kyndryl

Domanda 1: Cyber Operations Center

Kyndryl Italy Cyber Operations Center - In a nutshell

People & Organizations

+170 Italy Security e Resiliency Professionals

Engage

- Specialty Sellers
- Tech Sales
- Solutions
- Consulting

40

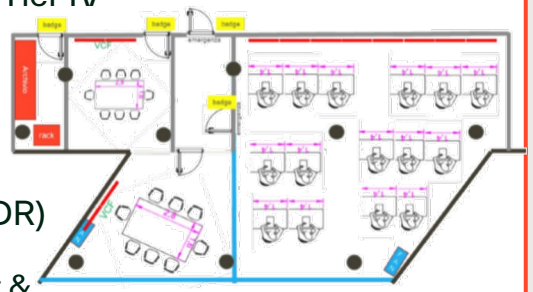
Deliver

- Technical Specialists
- L1/L2 analysts
- Cyber Experts
- Security Service Manager
- CTRAC

130

Cyber Operation Center

- **Control Room** operating 24x7 hosted in Tier IV DC in Rome
  - Facilities Redundancy
  - Multi Level Access Control
  - Building built wit anti-seismic criteria
  - 24x7 Supervision
- **Managed Platform** (SOAR, SIEMs, EDR)
- **Cyber Security Labs**
  - SOC Lab (Offense and Playbook Test & Validation)
  - Malware Lab (Malware analysis, threat detonation, Sandbox analysis)



Certifications & Skills

Kyndryl Italia

- ISO 9001
- ISO 20000
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 14001
- ISO 14064
- ISO 22301
- ENISIA Good Practice
- NIST800 Series

Practice Skills

- SOC Analyst
- SIEM experts
- SOAR experts
- Cyber Threat Intelligence
- Network Security
- Cyber Security Specialist
- Vulnerability Mgmt Analyst
- Project and Service Mgmt

Main Certifications

- Vendor Certifications (Fortinet, PaloAlto, CheckPoint, Akamai, Qualys, ...)
- Professional Certifications (CISSP, CISM, GIAC-GDAT & GCIH, CEH, CIS, Compitia Security+, ...)

180+ Security Vendor & Professional Certifications

Complete Cyber & Resilience Portfolio

Anticipate

- Risk Assessment
- Advisory Services
- Vulnerability Mgmt
- Red Teaming
- Phishing Awareness & Education

Protect

- EDR/XDR
- NDR
- Identity Management
- Privileged Access Management
- Zero Trust Network Access

Withstand

- Advanced Threat Detection
- Ticketing & Reporting
- Threat Intelligence (Early Warning, Bulletin)
- Threat Hunting
- Malware Analysis

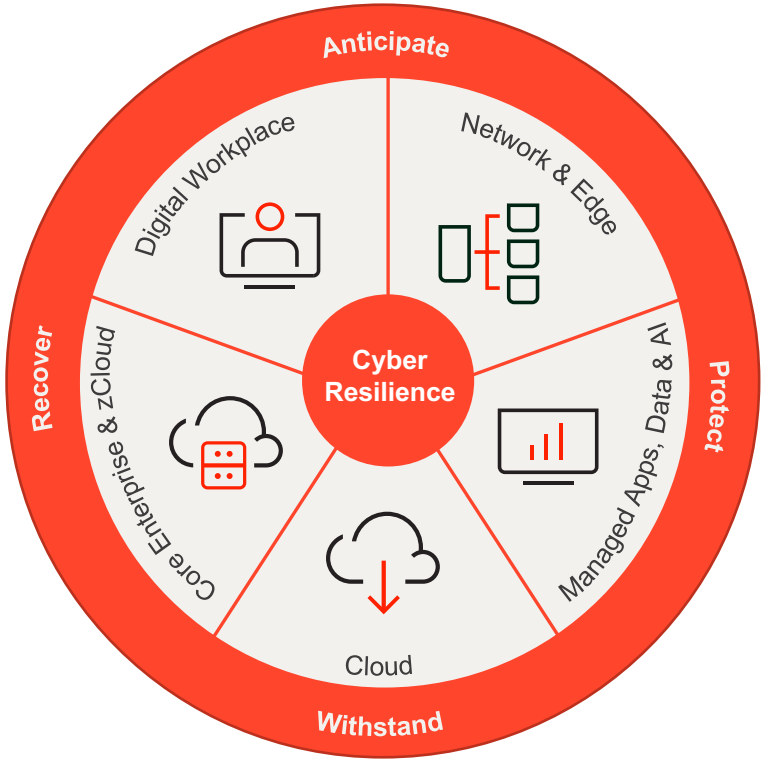
Recover

- Cyber Incident Recovery
- Managed Backup Services
- Hybrid Platform Recovery

kyndryl

Domanda 2: Cyber Incident Recovery

Framework to help anticipate and mitigate adverse cyber events



Security Assurance Services

Maintain compliance via consistent application of policies and controls

Zero Trust Services

Secure digital transactions with a zero-trust architecture

SOC Response Services

Discover, prevent and respond to advanced security incidents

Incident Recovery Services

Discover, prevent and respond to advanced security incidents

Anticipate → Protect → Withstand → Recover

Cybersecurity + Recovery

Deep expertise | Proven processes | Intelligent automation

kyndryl