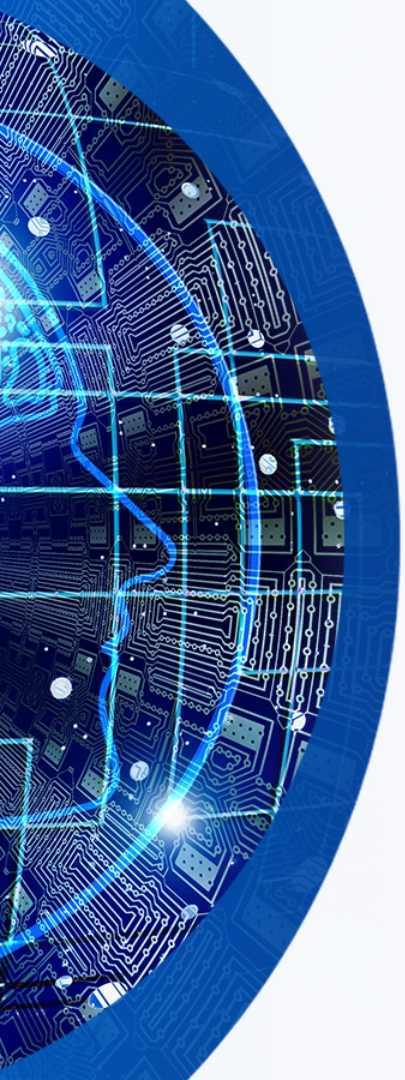
Managed Security Service Provider (MSSP)

Security Operation Center (SOC) as a Service

Comprehensive Security Solutions

Agenda

- What is SOC and Next-Generation SOC
- Core Components of SOC
- How SOC Functions to provide comprehensive Cyber Security
- Some common Use Cases
- SOC Architecture for On-Prem and MSSP model
- SOC Organization Structure and Functions

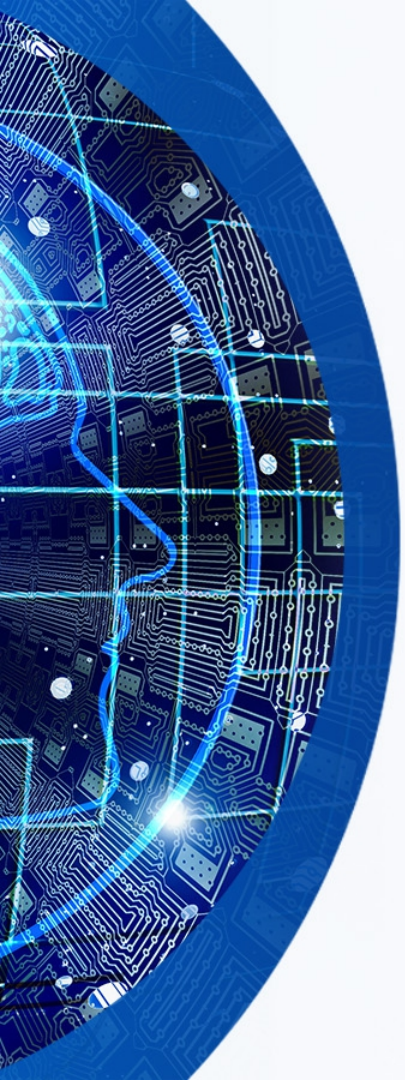


Security Operation Center (SOC)

- The function of the security operations center (SOC) is to **monitor**, **prevent**, **detect**, **investigate**, and **respond** to **cyber threats** around the clock.

- SOC teams are charged with monitoring and **protecting** the **organization's assets** including **intellectual property**, **personnel data**, **business systems**, and **brand integrity**.

- The SOC team implements the organization's overall **cybersecurity strategy** and acts as the **central point of collaboration** in **coordinated efforts** to **monitor**, **assess**, and **defend** against **cyberattacks**.



Traditional SOC

1. Compliance Monitoring
2. Detect known threats
3. Notification
4. Ticketing and Tracking
5. Manual response

Advanced Platform

1. Threat Hunting
2. Auto - Triage
3. Threat Intel (ML/DL)
4. Rapid Investigation
5. Auto containment

Specialized Skills

1. Hunters
2. End Point Analysis
3. Incident Responder
4. Investigators
5. Malware Analysis

Next Gen SOC

Core Components of Next Gen SOC

1. SIEM : Security Information and Event Management
2. UEBA : User and Event Behavior Analytics
3. NBAD : Network-Based Anomaly Detection
4. VA : Vulnerability Assessment
5. NTA : Network Traffic Analysis
6. EDR : Endpoint Detection and Response
7. XDR : Cross-Layered Detection and Response
8. File Integrity Monitoring (FIM)
9. TI : Threat Indicator
10. AI/ML/DL : Advanced Machine Learning and Deep Learning
11. SOAR : Security Orchestration, Automation and Response

SOC Functions

Inputs → Process → Outputs

Raw Security Logs
OS, Applications, Databases, Services, Processes

Router & Switch Flows:
NetFlow, IPFix, SFlow and Raw Traffic

User Identity:
Windows AD, DNS, DHCP, any LDAP

Cloud Logs:
IaaS, PaaS, SaaS, Audit, VPC, Identity

Existing Security Systems
Alerts from Firewall and other devices

Input

Input

Input

Input

Input

- AI With Actionable Intelligence
- Machine Learning
- Auto Remediation Policy Engine
- Global Threat Intelligence
- Dynamic Threat Model Engine
- Advance Real Time Correlation
- Security Analysis
- Network Policy Engine
- Anomaly Detection
- Vulnerability Scanner

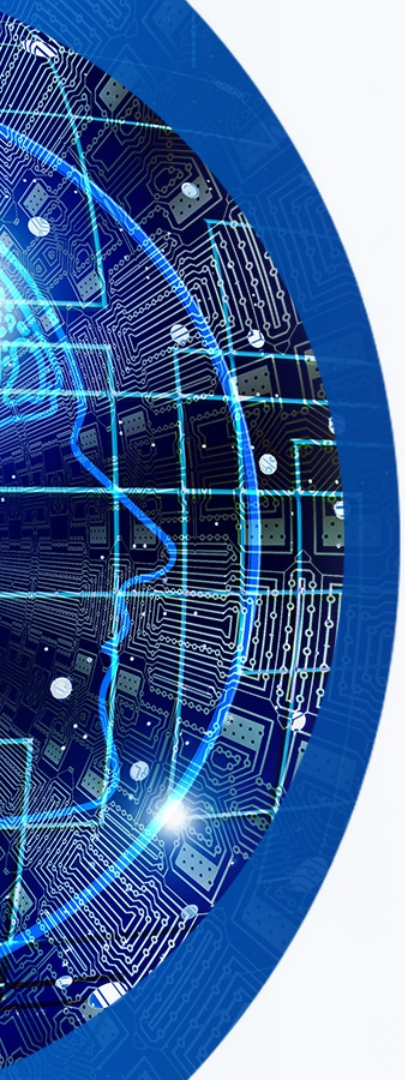
Output → Comprehensive Visibility

Output → Proactive Threat Detection

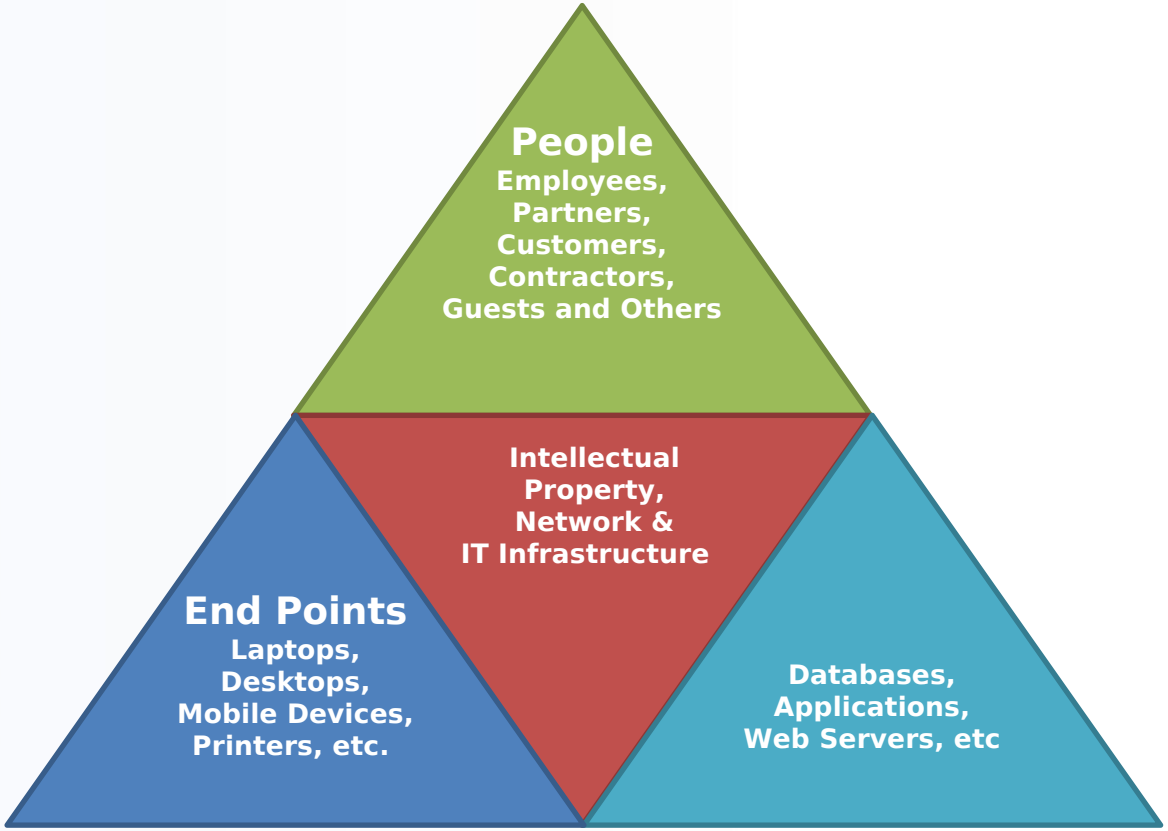
Output → Automatic Real-Time Threat Containment & Elimination

Output → Continuous Compliance and Reporting

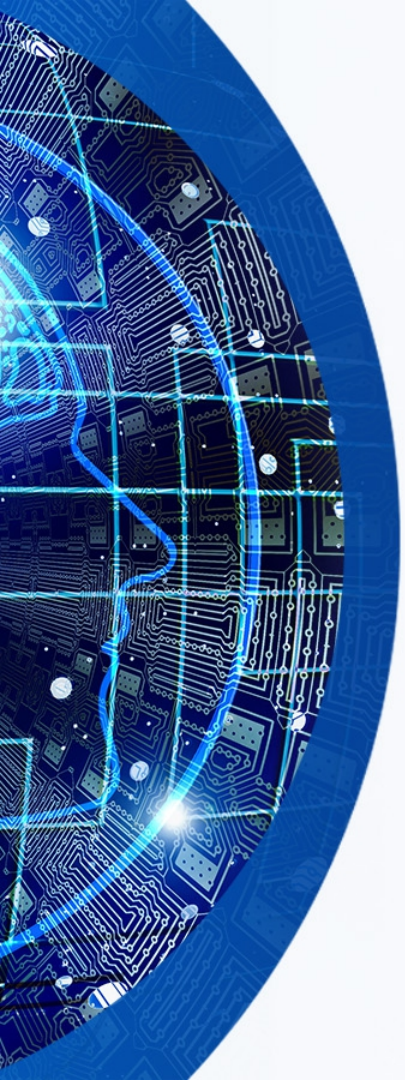
Output → Complete Protection of Information Assets

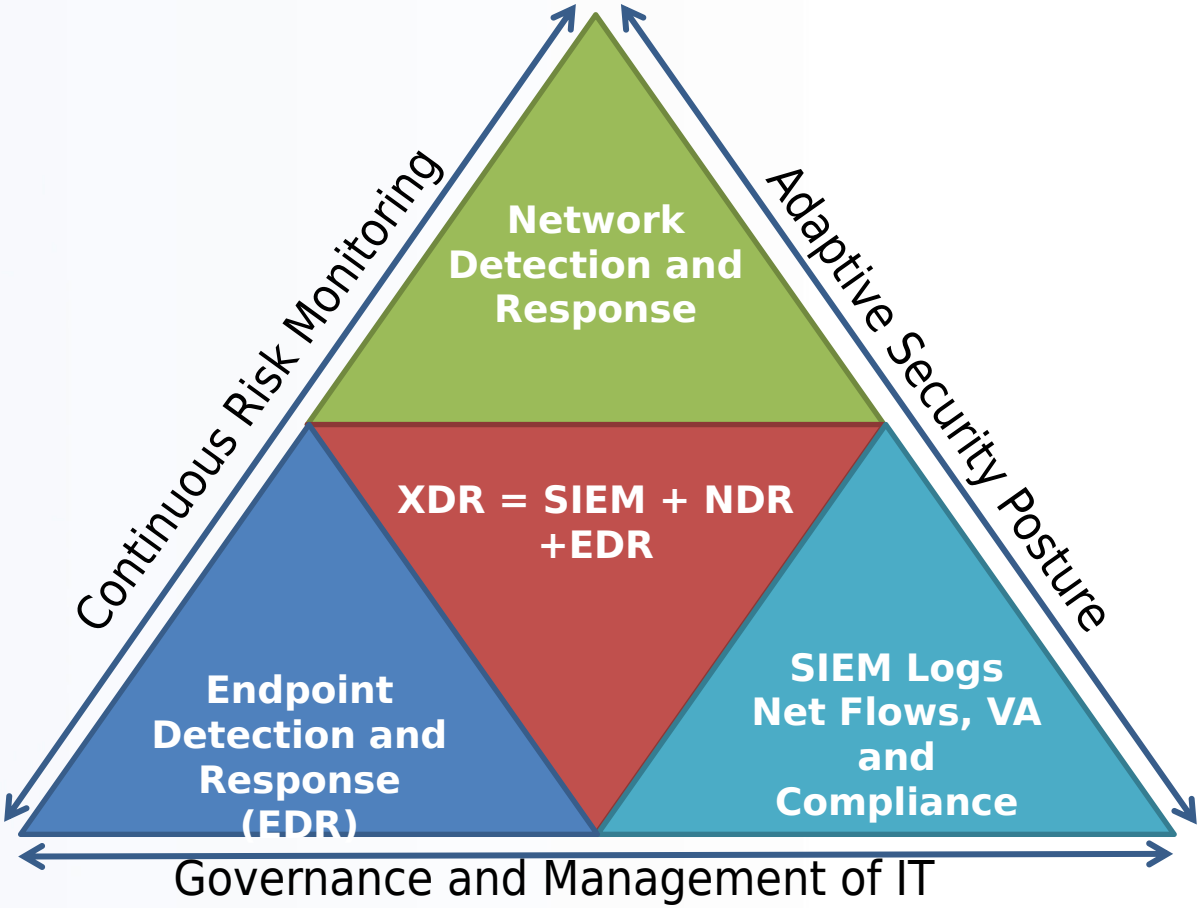


IT Environments



Comprehensive Cyber Security





Use Cases

An **integrated platform** that covers a comprehensive set of use cases and provides continous compliance

Cyber Crime

1. Ransomware
2. Malware
3. Spyware
4. APTs
5. Botnet Detection
6. Potential Infiltration
7. Torjan Activity

NB: All Known and Zero Day

Insider Threats

1. Malicious Insider
2. Compromised Credentials
3. UEBA
4. Privilege Misuse
5. Suspicious Login
6. Traffic Analyzer (IDS)

Denial of Service

1. Volumetric
2. Application Layer
3. Protocols
4. ICMP
5. Amplification
6. SYN Attack

Use Cases

An **integrated platform** that covers a comprehensive set of use cases and provides continous compliance

Policy Enforcement

1. Limit Access to Critical Assets
2. Stop Unwanted Connectivity Applications
3. Network Segregation and Segmentation
4. Catch multi-stage, multi-vectors, malware and Ransomware attacks proactively

Vulnerability Exploits

1. Unknown
2. Known OS
3. Apps
4. Firmware
5. Vulnerability Assessed

Cloud Security

1. IaaS
   - AWS, GCP, Azure
2. SAAS
   - O365
   - Azure AD
3. PaaS
4. CASB
   - API-based

Use Cases

An **integrated platform** that covers a comprehensive set of use cases and provides continous compliance

Brute Force

1. Password Spraying
2. Dictionary Attack
3. Credential Surfing

Web/Email Exploits

1. **Web**
   SQL Injection
   Sross-Site Scripting
   Local File Inclusion
   Directory Traversal
   Remote File Execution
   Cross-Site Request Forgery
2. **Email**
   Spam
   Business Email Compromise

DNS Protection

1. DNS Tunneling
2. DNS Fast Fluxing

Use Cases

An **integrated platform** that covers a comprehensive set of use cases and provides continous compliance

Continous Compliance

1. HIPPA
2. PCI-DSS
3. NIST
4. GDPR
5. SOX

Other Use Cases

1. **Data/IP Exfiltration**
2. **IoT/IIoT Cybersecurity**
3. **OT/ICS Cybersecurity**
4. **Detect IT Mistakes**
5. **Detect Shadow IT**
6. **NBAD**

File Integrity Monitoring

1. Detecting Illicit Activity
2. Diagnosing Unwanted Changes
3. Managing Compliance Mandates

Use Cases

An **integrated platform** that covers a comprehensive set of use cases and provides continous compliance

Threat Hunting

Proactively explore your entire environment for potential vulnerability and threats leveraging global threats intelligence and **contextual & behavioral analytics**. This includes, login and logout, file event, USB device activity etc.

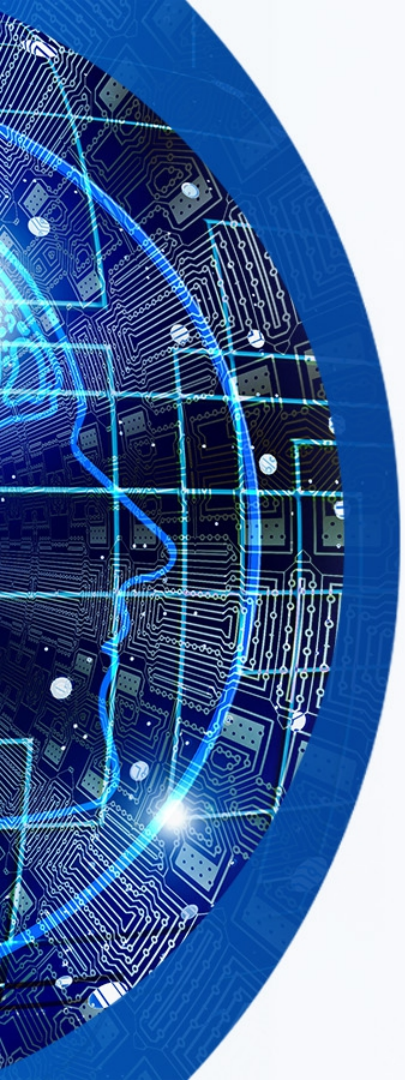
Incident Response and Forensics

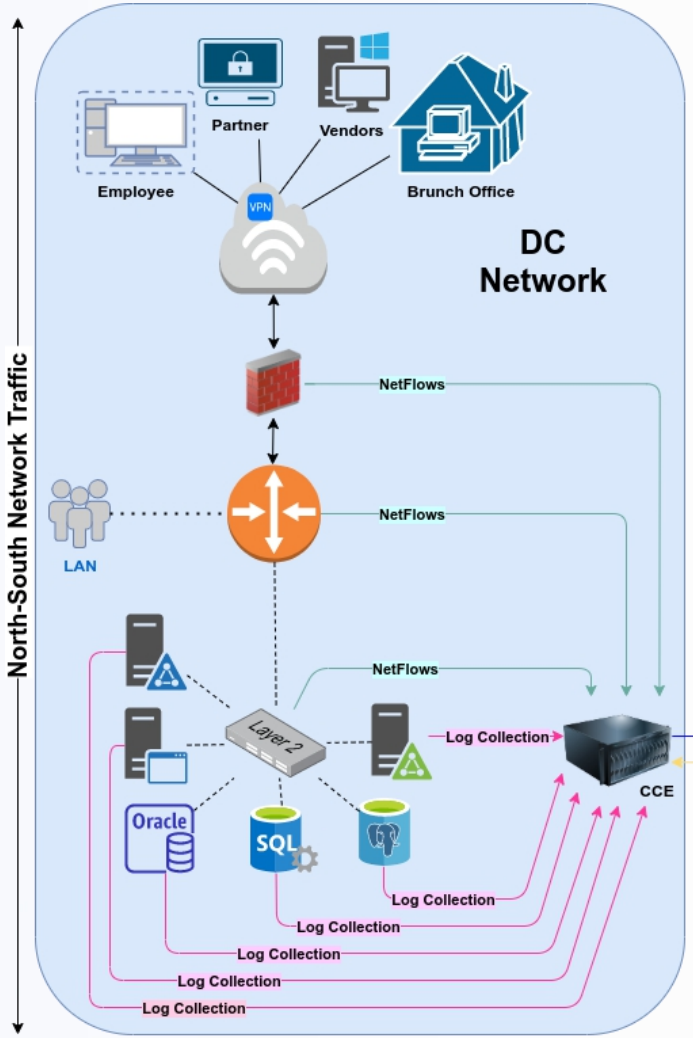
1. Automated response in real-time that meets the anticipated need of the organization
2. Collect data relevant to the phases of an attach such as exploitation, installation and C&C and lateral movement
3. Store detailed forensic data for post-incident investigation

Data Loss Prevention

1. Uses anomaly detection mechanism
2. Provide visibility into data stored on the all endpoints (inside and outside the ogganization)

SOC Architecture

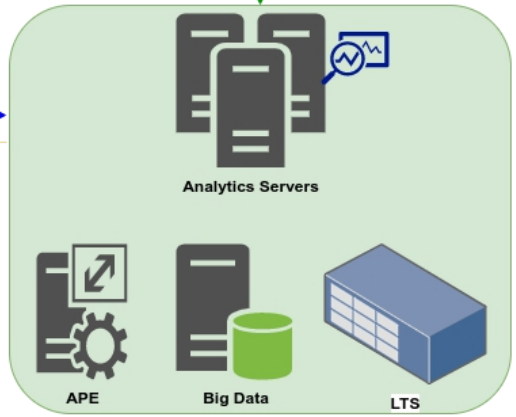




SOC Team

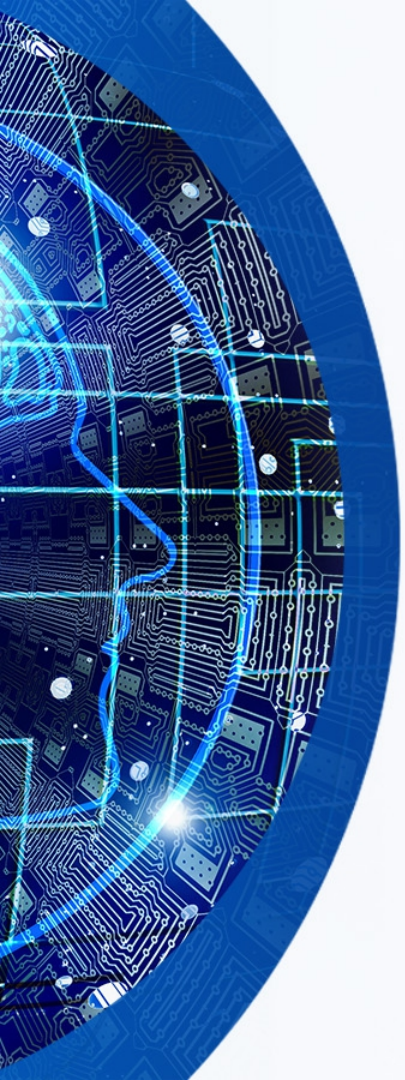
Meta Data

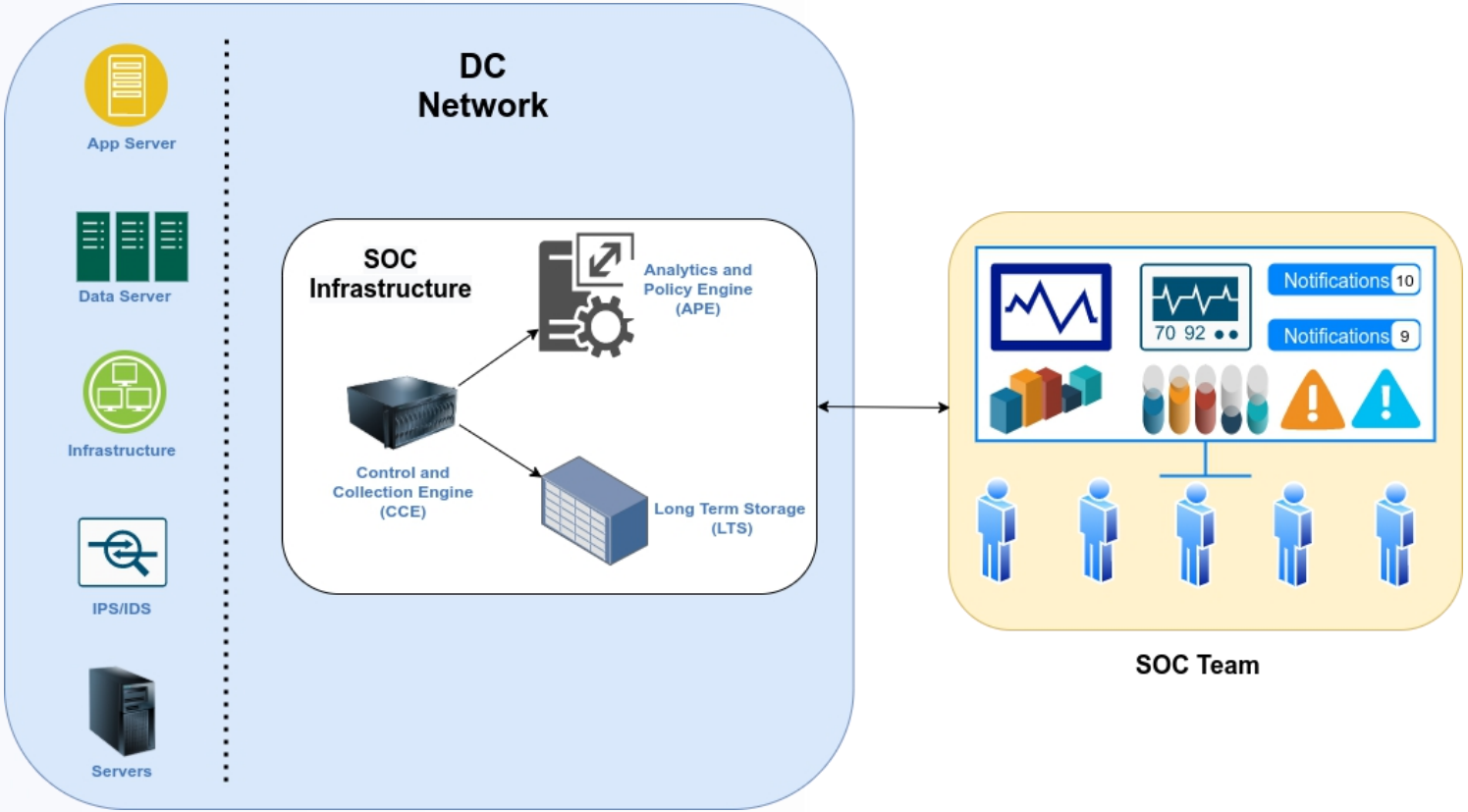
Policy Enforcement



SOC Infrastructure

On-Prem Deployment





Hardware Sizing

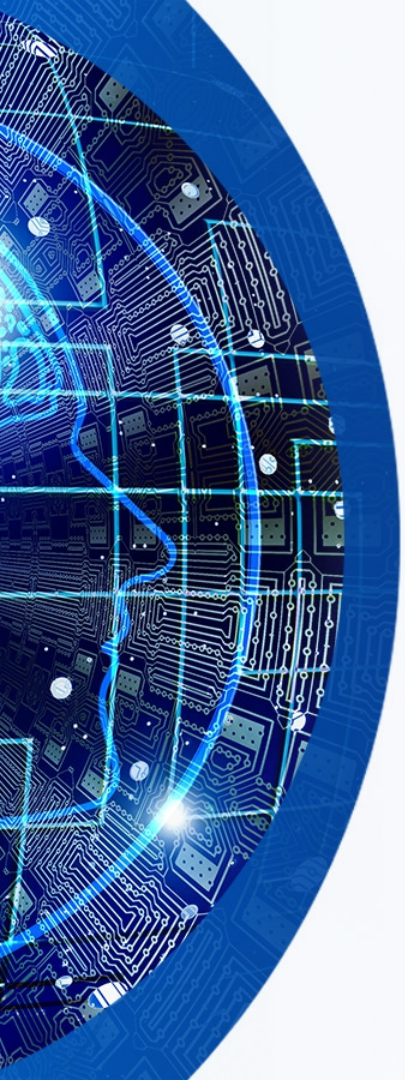
APE Server	
Hardware details	x86
Core >2GHz	16C (32vCore)
DRAM > 2400MHz	128GB
NVMe SSD's	6 X 480 GB >30000/10000 IOPS
LTS(1 Year)	8TB HDD

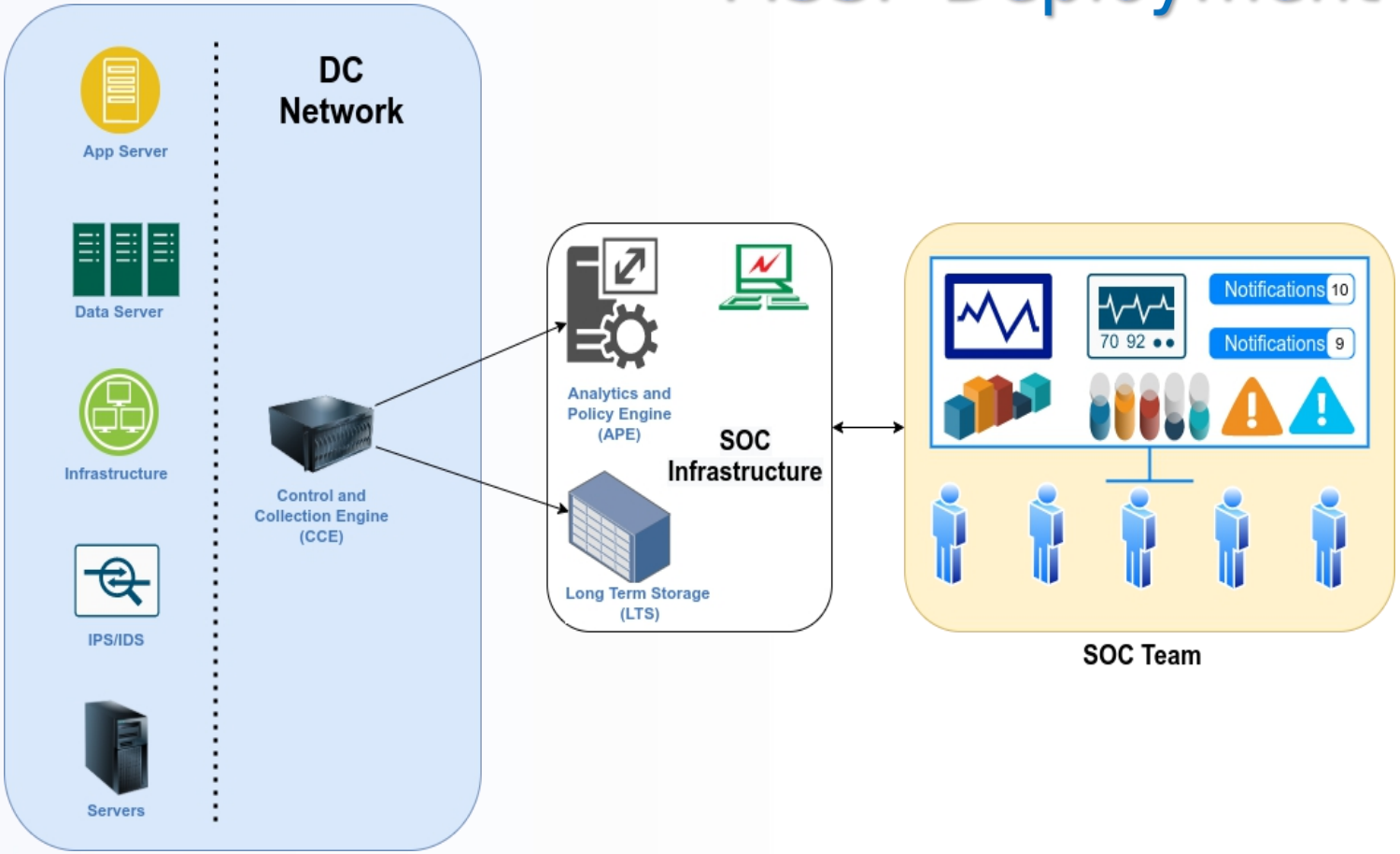
CCE	
Compute	4 CPU
RAM	4GB
Disk	300 SDD
Network Interface	1 GigE

LTS	
Compute	4 CUP
RAM	8GB
HDD	1 TB
Storage LTS (1 Year)	8TB HDD (usable)
Network Interface	1 GigE

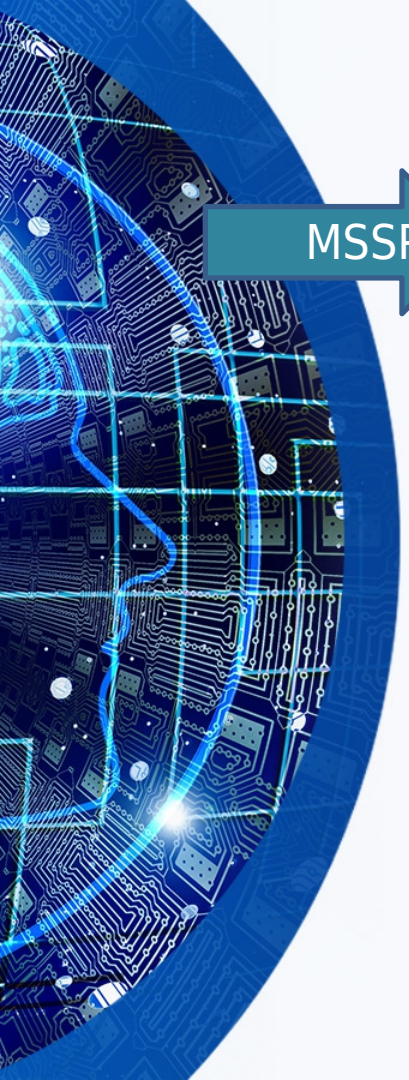
*** Assumption: Hardware Sizing considering 80 Servers Log Collection and 20 Network device**

MSSP-Deployment





On-Prem vs MSSP Deployment



MSSP

Advantages

- Avoid capital expenses
- Offer cheaper than in-house
- No Collusion between business operations and security operation
- Good security people provide service
- Good SLA

Disadvantages

- The contractor will never know your environment as an internal employee
- Sending job outside required good governance
- Risk of external data mishandling

... VS...

On-Prem

Advantages

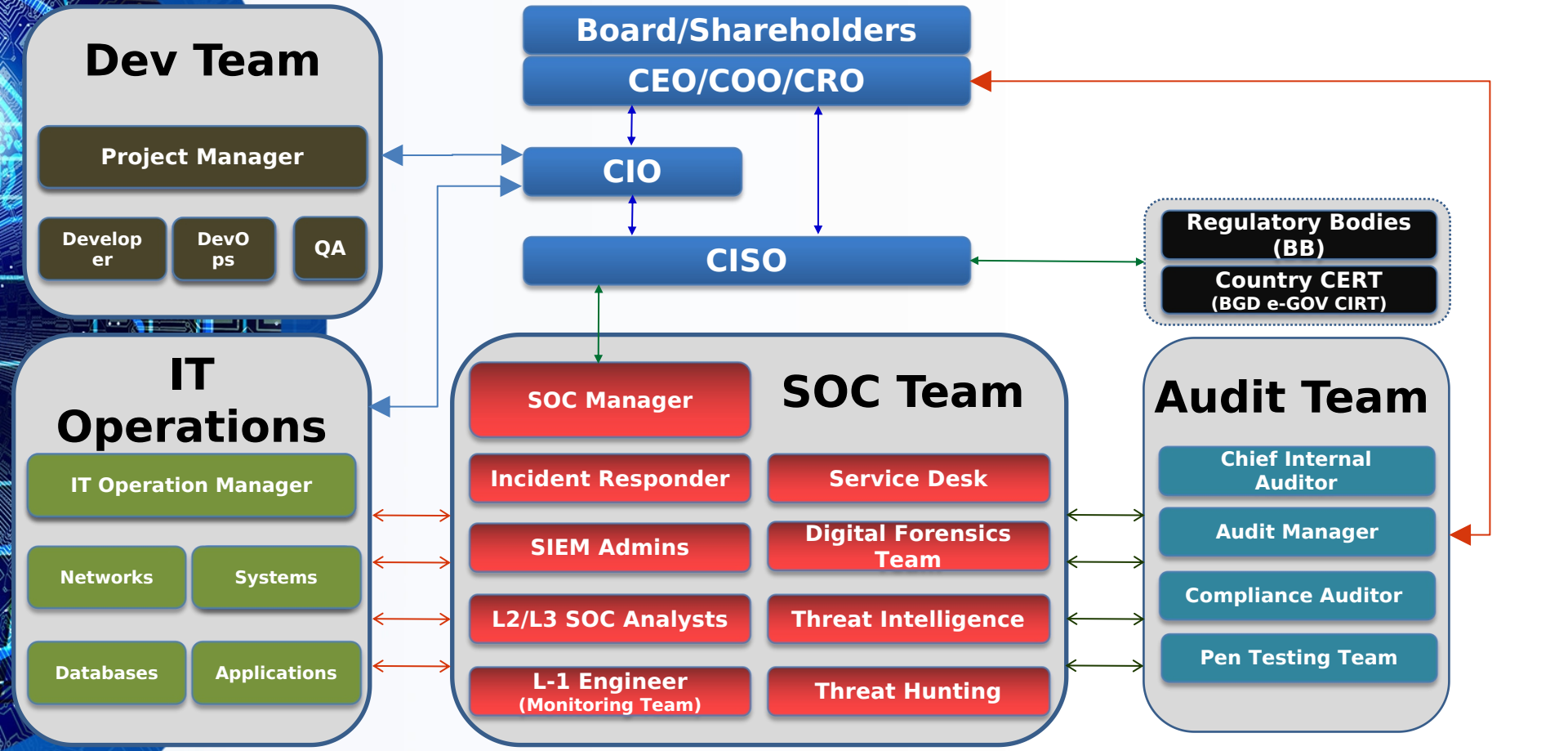
- Know the environment better than a third party
- Data are stored in the Organization

Disadvantages

- Larger up-front investment
- Higher pressure to show ROI quickly
- Focus on IT Security and IT Operation become difficult
- Aditional responsibility to manage SOC Infrastructure

SOC Organization Structure and Functions

SOC organization associated roles and responsibilities should be clearly defined



Thanks

Question & Answer