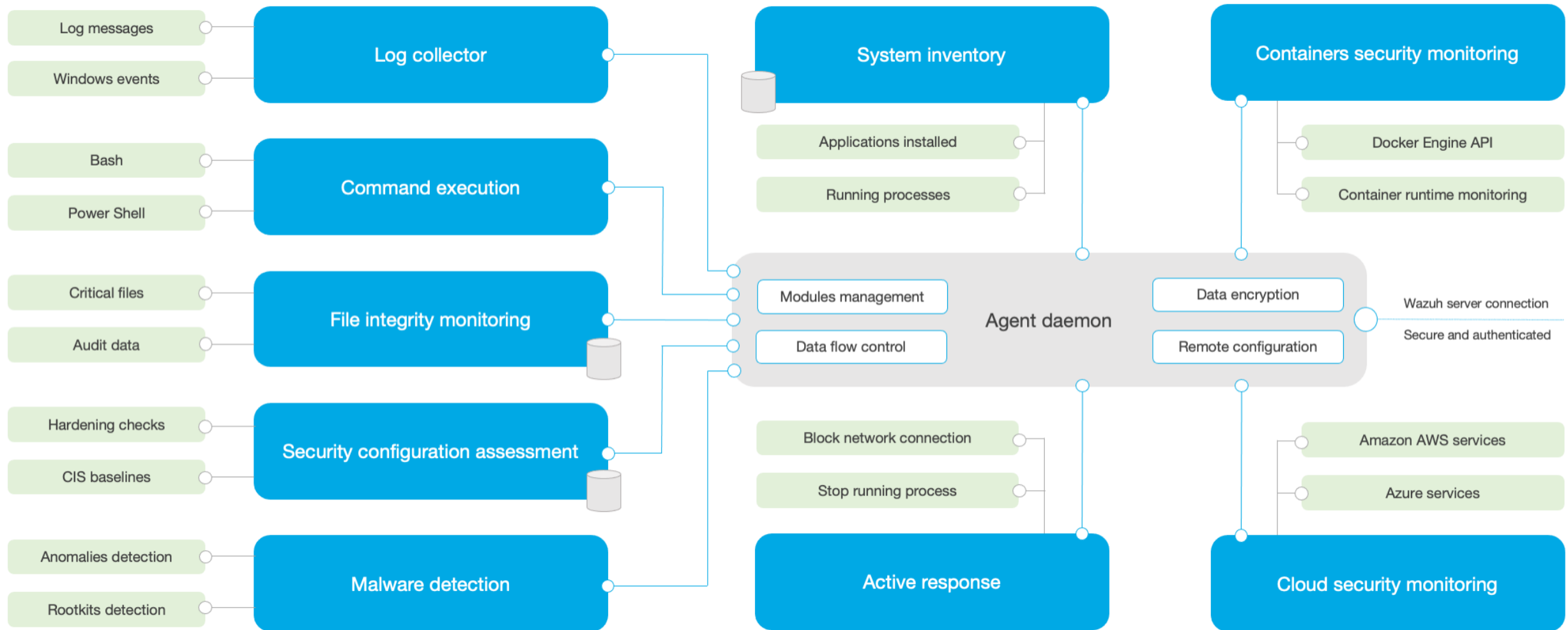
Wazuh is a free and open-source platform used for threat prevention, detection, and response. Wazuh is capable of protecting workloads across on-premises, virtualized, containerized, and cloud-based environments.



# Wazuh Architecture



# Agent Architecture



Notes: [github.com/zachroofsec/os-analysis-with-wazuh](https://github.com/zachroofsec/os-analysis-with-wazuh)





Agents: Mac, Windows, Linux

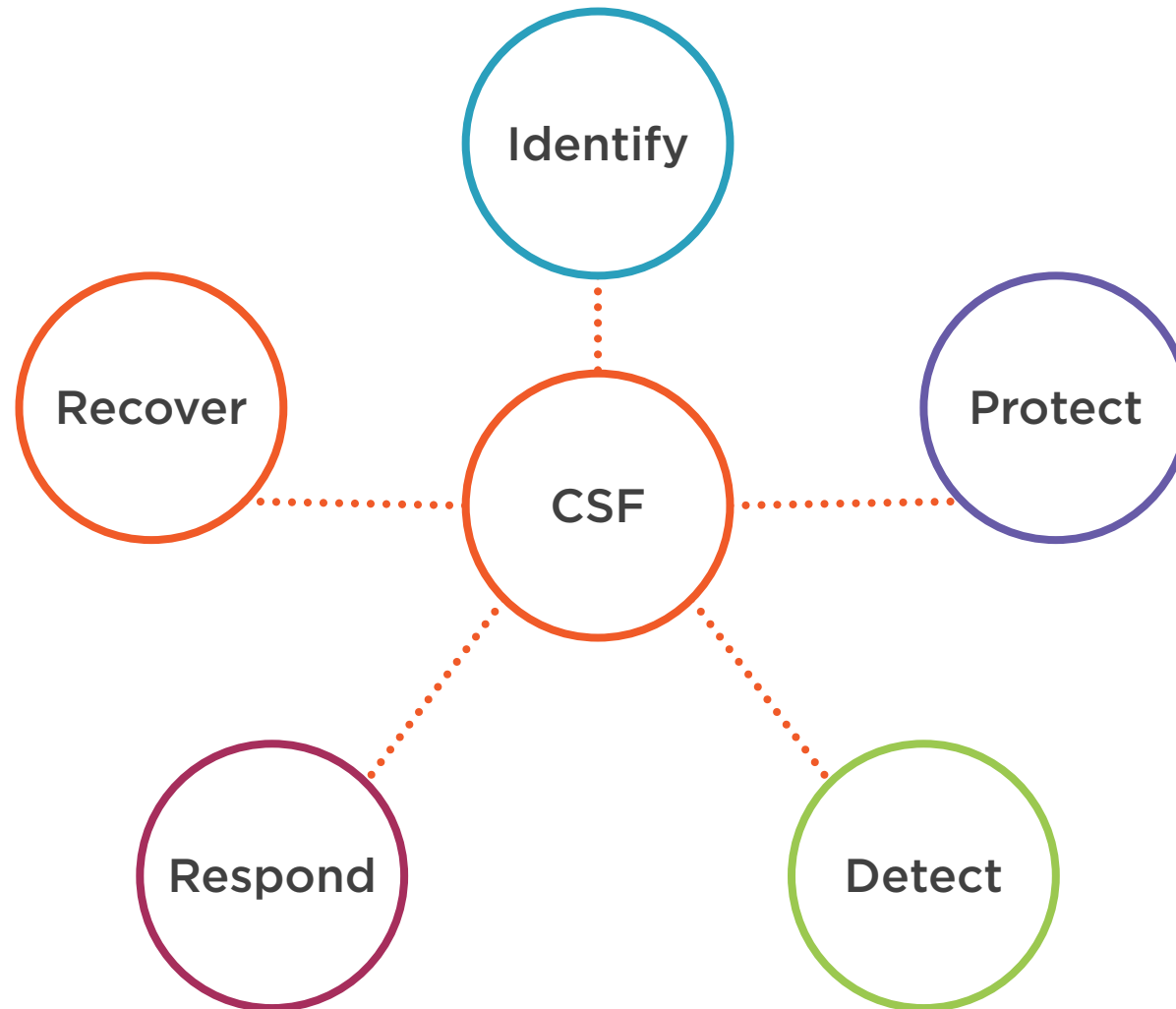
[github.com/wazuh/wazuh-docker](https://github.com/wazuh/wazuh-docker)

[documentation.wazuh.com/4.0/docker/index.html](https://documentation.wazuh.com/4.0/docker/index.html)

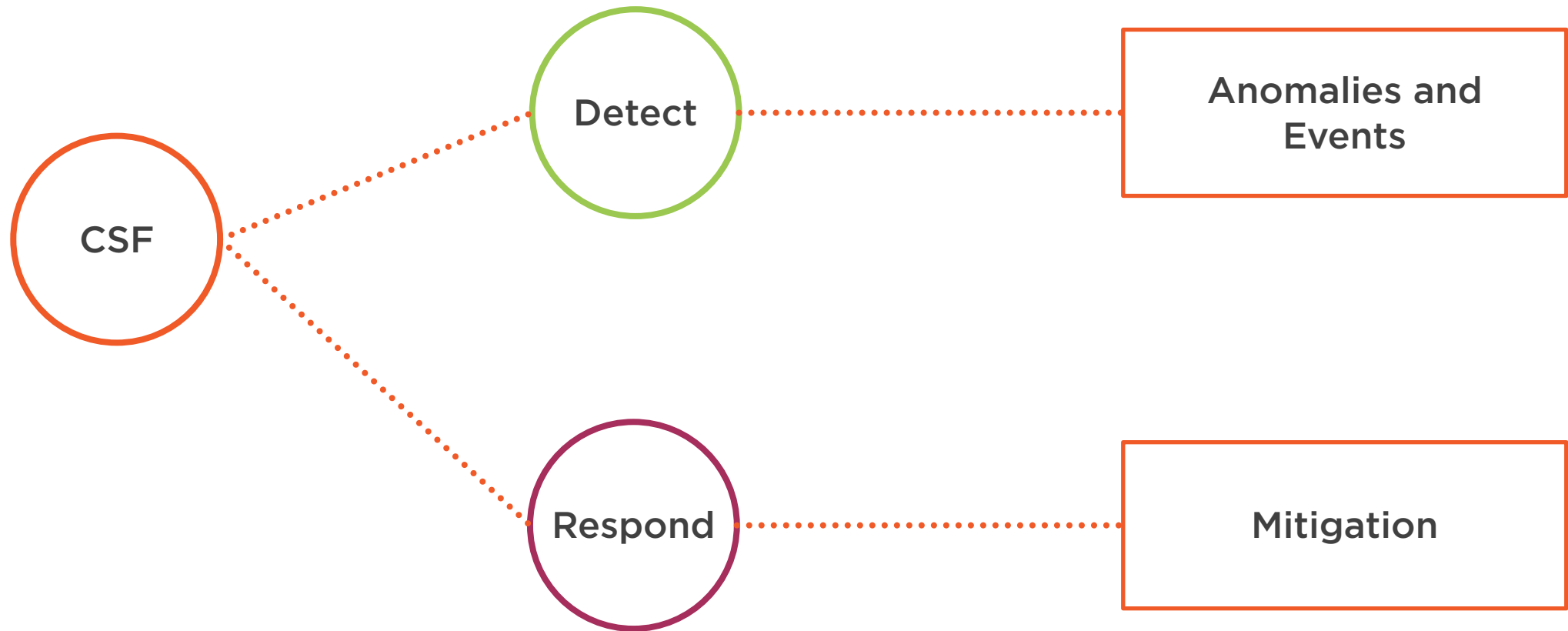
[documentation.wazuh.com/4.0/installation-guide/wazuh-agent/index.html](https://documentation.wazuh.com/4.0/installation-guide/wazuh-agent/index.html)



# NIST Cybersecurity Framework (Core)

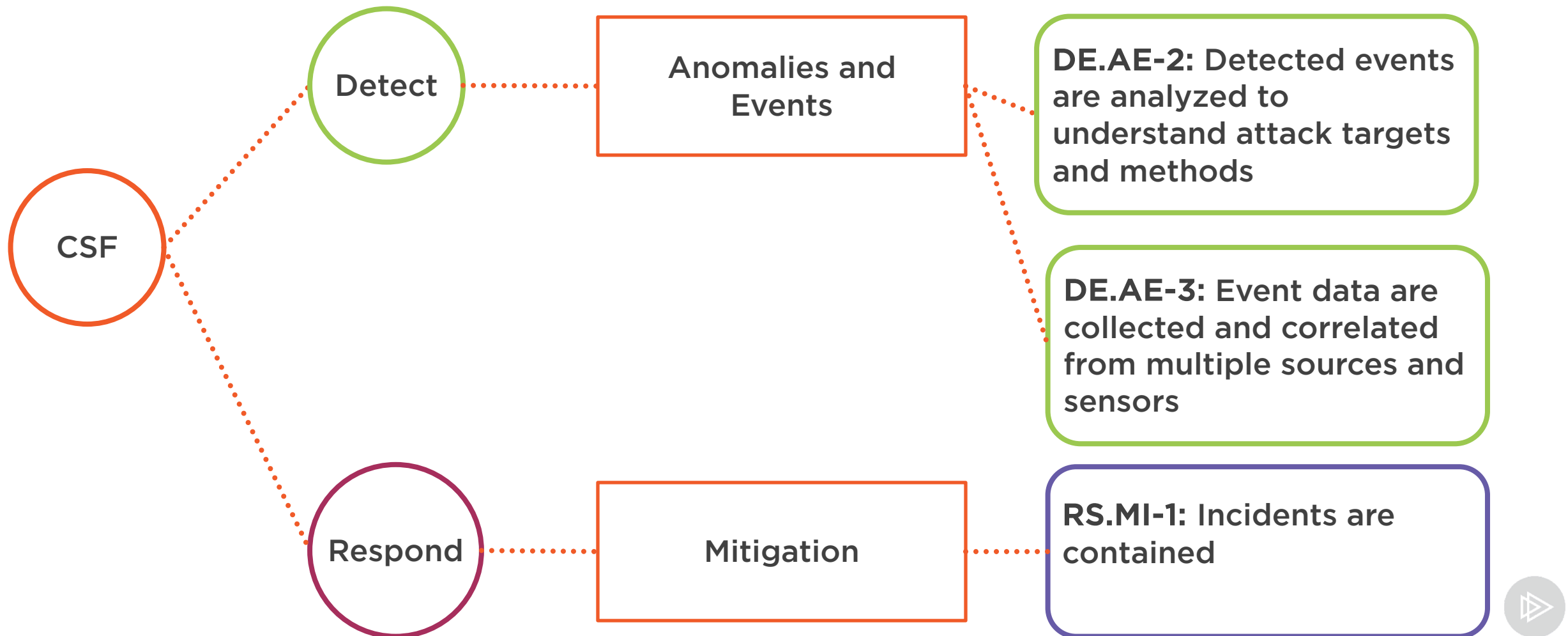


# NIST Cybersecurity Framework





# NIST Cybersecurity Framework



# MITRE ATT&CK

## Data Analysis Type

Network Analysis

OS Analysis

Application Analysis

Infrastructure Analysis

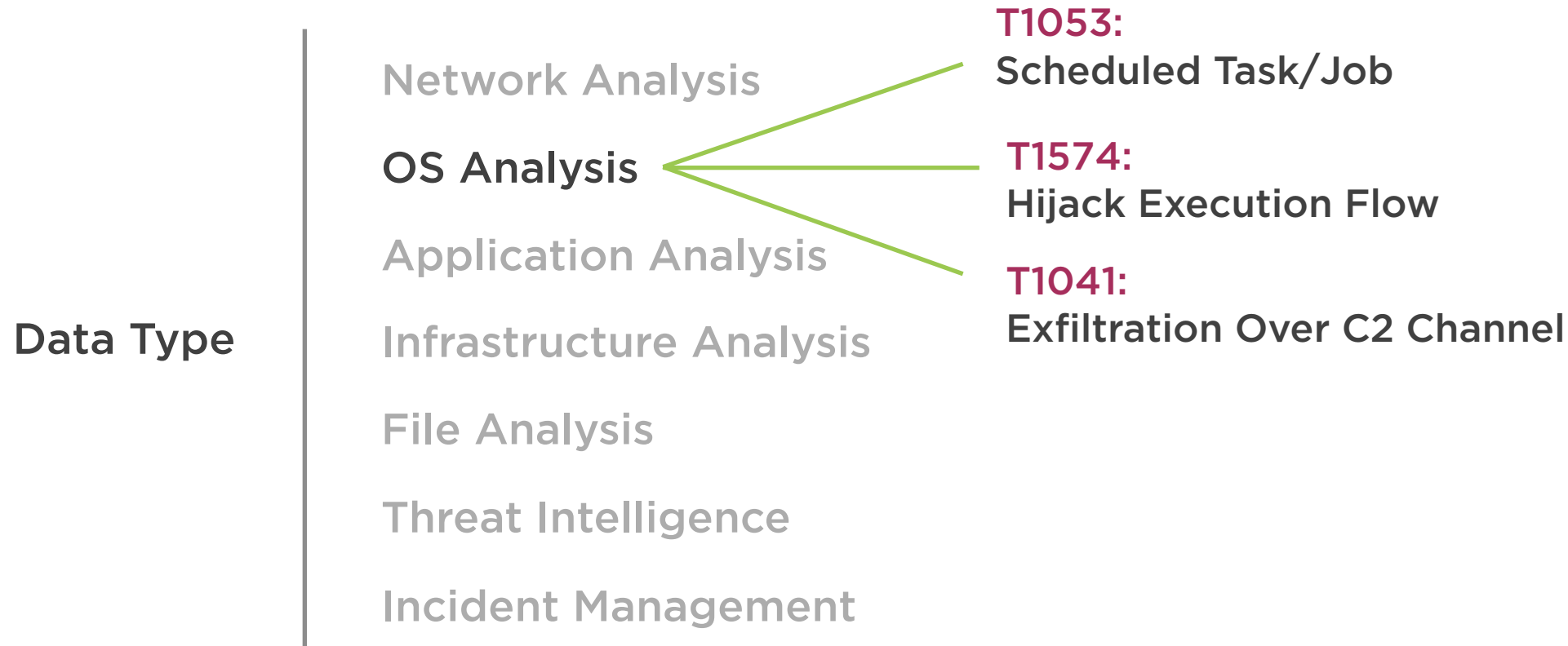
File Analysis

Threat Intelligence

Incident Management



# MITRE ATT&CK



# MITRE SHIELD

## T1053:

### Scheduled Task/Job

\_\_\_\_\_ DTE0034 - System Activity Monitoring: A defender can capture system activity logs and generate alerts if the adversary creates new scheduled tasks or alters existing tasks (DUC0027)

## T1574:

### Hijack Execution Flow

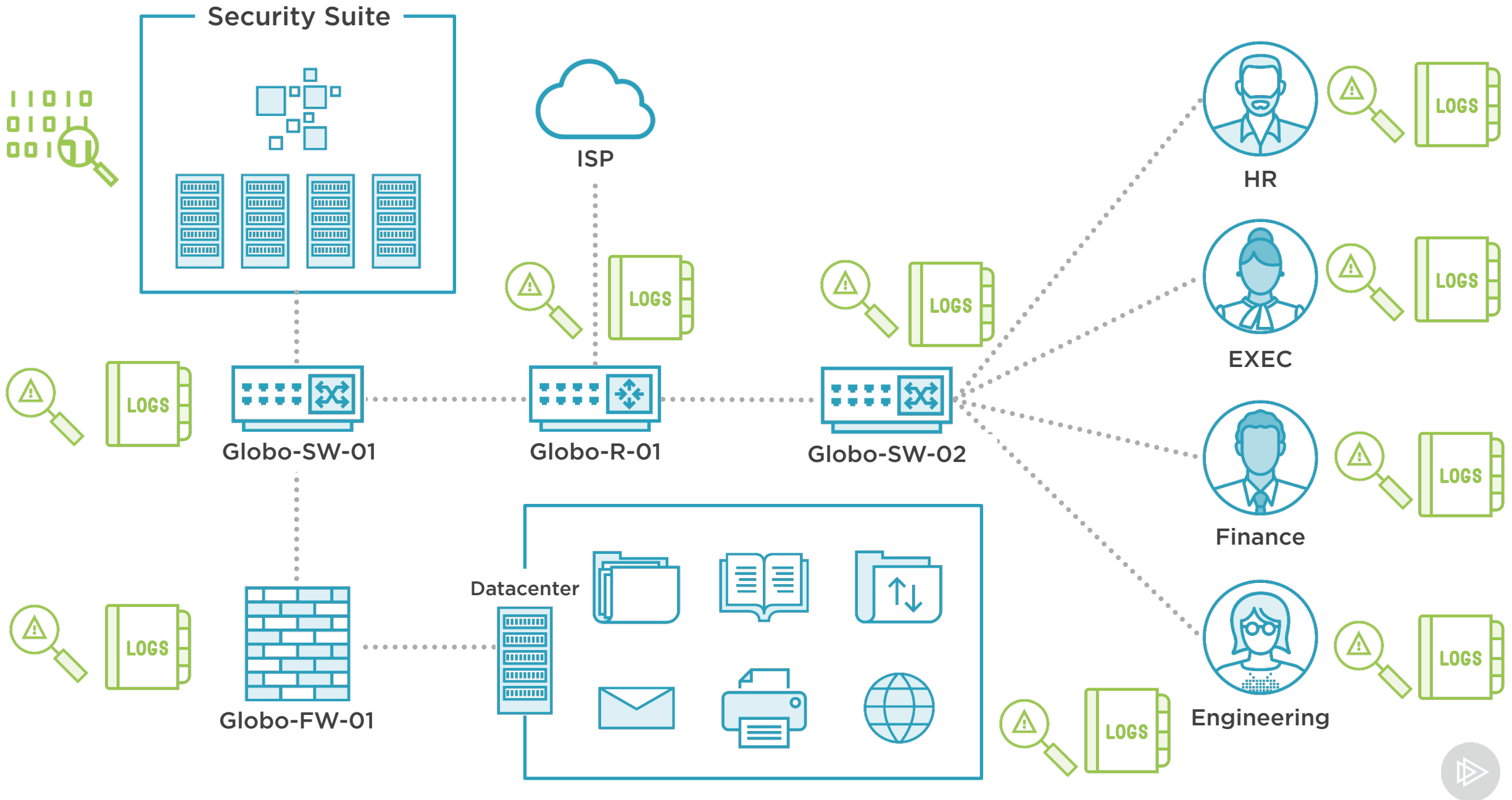
\_\_\_\_\_ DTE0032 - Security Controls: A defender can block execution of untrusted software (DUC0048)

## T1041:

### Exfiltration Over C2 Channel

\_\_\_\_\_ DTE0026 - Network Manipulation: A defender can restrict network traffic making adversary exfiltration slow or unreliable (DUC0175)





Simulation Environment

Merlin Server Container

Victim Container

Security Suite



Blue Team Containers

Wazuh Server  
ELK



ISP



Globo-R-01



HR

Wazuh Agent  
Merlin Agent



# Additional Resources

## Capabilities

<https://wazuh.com/blog/emotet-malware-detection/>

<https://wazuh.com/blog/monitoring-root-actions-on-linux-using-auditd-and-wazuh/>

<https://github.com/wazuh/wazuh/wiki/Proof-of-concept-guide>

<https://wazuh.com/blog/using-wazuh-for-windows-vulnerability-detection/>

## Related Information

### Hijack Execution Flow

<https://attack.mitre.org/techniques/T1574/>

### Supporting Technology

- Kibana
- <https://www.elastic.co/guide/en/kibana/7.9/introduction.html>
- Elasticsearch
- <https://opendistro.github.io/for-elasticsearch-docs/>



# OS Analysis with Wazuh

---



**Zach Roof**

LEAD SECURITY ENGINEER

@zachroofsec [www.zachroofsec.com](http://www.zachroofsec.com)

