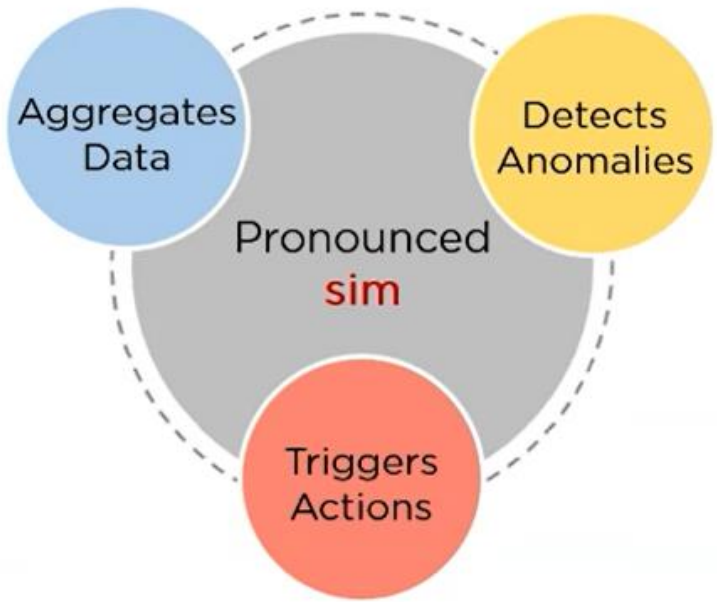
What is SIEM?

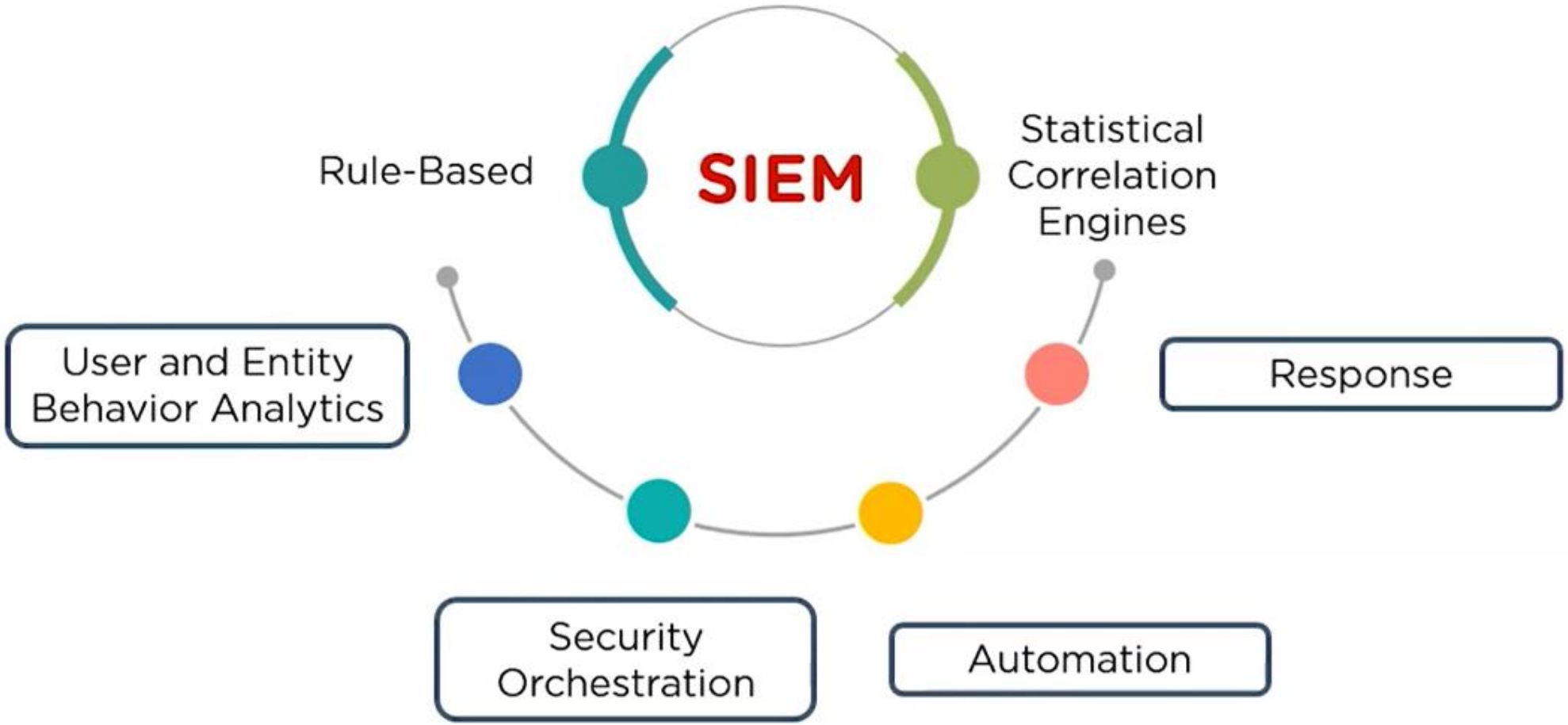
Security Information and Event Management (SIEM) is a holistic security approach merging Security Information Management (SIM) and Security Event Management (SEM)



Large Enterprises

Smaller Organizations

What is SIEM?


Rule-Based
SIEM
Statistical Correlation Engines
User and Entity Behavior Analytics
Response
Security Orchestration
Automation

Functionality of SIEM

Event

Log Data

Organization

This data is centralized and includes information from applications, security devices, antivirus filters, and firewalls

Why is SIEM important?

SIEM streamlines security management, sifting through vast data to prioritize alerts for enterprises. It uncovers potential incidents, identifying malicious activity in log entries and reconstructing attack sequences

- Automated
- Comprehensive Reports
- Eliminating Manual Efforts

Advantages of SIEM

Advantages

Rapid Threat Identification

Holistic Security View

Versatile Use Cases

Scalability

Threat Detection and Alerts

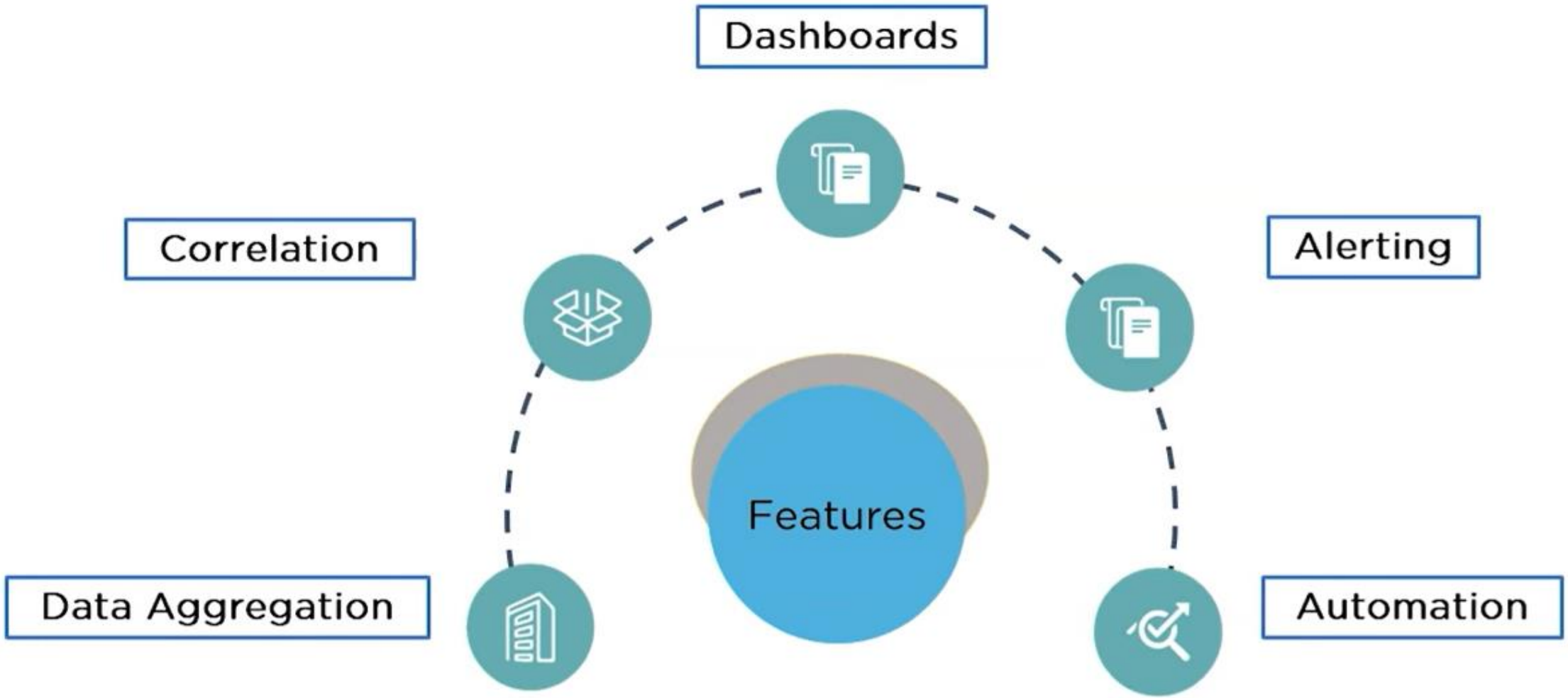
Forensic Analysis Capability

Limitations of SIEM

Limitations

- Implementation Time
- Cost Factors
- Expertise Requirement
- Rule-Based Analysis
- Misconfiguration Risks

Exploring SIEM Features and Capabilities



SIEM Tools and Software

splunk>

IBM QRadar

LogRhythm

solarwinds

ManageEngine Log360

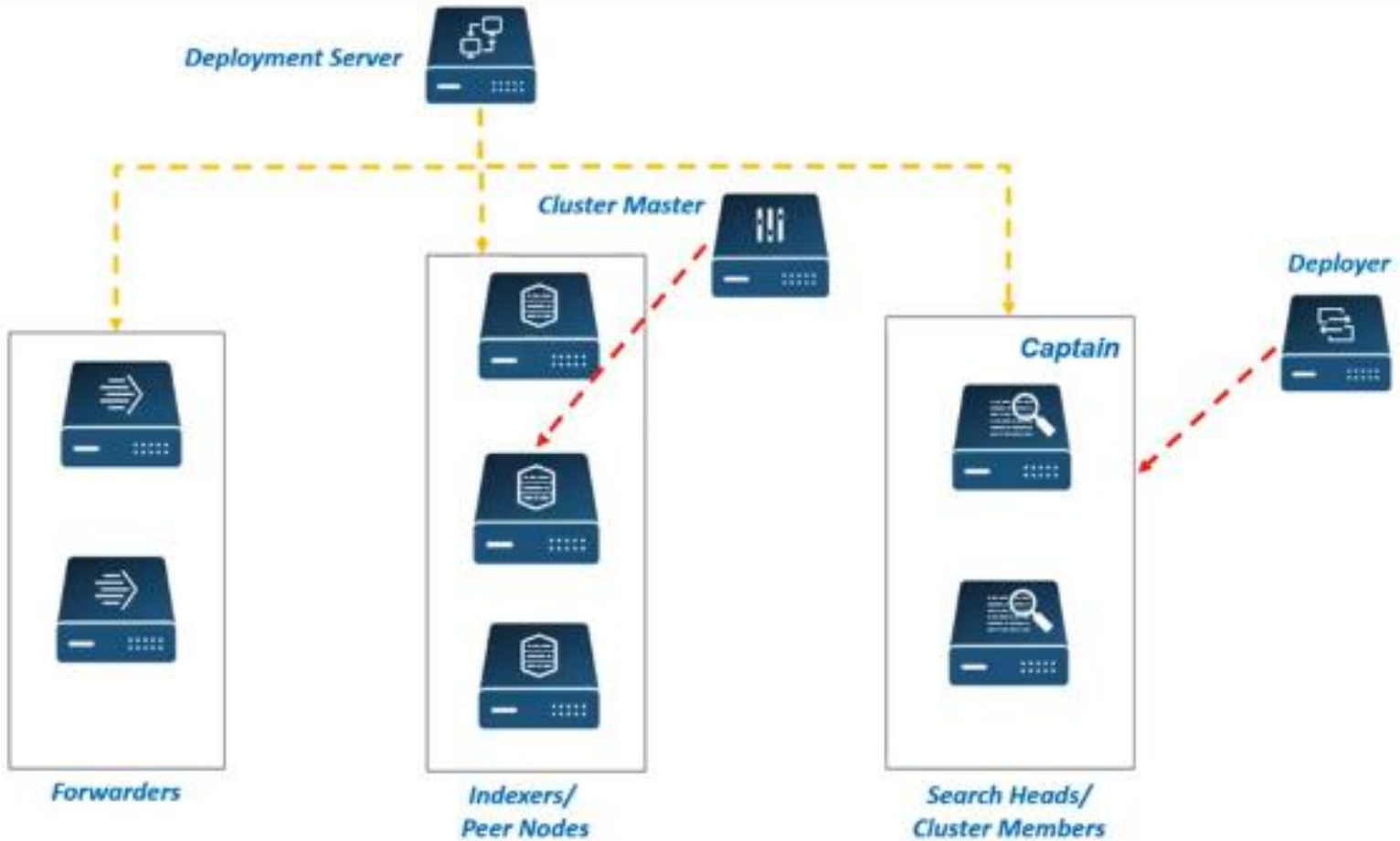
exabeam

NETWITNESS

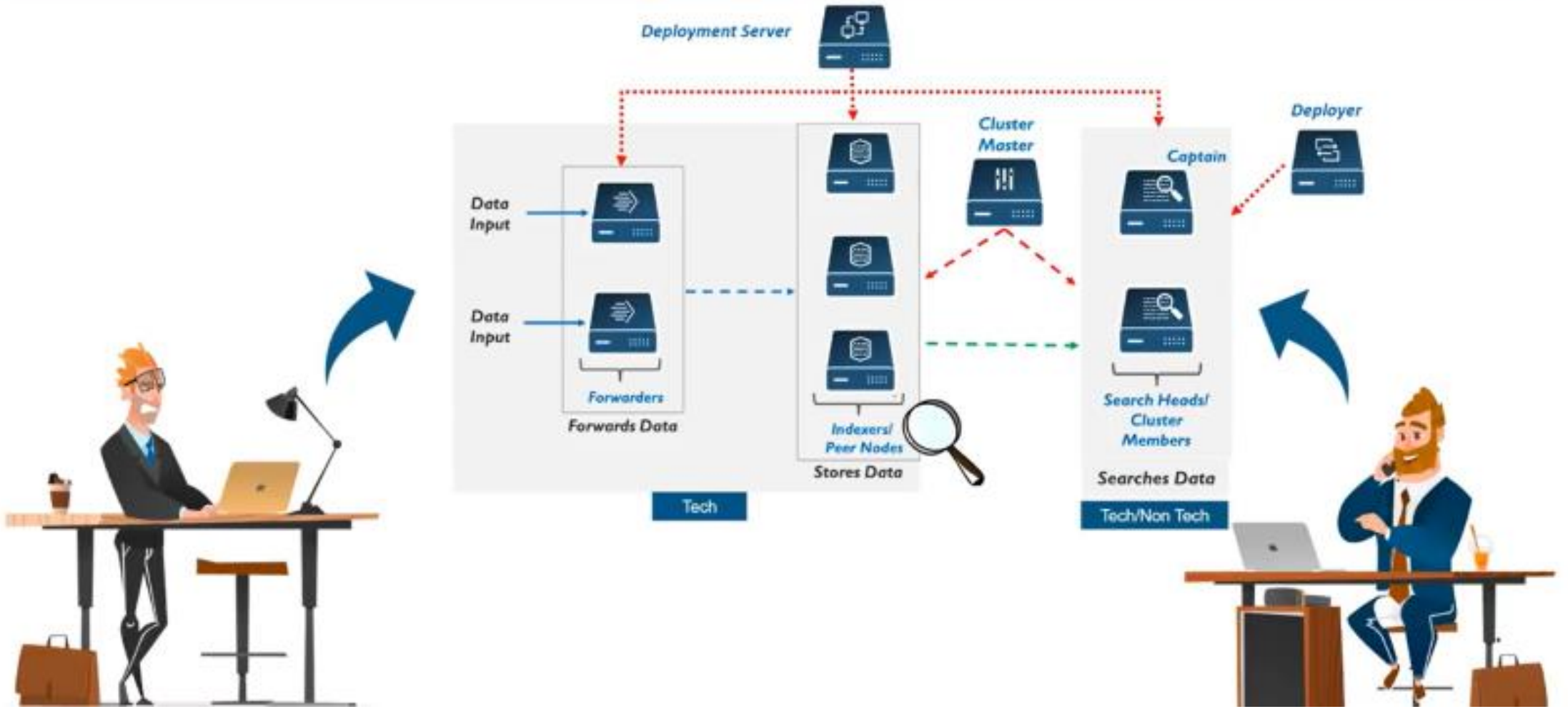
Components In A Distributed Splunk Cluster

*"A **Splunk cluster** is a group of Splunk instances"*

Roles Of Components In A Splunk Cluster



Roles In A Distributed Splunk Cluster



Architecture Of Splunk