kyndryl

Security Operations Center Roma

Security Operations Center: proteggiamo la tua azienda dalle minacce informatiche 24/7

Il Security Operations Center è un centro avanzato per la gestione della cybersecurity dove operano risorse altamente qualificate che si occupano della gestione operativa e del monitoraggio degli eventi di sicurezza. Gli esperti di cybersecurity operano 24 ore su 24, sette giorni su sette sulla base delle segnalazioni di eventi di sicurezza che devono essere gestiti, classificati e risolti velocemente.

Il centro si trova a Roma, all'interno di un Data Center Tier IV, sicuro e affidabile.

La struttura risponde alle esigenze di supporto e protezione per l'intero ciclo di vita delle minacce: dall'identificazione al ripristino delle condizioni iniziali, facendo leva su una piattaforma di orchestrazione e automazione, che permette, anche grazie all'integrazione con le fonti di Threat Intelligence, di analizzare velocemente gli eventi e rispondere efficacemente all'attacco.

I valori distintivi del centro sono:

- **L'ampio portafoglio di servizi**, che integra **Cybersecurity e Resiliency**, per coprire tutte le fasi di un attacco informatico: anticipare, proteggere, resistere, rispondere alle compromissioni e ripristinare le condizioni precedenti all'incidente.
- **La piattaforma di automazione e di orchestrazione** dei processi di identificazione dell'incidente e della relativa risposta, che riduce il lavoro di routine degli analisti che possono così concentrarsi su attività più complesse e rispondere agli attacchi più efficacemente.
- **Il network globale,** che consente una visione e una gestione internazionale del cyber crime.
- I centri di competenza per attività di **Red Teaming**, che operano a livello globale e che hanno una solida esperienza nei diversi settori merceologici.
- **Il Malware Lab**, un ambiente completamente isolato dalle infrastrutture operative, dedicato all'analisi del codice malevolo e allo studio di nuove tendenze di attacco.
- **L'ecosistema di partner**, che oltre ai maggiori hyperscaler, comprende i più importanti vendor di tecnologia di sicurezza.

I nostri servizi avanzati per la sicurezza della tua azienda

Il portafoglio di offerta Security & Resiliency ricalca il security framework del NIST *(National Institute of Standards and Technology)* coprendo tutte le sue cinque fasi *(Identify, Protect, Detect, Respond, Recover)*.

Security Assurance Services

Servizi di consulenza per valutare la maturità e la completezza delle soluzioni adottate, per confrontare il livello di maturità dei servizi rispetto a modelli e best practice e per fornire supporto per la gestione della compliance.
(Security, Strategy & Risk Management, Offensive Security Testing e Compliance Management).

SOC Response Services

Servizi di monitoraggio, di gestione degli incidenti di sicurezza e di risposta alle minacce.
(Event Monitoring, Incident Detection and Investigation, Incident Triage, Incident Management, Threat Intelligence).

Zero Trust Services

Servizi per aumentare la postura di sicurezza aziendale che si concentrano sulla gestione degli accessi alle applicazioni e ai dati e sulla protezione dei device e della rete.
(Identity & Access Management, Privileged Access Management, Endpoint Security (MDR, XDR), Network Security (NDR, Microsegmentation, Zero Trust Network Access), Application & Workload Security, Data Protection & Privacy).

Incident Recovery Services

Servizi per mitigare l'impatto di un incidente, per ripristinare velocemente i dati aziendali critici e per garantire la resilienza delle infrastrutture logiche e fisiche.
(Cyber Incident Recovery, Managed Backup Services, Hybrid Platform Recovery e Data Center Design & Facilities, Cyber Incident Recovery, Managed Backup Services, Hybrid Platform Recovery, Site, Facilities and Data Center Service).

Il Malware Lab, per essere sempre pronti ai nuovi attacchi.

All'interno del Security Operations Center è presente anche il Malware Lab, un ambiente completamente isolato dalle infrastrutture operative, dedicato all'analisi del codice malevolo e allo studio di nuove tendenze di attacco.

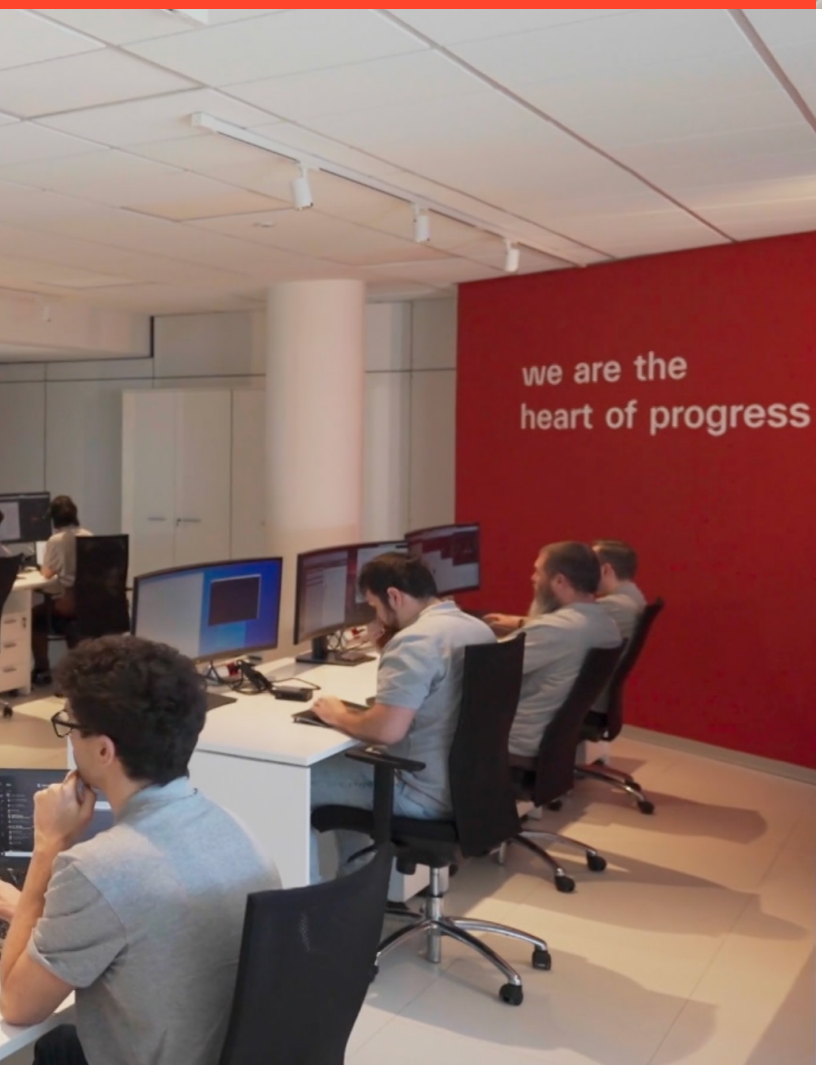
L'analisi del malware ha l'obiettivo di comprendere tempestivamente le caratteristiche degli attacchi (tattiche, tecniche e procedure, fasi, tempistiche, target) per migliorare la capacità di osservazione, rilevamento e risposta del Security Operations Center.

Malware Lab – attività principali

- **Esecuzione di file sospetti**
- **Analisi manuali**
- **Osservazione del malware sul lungo periodo**
- **Test delle capacità tecnologiche difensive**
- **Exploit di vulnerabilità**

Kyndryl's Security Operations Centers are built for the modern needs of cybersecurity teams by incorporating flexibility at the core. Traditional security operations centers are rigid - they often implement a one-size-fits-all approach and don't adapt to the changing needs of the business. Our Security Operations Centers provide the flexibility to centralize existing security investments, leverage hybrid teams, and continuously adapt for the changing threat landscape.'

Kris Lovejoy,
Global Practice Leader
Kyndryl Security & Resiliency Practice



Il Security Operations Center in breve

Security Operations Center Roma
via Giacomo Peroni, 292 – Roma

- Servizi di cybersecurity attivi 24/7
- Progettato all'interno di un Datacenter Tier IV
- +170 esperti di cybersecurity, 7.500 a livello globale
- +180 certificazioni
- +70 clienti italiani ed europei in ambito cyber resilience
- Certificazioni ISO: ISO9001, ISO20000, ISO27001, ISO27017, ISO27018, ISO14001, ISO14064, ISO22301
- Standard di riferimento: NIST CSF, MITRE ATT&CK, Enisa, SOC-CMM

Contatti

Federico Botti
Vice President Security & Resiliency Practice, Kyndryl Italia
Federico.Botti@kyndryl.com

Piero Poce
Associate Director Customer Technology Advisor,
Security & Resiliency, Kyndryl Italia
Pierfrancesco.Poce@kyndryl.com

Andrea Boggio
Associate Director Alliances,
Security & Resiliency, Kyndryl Italia
Andrea.Boggio@kyndryl.com

Alessio Gabrielli
Security Operations Center Manager,
Security & Resiliency, Kyndryl Italia
Alessio.Gabrielli@kyndryl.com

Guido Montalbano
Senior Lead, Customer Technology Advisor
Security & Resiliency, Kyndryl Italia
Guido.Montalbano@kyndryl.com

Kyndryl

Kyndryl è il leader mondiale nell'ambito dei servizi gestiti per le infrastrutture ibride.
Opera in 63 paesi e ha circa 90mila dipendenti. Progetta, gestisce e modernizza sistemi mission-critical, fondamentali per il business e per la capacità competitiva di aziende d'ogni settore. Conta migliaia di clienti su scala globale che includono il 75% delle aziende Fortune 100 e oltre la metà di quelle Fortune 500.
https://www.kyndryl.com/it/it

Security Operations Center

via Giacomo Peroni, 292 - Roma

Per saperne di più visita il sito:

https://www.kyndryl.com/it/it/services/cyber-resilience/security-operations/center/italy

Kyndryl Security & Resiliency

Kyndryl Security & Resiliency fornisce supporto e protezione per l'intero ciclo di vita delle minacce. I servizi che offre comprendono l'identificazione dei rischi, l'intelligence sulle minacce guidata dall'intelligenza artificiale, la gestione delle vulnerabilità, il rilevamento di incidenti e l'individuazione delle strategie di risposta e di mitigazione degli attacchi, fino alla protezione dei dati e il ripristino degli stessi in condizioni di emergenza.

La divisione Kyndryl Security & Resiliency conta a livello mondiale oltre 7.500 professionisti, più di 475 brevetti e un portafoglio di migliaia di clienti.

In Italia, l'unità ha più di 170 professionisti e oltre 180 certificazioni.

https://www.kyndryl.com/it/it/services/cyber-resilience