kyndryl

Security Operations Center Services Kyndryl Point of View

Indice

Executive Summary

Dalla costituzione dell'azienda, Kyndryl è entrata nel mercato dei servizi informatici con la divisione Security & Resiliency che oggi conta su un'organizzazione di **oltre 7.500 professionisti, +475 brevetti e un portafoglio di più di 4.000 clienti**. Kyndryl Security & Resiliency, con la sua blueprint di riferimento e il suo modello operativo, si confronta nel mercato competitivo con un ampio livello di certificazioni e un consolidato rapporto con i leader tecnologici e un ecosistema di Cloud provider (AWS, Azure, Google Cloud Platform, Oracle Cloud Infrastructure).

La direttiva strategica di Kyndryl ritiene determinante il ruolo della Security & Resiliency per la modernizzazione dei servizi e dei sistemi legacy e per il successo delle trasformazioni informatiche verso il Cloud. In Italia, la practice si posiziona con **+170 professionisti** ed è protagonista di un continuo e progressivo rafforzamento di nuove competenze. Tra i servizi centralizzati offre il proprio Security Operations Center evoluto, 7×24 con Threat Intelligence e sistemi di automazione integrati. Il portfolio dei servizi centralizzati si estende con ulteriori opportunità di *Zero Trust, Incident Response e Consult Services*.

Oggi tutte le organizzazioni informatiche hanno costituito o delegato un impianto di monitoraggio della sicurezza tramite un Security Operations Center con il primario obiettivo di **intercettare attacchi informatici e di rispondere tempestivamente**, mitigando i rischi di sicurezza. I settori d'industria sono guidati da normative sempre più stringenti per la prevenzione, il monitoraggio e il ripristino di possibili attacchi cyber. Le aziende sono inoltre sottoposte a sostenere verifiche degli Auditor Cyber, sia dalle funzioni interne che quelle esterne di settore, e si esercitano a verificare periodicamente il proprio stato di salute tramite i servizi di Red Team.

Il Red Team, antagonista del Security Operations Center, è composto da esperti di sicurezza di tipo ethical hacking che simulano gli attacchi delle minacce esterne con lo scopo di identificare vulnerabilità e debolezze nella sicurezza aziendale. Svolgono attività come *penetration testing, phishing, social engineering*, attacchi a infrastrutture e applicazioni per aiutare le organizzazioni a migliorare la loro difesa e prevenire attacchi reali. Il loro compito è quello di fornire una valutazione obiettiva e indipendente delle capacità di sicurezza aziendali.

Kyndryl, infatti, osserva le continue sfide dei CISO e dei Cybersecurity Manager nel gestire l'aumento dei rischi informatici, nella necessità di migliorare l'efficienza operativa, nell'affrontare l'adeguamento alle nuove norme di sicurezza, l'integrazione con nuove tecnologie, l'aumento del carico di lavoro, il cambiamento delle esigenze aziendali e nel gestire l'estensione della superficie d'attacco e le nuove minacce, anche derivate dall'innalzamento dei servizi digitali e dall'adozione del Cloud.

Le aziende sono attente nel valutare le effettive prestazioni e i costi d'esercizio del loro servizio di Security Operations Center e si preparano costantemente a valutare alternative quando uno o più fattori si evidenziano nell'erogazione del servizio in corso:

1. prestazioni insufficienti o inefficacia nei risultati del servizio;
2. costi d'esercizio elevati o non corrispondenti all'aspettativa;
3. inadeguato supporto tecnico e d'ingegneria Cyber;
4. scarse conoscenze per l'integrazione con altre soluzioni di sicurezza cyber;
5. utilizzo di infrastrutture tecnologiche obsolete e/o difficili da integrare nell'ecosistema della sicurezza;
6. sofferenza nell'industrializzazione operativa del servizio;
7. insufficienza o mancanza di risposta a funzionalità emergenti.

Per fronteggiare questo scenario serve innanzitutto approcciare il problema della *security defence* in **modalità estesa**, focalizzando l'attenzione non solo sulle infrastrutture IT, ma anche sui dipendenti e sui processi aziendali. Per tale ragione serve costruire una squadra forte e vincente, un teamwork competente, costantemente aggiornato ed efficiente nell'operatività perché dotato di strumenti tecnologici all'avanguardia, con un governo del servizio puntuale e metodologico.

Realizzare da soli tutto questo è decisamente complicato e oneroso in quanto comporterebbe impatti sull'organizzazione e richiederebbe investimenti economici importanti. Le aziende, infatti, si trovano oggi sempre più a dover concentrare la loro forza lavoro sull'evoluzione del proprio core business, piuttosto che sulla gestione della sicurezza. Il doversi dotare inoltre di piattaforme software evolute per poter erogare le attività operative, così come formare e/o assumere competenze esperte aggiornate sulle evoluzioni delle minacce informatiche, ha un impatto non banale sui costi e spesso risulta non sostenibile per i budget IT delle aziende.

A tal proposito nasce l'esigenza di affidarsi alla collaborazione di partner strutturati, credibili e specifici del settore, denominati **MSSP (Managed Security Service Provider)**, che siano in grado di erogare servizi evoluti a protezione della cybersecurity e di mettere a disposizione del cliente tutta la loro esperienza e/o asset con l'obiettivo di contribuire a garantire protezione dagli incident di sicurezza e conseguentemente la resilienza delle infrastrutture e dei dati di un cliente.

Kyndryl Security & Resiliency fornisce le competenze, i servizi e le tecnologie che aiutano le aziende ad anticipare, proteggere, resistere e riprendersi da condizioni avverse, stress, compromissioni dei servizi a causa di attacchi cyber, fornendo una copertura non solo proattiva (identificare e proteggere) e reattiva (rilevare e rispondere), ma anche adattativa (recupero veloce a seguito di un attacco di sicurezza).

Introduzione

Oggi le aziende e le pubbliche amministrazioni sono coinvolte in una continua trasformazione digitale del proprio business; per massimizzarne i benefici e cogliere tempestivamente le opportunità offerte dal nuovo scenario di mercato, devono poter fronteggiare un insidioso pericolo: le minacce digitali di varia natura al business e ai servizi critici pubblico/privati, sempre più sofisticati, diversificati e frequenti. Da questa minaccia nessun comparto merceologico può considerarsi al sicuro e tutto ciò mette soprattutto a rischio gli elementi che possono considerarsi il patrimonio più importante per un'azienda: le persone, la revenue, i dati (sia personali sia funzionali al sostentamento del business) e la reputazione del brand.

Affrontare la complessità di un tale fenomeno impone un approccio olistico per individuare le superficie di attacco e l'adozione di soluzioni puntuali che indirizzino tutte le potenziali esposizioni dell'azienda, inclusi i propri dipendenti, e il rispetto delle leggi e delle regolamentazioni in materia, onde evitare che la situazione degeneri improvvisamente con grave danno per l'azienda.

Analizzando le cause che hanno portato a questa nuova situazione possiamo evidenziare tre elementi principali, introdotti dal processo di *digital transformation*:

1. **L'evoluzione delle infrastrutture IT**, sempre più complesse e articolate, verso modelli ibridi (on-premise/Cloud) per permettere l'integrazione di applicazioni e di dati a vantaggio della flessibilità e della scalabilità di una azienda, rendendola accessibile da molteplici sorgenti e senza limitazioni di tempo *(everytime/everywhere)*. Il sempre più ricorrente ricorso alle infrastrutture erogate dai principali hyperscaler impone di riconsiderare complessivamente la sicurezza informatica, cogliendo al massimo le opportunità tecnologiche offerte dagli stessi hyperscaler per indirizzare al meglio la *Cloud Security Posture*, la sicurezza di *Cloud Workload* e di *Cloud Native Applications*.
2. **I nuovi modelli organizzativi nelle aziende**, che sempre più vengono adottati con l'obiettivo di supportare al meglio la trasformazione digitale anche della propria forza lavoro, che diventa fluida e agile per favorire l'operatività in mobilità (es. smartworking), un fenomeno già in corso e accelerato dalla recente pandemia.
3. **Lo sviluppo del business del cyber crimine** come elemento di business parallelo, costituito da organizzazioni industrialmente ben strutturate nell'individuare nuove vulnerabilità e nel predisporre nuove tecniche di attacco, motivate da obiettivi non solo di raggiungimento di enormi guadagni, ma spesso anche di tipo strategico/politico.

Tali cause hanno incrementato sia la tipologia, sia il numero di accessi ai vari servizi di una azienda e di conseguenza anche il rischio di attacchi alla sicurezza informatica da parte degli hacker. Se si considera il numero crescente sia dei dispositivi oggi connessi a internet (smartphone, notebook, laptop o dispositivi IoT) che dei nuovi software malevoli (ransomware, cryptolocker, virus, worm e trojan), è possibile prevedere che, in prospettiva, le minacce alla sicurezza informatica saranno sempre più numerose e sofisticate tanto da richiedere risposte immediate per essere neutralizzate prima che diventino un pericolo serio per il business dell'azienda. Il tema è quindi complesso da affrontare anche perché in trasformazione ed evoluzione continua, quindi difficilmente prevedibile.

In questo scenario, un altro aspetto importante a cui porre attenzione, è quello legato al **rispetto delle regolamentazioni governative** in materia di salvaguardia e di integrità dei dati e delle infrastrutture. La regolamentazione impone già oggi alle aziende di assumere tutte le possibili precauzioni per proteggere le informazioni sensibili da attacchi informatici, ma al crescere delle minacce informatiche anche lo scenario regolatorio evolverà imponendo sempre più l'adozione di contromisure adeguate in termini di servizi e di process idi controllo e di governance. Ad esempio, le prossime direttive europee per la cybersecurity (es. l'attuazione di NIS2) imporranno a imprese e Pubbliche Amministrazioni di potenziare la capacità di reazione e di risposta ad attacchi informatici attraverso un nuovo insieme di standard minimi di cybersecurity che dovranno essere assimilati dalle normative dei singoli Paesi.

Questo scenario, così articolato e mutevole, impone oggi alle organizzazioni di percorrere un processo di trasformazione della propria sicurezza informatica tramite l'adozione di soluzioni (tecnologie e servizi) per la sicurezza IT che risultino ritagliate sulla propria realtà, continue e progressive nel tempo con l'obiettivo di tenere costantemente allineata l'azienda alle evoluzioni del proprio business e al mercato di riferimento, con investimenti economici proporzionati a questo contesto.

La spinta accelerata alla digitalizzazione ha introdotto nuove priorità per i CISO/CTO, come la resilienza informatica, la regolamentazione, la conformità e la carenza di competenze reperibili sul mercato del lavoro. Le organizzazioni devono essere preparate in termini di resilienza operativa per garantire di poter fornire servizi aziendali critici in caso di interruzioni.

I Security Operations Center sono strutture operative che lavorano in modalità h24 e mettono a disposizione dei clienti un insieme di risorse con competenze ed esperienze nell'ambito del monitoraggio, dell'identificazione e della gestione degli incidenti di sicurezza. Grazie all'utilizz odi tecnologie *best-of-breed*, al monitoraggio di feed OSINT e CLOSINT di *threat intelligence* e a lab destinati alla sperimentazione di nuove tecniche di attacco o alla riproduzione di incident per l'individuazione della corretta root cause analysis, i centri sono in grado di governare con competenza ed efficienza la gestione della sicurezza delle infrastrutture e dei servizi mission critical dei clienti. Sono importanti le partecipazioni e le condivisioni di **Information Sharing and Analysis Center (ISAC)**, come i centri European Union Agency for Cybersecurity (ENISA) e Center for Internet Security (CIS).

I benefici attesi

Nel definire il valore e i benefici offerti dal Security Operations Center di Kyndryl, le attenzioni primarie si sviluppano nel **governare il rischio cyber** dell'intero perimetro interno ed esterno dell'azienda, **rispettare le conformità di sicurezza** a normative e regolamenti d'impresa e di settore, **identificare e rispondere rapidamente** a eventuali minacce, **evidenziare esposizioni di sicurezza** cyber e di protezione dei dati sensibili dell'azienda, elaborare **piani per la prevenzione** di futuri attacchi e disporre di una **efficacia estrema** nella gestione delle attività di Security Operations Center.

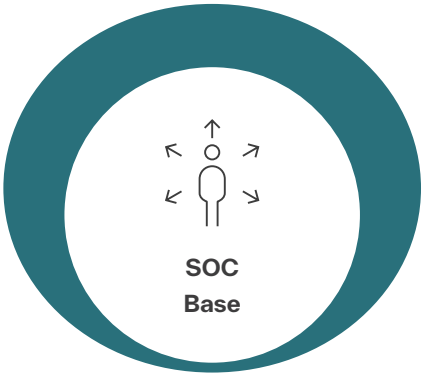
Le prestazioni e l'efficacia di un Security Operations Center si misurano secondo tre direttrici:

1. Disporre di una ***buona tecnologia*** per la raccolta, il monitoraggio e la correlazione degli eventi di sicurezza dell'intero perimetro informatico comunemente conosciuto come *Security Information and Event Management (SIEM)*. I SIEM di ultima generazione dispongono di moduli di *Artificial Intelligence* e di *Machine Learning* in grado di anticipare le interpretazioni malevole già all'intercettazione di segnali apparentemente deboli. Vedremo di seguito che impianti evoluti mettono a disposizione tecnologie complementari per l'orchestrazione e l'automazione dei possibili incidenti tramite le piattaforme di *Security Orchestration and Automation Response (SOAR)*. Tra le recenti tecnologie, in progressiva adozione, ci sono le piattaforme di tipo *eXtended Detection and Response (XDR)* in grado di raccogliere e confrontare la telemetria nell'intero ambiente informatico, lo scambio dei dati tra endpoint, e-mail, reti, server, parametri di identità, accessi e ambienti cloud. L'XDR rileva, correla, contestualizza e dà priorità ai dati e agli alert raccolti attraverso l'intelligenza artificiale (AI), l'apprendimento automatico (ML) e l'analisi comportamentale e dà una risposta cyber accurata ed efficace.
2. Dotarsi ***di un'ingegneria Cyber di alto livello*** per analizzare i fenomeni di compromissione, tenendo conto delle evoluzioni degli indicatori di compromissione, che possono essere facilmente modificati dagli aggressori. L'ingegneria Cyber sviluppa l'adozione di tecniche di rilevamento basate sulle tattiche, sulle tecniche e sulle procedure per dare a ldifensore un maggiore potere. Inoltre, provvede alla continua integrazione di fonti di dati interne ed esterne per aumentare la consapevolezza delle minacce e la capacità di rispondere. L'ingegneria Cyber risponde anche all'adeguamento delle regole e delle correlazioni per tenere conto dei cambiamenti nelle applicazioni aziendali, dell'integrazione di nuove tecnologie e dell'adozione del cloud. Infine, mantiene e sviluppa i playbook per la gestione quotidiana delle minacce cyber.
3. Realizzare ***un'eccellente macchina operativa*** per garantire un servizio 7×24 che includa funzioni operative di Livello 1 per l'analisi e il monitoraggio *(Triage)*, di Livello 2 per l'analisi degli incidenti elaborati dal Livello 1 con l'identificazione delle azioni di rimedio *(Incident Containment)* e di Livello 3 con la responsabilità di rispondere agli incidenti *(Incident response)* con capacità di analisi profonde e specializzate negli aspetti del monitoraggio ella sicurezza *(Malware analysis, Packet capture analysis, Deep complex threat hunting for advanced threats)*. L'efficacia dell'operatività, nei termini di organizzazione, processi e reporting, sono orchestrati e automatizzati dalle piattaforme di *Security Orchestration and Automation Response (SOAR)*.
I centri evoluti si fanno carico di funzioni e attività convenzionalmente coordinate e supervisionate ad altri organi di cybersicurezza, come il CSIRT *(Computer Security Incident Response Team)* o il CERT *(Computer Emergency Response Team)*.

La visione del mercato di Kyndryl

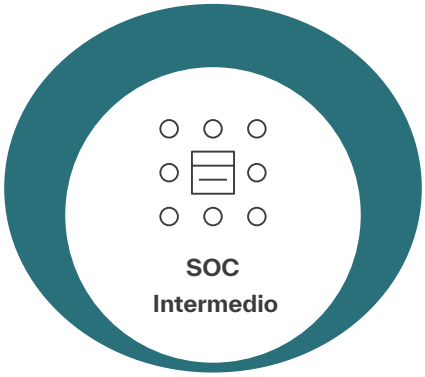
Kyndryl osserva sul mercato diversi livelli di adozione dei Security Operations Center con diversi gradi di maturità, di relativa prestazione operativa e di complessità funzionale, che danno una vista tridimensionale del servizio. Per convenzione e semplificazione identifichiamo tre gradi di adozione (Base, Intermedio, Avanzato) che rispondono a esigenze temporanee/attuali, ma che nella maggior parte dei casi, stanno evolvendo per rispondere a una continua necessità di abbattimento/mitigazione del rischio di sicurezza.

1. **I Security Operations Center di tipo base** utilizzano prevalentemente una piattaforma *Security Information and Event Management (SIEM)* che integra eventi e log di sicurezza da fonti primarie dell'informatica (Server, Network Security, Sistemi di IPS/IDS, Sistemi di Identity, Database, Applicazioni, antivirus...). L'operatività è tipicamente di Livello 1 e di Livello 2 con un presidio giornaliero e in escalation per il fuori orario e festivi. L'attività forense di risposta agli incidenti *(Incident Response & Forensic Analysis)* è tendenzialmente ad hoc e su richiesta.
2. **I Security Operations Center di tipo intermedio** utilizzano prevalentemente una piattaforma *Security Information and Event Management (SIEM)* che, in aggiunta al modello Base, integra la *Threat Intelligence*, opera con sistemi di analisi comportamentale *(User Behavior Analytics)* e migliora la vista cyber complessiva con fonti di tipo *Endpoint Detection and Response (EDR)* e *Network Detection and Response (NDR)*. L'operatività di Livello 1 e di Livello 2 ha caratteristiche 7×24 con l'adozione anche di un framework di *Threat Hunting*. L'attività forense di risposta agli incidenti *(Incident Response & Forensic Analysis)* è tendenzialmente erogata da entità esterne al Security Operations Center.
3. **I Security Operations Center di tipo avanzato** utilizzano prevalentemente una piattaforma *Security Information and Event Management (SIEM)* evoluta con funzionalità di *Artificial Intelligence* e di *Machine Learning*, che, in aggiunta al modello intermedio, integra l'orchestrazione e l'automazione operativa tramite le piattaforme di *Security Orchestration and Automation Response (SOAR)* e con un ulteriore arricchimento di tipo *eXtended Detection and Response (XDR)* per una risposta e un ripristino ad alte prestazioni. L'operatività si eleva con servizi di Livello 1, di Livello 2 e di Livello 3 con caratteristiche 7×24 e una maggior maturità d'adozione di un framework di *Threat Hunting*. Il servizio avanzato offre anche una possibile diversificazione di priorità, in base al contesto applicativo, di business line o di legal entity per la mitigazione degli impatti prevalenti, nel contesto del cliente. Oltre all'integrazione della *Threat Intelligence*, si eseguono anche attività di analisi proattiva di tipo *Cyber Early Warning* ed esecuzioni di campagne di attacco simulato *(Simulation Attack)*. L'attività forense di risposta agli incidenti *(Incident Response & Forensic Analysis)* è offerta nel servizio avanzato.



Technology
SIEM

Operation
L1/L2 basic support in prime time and 24x7 availability only in escalation



Technology
SIEM
UEBA
EDR

Operation
L1//L2 24x7 support
L3 with basic Threat hunting capabilities

Technology
SIEM
XSOAR
XDR

Operation
L1/L2 24x7 support
L3 advanced Threat hunting capabilities, advanced Threat Intelligence Red Teaming exercise

Gli indicatori della gestione della complessità di un Security Operations Center si applicano sui tre modelli di adozione precedentemente illustrati, con una derivata differenziazione del peso complessivo.

I Key Indicators della complessità di un Security Operations Center sono riassunti di seguito:

KPI

Incident Analysis
Regole e correlazioni
Playbook
Falsi positivi
Incidenti (detected)

Infrastructure Perimeter
Casi d'uso cyber
Varietà dei Data Sources
Varietà degli ambienti gestiti
(Legacy / Distribuiti / Cloud)

SecOps
Rapporto operativo tra
Livello 1 - Livello 2 – Livello 3

SLA & Reporting
Stipula di SLA nei contratto
Grado di reporting

Kyndryl ha predisposto nel proprio Security Operations Center di Roma, nella modalità Avanzata, il più alto livello di risposta alla domanda di mercato, combinando l'insieme delle tecnologie più evolute, un'ingegneria Cyber di alto profilo e la capacità operativa 7×24 per rispondere alle sfide attuali e alle prossime d'integrazione degli ambienti Cloud e della trasformazione digitale.

L’approccio Kyndryl

Kyndryl ha costituito la practice Security & Resiliency, interamente dedicata all’erogazione di soluzioni di Cyber Resilience, in grado di fornire supporto e protezione per l’intero ciclo di vita delle minacce: dai servizi per l’identificazione dei rischi, l’intelligence sulle minacce guidata dall’intelligenza artificiale, la gestione delle vulnerabilità, il rilevamento di incident e l’individuazione delle strategie di risposta e di mitigazione degli attacchi, sino alla protezione dei dati e il ripristino degli stessi in condizioni di emergenza. I piani d’investimento sono in costante progressione nella formazione di risorse professionali per l’ingegneria Cyber e nell’operatività quotidiana. Anche l’adozione delle tecnologie è all’avanguardia.

L’ampio portafoglio dei servizi erogabili da Kyndryl si pone come obiettivo non solo quello di avere la capacità di analizzare per anticipare, proteggere, resistere, rispondere agli attacchi cyber che spesso impattano e compromettono la corretta erogazione dei servizi IT, ma anche quello di supportare il ripristino delle condizioni precedenti all’attacco, a salvaguardia del business di un’azienda.

Di seguito alcuni dei principali elementi distintivi con cui Kyndryl si pone come MSSP di riferimento per le aziende e le Pubbliche Amministrazioni:

ESPERIENZA GLOBALE

Il Security Operations Center di Kyndryl Italia trae vantaggio dalle esperienze globali di Kyndryl su come gestire gli attacchi informatici e implementare le migliori pratiche per la gestione degli incidenti.

PORTAFOGLIO DI SERVIZI ESTESO

Un portafoglio esteso di servizi di sicurezza per identificare, proteggere, rispondere e ripartire velocemente.

- Security Assurance Services
- SOC Response Services
- Zero Trust Services
- Incident Recovery Services

AUTOMAZIONE

Il portafoglio di servizi fa leva sulla tecnologia di orchestrazione, di automazione e di risposta (SOAR) per aumentare la produttività e l’efficienza degli analisti di sicurezza nella gestione degli incidenti.

INTEGRAZIONE TRA SECURITY E RESILIENCY

Combinare Sicurezza e Resilienza aiuta ad affrontare le minacce informatiche non solo in modo preventivo (identificare e proteggere) e reattivo (rilevare e rispondere), ma anche secondo una prospettiva adattiva (ripartire velocemente dopo un incidente di sicurezza).

1. **Presenza ed esperienza globale:** Kyndryl Italia è parte integrante di un'azienda che ha una dimensione globale, con circa 90.000 professionisti di cui oltre 7.500 focalizzati sui servizi di Security & Resiliency, e che gestisce migliaia di clienti in diversi settori merceologici (automobilistico, bancario e assicurativo, manifatturiero, Pubblica Amministrazione ,retail e Grande Distribuzione Organizzata, sanità e trasporti). Ciò consente di trarre vantaggio da esperienze quotidiane maturate nella gestione di attacchi informatici, nello sviluppo e nell'implementazione di best practice per la gestione delle attività di monitoraggio e di classificazione degli incident e di predisposizione delle strategie di risposta e di mitigazione degli attacchi, nella raccolta di feed e di informazioni di contesto relative a minacce e a potenziali attacchi grazie all'analisi delle fonti OSINT e CLOSINT di *Threat Intelligence* e nello sviluppo di soluzioni di automazione (playbook), integrando e gestendo le migliori tecnologie di orchestrazione e di automazione.
2. **Portafoglio di servizi esteso:** la practice Security & Resiliency, attraverso i suoi centri di competenza, è in grado di rendere disponibile un esteso portafoglio di servizi che ricalca il security framework di riferimento del NIST *(National Institute of Standards and Technology)* coprendo tutte le sue 5 fasi *(Identify, Protect, Detect, Respond, Recover)*:

   - **Security Assurance Services:** si tratta di servizi di assessment per valutare la maturità e la completezza delle soluzioni adottate, confrontare, rispetto a modelli e best practice, il livello di maturità dei servizi e fornire supporto per la gestione della compliance *(Security, Strategy & Risk Management, Offensive Security Testing e Compliance Management)*.

   - **SOC Response Services:** rientrano in questo gruppo tutti i servizi di monitoraggio e di gestione degli incident di sicurezza e i servizi di risposta alle minacce *(Event Monitoring, Incident Detection and Investigation, Incident Triage, Incident Management, Threat intelligence)*.

   - **Zero Trust Services:** Kyndryl adotta la metodologia Zero Trust che si basa sui principi fondamentali 'Mai fidarsi, verificare sempre – Valutare continuamente parametri funzionali alla postura di sicurezza – Applicare sempre il privilegio minimo'. Quindi, in questo contesto, rientrano tutti i servizi di *Identity & Access Management, Endpoint Security, Network Security, Application & Workload Security, Data Protection & Privacy (MDR, XDR, NDR, Microsegmetation, Identity Management, Privileged Access Management, Zero Trust Network Access).*

   - **Incident Recovery Services:** facendo leva sull'esperienza acquisita nella gestione IT di infrastrutture complesse e critiche, Kyndryl ha potuto maturare un insieme di competenze e di metodologie efficaci per mitigare l'impatto di un incidente e offrire la possibilità di ripristinare il prima possibile i dati aziendali critici. Pertanto, con *Cyber Incident Recovery, Managed Backup Services, Hybrid Platform Recovery e Data Center Design & Facilities*, Kyndryl consente di garantire ai clienti la resilienza delle proprie infrastrutture logiche e fisiche *(Cyber Incident Recovery, Managed Backup Services, Hybrid Platform Recovery, Site, Facilities and Data Center Service)*.
3. **Automazione e orchestrazione:** l'automazione e l'orchestrazione dei processi di analisi e di mitigazione è oggi un punto essenziale per garantire una gestione non solo reattiva ma anche proattiva della sicurezza, rendere più efficienti le attività di analisi e di classificazione degli incidenti da parte del personale di Operation e forni rerisposte immediate a fronte di azioni di compromissione delle infrastrutture dei clienti. Kyndryl ha sviluppato la propria struttura di Operation ponendo al centro della sua architettura una piattaforma di orchestrazione e di automazione, potente e flessibile, opportunamente programmata attraverso playbook sviluppati con competenze interne.
4. **Integrazione tra Security & Resiliency:** coniugando la Cybersecurity e la Resiliency, Kyndryl si posiziona in modo distintivo rispetto agli attuali principali MSSP, in grad odi affrontare la minaccia informatica non solo in modo preventivo (identificare e proteggere) e reattivo (rilevare e rispondere), ma anche secondo una prospettiva adattiva (recupero a seguito di un incidente di sicurezza). I servizi di Cyber Incident Recovery (CIR) consentono pertanto di avere una reazione rapida a ransomware e ad altri attacchi informatici una volta che hanno danneggiato dati e sistemi, consentendo alle aziende di poter ripartire con l'operatività dei sistemi mission critical in tempi rapidi e sicuri.

Grazie a una serie di accordi globali con i principali hyperscaler (AWS, Google Cloud, Microsoft, Oracle e VMware), con i fornitori di soluzioni infrastrutturali e a un ampio ecosistema costituito dai principali vendor di tecnologia di sicurezza e data protection, Kyndryl è in grado in modo distintivo di **supportare i clienti in un percorso di transizione end-to-end** volto ad aumentare il livello di controllo e di gestione della cybersecurity adottando tecnologie di ultima generazione in grado di offrire livelli di servizio in linea con le aspettative e facendo leva su consolidate best practice, relative alla gestione dei servizi, e su metodologie in grado di mantenere il controllo rispetto alla qualità dei servizi forniti.

Tutti questi fattori costituiscono l'elemento distintivo dei servizi gestiti di sicurezza di Kyndryl.

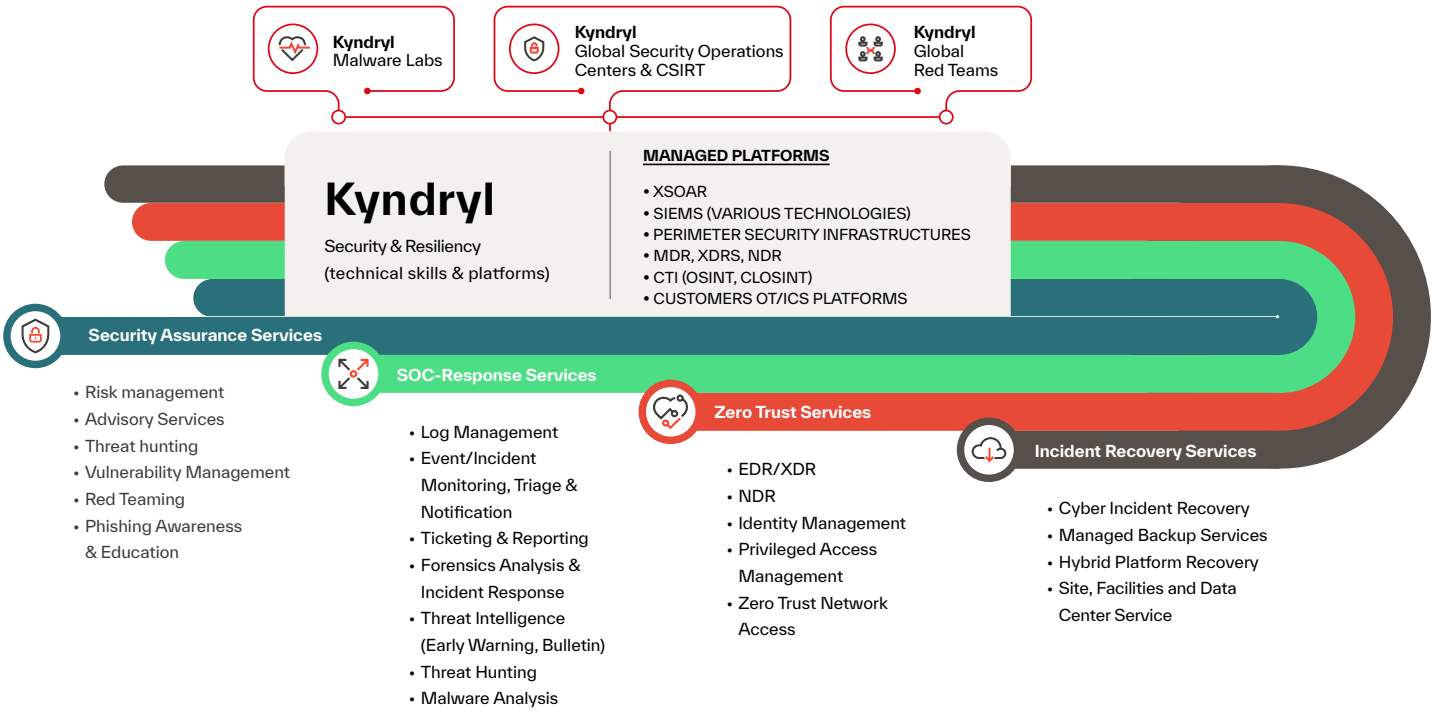
Il Security Operations Center è un centro di eccellenza per la gestione della cybersecurity operante sul nostro territorio nazionale, costituito da risorse con elevate competenze, certificazioni ed esperienze nell'ambito della cybersecurity che gestiscono piattaforme e tecnologie per assicurare la gestione operativa e il monitoraggio degli eventi di sicurezza (SIEM, SOAR, MDR, XDR, NDR, sicurezza perimetrale, fonti di threat intelligence sia OSINT sia CLOSINT, etc.)

Il fatto che il Security Operations Center di Kyndryl Italia sia parte del network dei centri di competenza sulla Security di Kyndryl Global, permette di beneficiare di una knowledge base in termini di gestione di incident di sicurezza che risulta misurata e provata su una vasta gamma di clienti di medio-grandi dimensioni in termini di numerosità di elementi infrastrutturali gestiti e di fatturato su scala globale, operanti in tutti i settori mercelogici, supportati da un CSIRT Kyndryl che, oltre a fornire evidenze sulle principali minacce e le linee guida da seguire, può fornire anche indicazioni operative nella attività di incident response, assicurando la governance della gestione degli incidenti di sicurezza in accordo alle policy e alle best practice Kyndryl. Inoltre, il Security Operations Center ha la possibilità di ricorrere a un Red Team Global, distribuito su più Paesi, con competenze e metodologie specifiche nella conduzione di attacchi pilotati alle infrastrutture clienti, al fine di verificarne le robustezze o i punti di potenziale vulnerabilità.

Un ulteriore punto di forza, che permette di evolvere continuamente la conoscenza e l'esperienza nel trattare attacchi informatici, è costituito dal **Malware Lab**, un centro di competenze interno al Security Operations Center, costituito da un ambiente completamente isolato dalle infrastrutture operative, nel quale un team di esperti è impegnato in attività di laboratorio a studiare nuove minacce, riprodurre attacchi noti per individuare e isolare vettori di attacco e livello di compromissione delle infrastrutture ed effettuare simulazioni di attacchi per testare contromisure automatiche per contrastarne gli effetti.

La Security Research è un asset importante del Security Operations Center nel continuo sviluppo di competenze ed esperienze che alimenta non solo il know how dei professionisti operanti nell'ambito del Design, Delivery e Operation, ma sviluppa soprattutto la capacità di interpretare velocemente i fenomeni critici e di sviluppare asset tecnologici per rendere più efficace e immediata la risposta.

Kyndryl Security & Resiliency Practice Services



Il valore di Kyndryl

La practice Security & Resiliency in Italia è costituita da circa 170 professionisti, suddivisi in figure di Delivery, Consult e Design, con competenze certificate negli ambiti SOC Analyst, SIEM Specialist, SOAR Specialist, Cyber Threat Intelligence, Cybersecurity Specialist in vari ambiti (Network Security, Cloud Security, EDR/XDR, NDR, IAM/PAM), System Management, Service Management, Project Management.

Kyndryl pone molta attenzione alla formazione dei propri professionisti, investendo in piani di learning e di aggiornamento continuo e nel conseguimento di certificazioni sia legate a vendor specifici, sia di tipo professionale in ambito cybersecurity.

L'intera practice in Italia può contare oltre 180 certificazioni conseguite nei seguenti ambiti:

- **Certificazioni Vendor,** come ad esempio Akamai/ Guardicore (GCSA, GCSE), Amazon (AWS Certified Fundamentals), Azure Security Engineer Associate, Checkpoint (CCSA, CCSE, CCSM), Fortinet (NSE 4, NSE 5, NSE 6, NSE 7), Google (Google Professional Cloud Architect), Microsoft Certified (Azure Fundamentals, Microsoft 365 Certified-Security Administrator Associate), Palo Alto (PCNSE, PSE), Qualys (Qualys Certified Specialist, Vulnerability Management)
- **Certificazioni Professionali** nell'ambito Cyber Security come CISSP, CISM, GIAC (GDAT, GCIH), CEH, EC-Counsil E-HA, MITRE ATTACK, CRISC, CGEIT, CDPSE, CISA, Comptia Security+, ISACA CSX Foundation, ISO 22301 BCMS, ISO 22301 Lead Auditor, ISO 27001 Lead Auditor, Certificazioni Professionali di Project e Service Management (ITIL v3, ITIL v4, COBIT, PMP, Prince2)

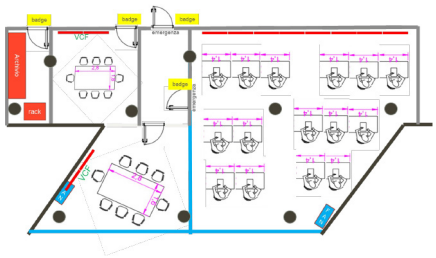
Kyndryl Security & Resiliency Practice Services - At a glance

People & Organizations

- +170 Italy Security e Resiliency Professionals
- Sales, Tech Sales & Consulting
- Delivery
- Operation

Security Operations Center Site

- The Control Room is hosted in Tier IV Data Center in Rome
- Facilities redundancy
- Building built with anti-seismic criteria
- Multi-level access control system
- Supervision of specialized technical personnel 24×7
- The Data Center site is connected at high speed with Tier IV DCs Pero and Castelletto where platforms are hosted



Kyndryl Italia Certifications

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

People Skills & Certifications

SKILLS	VENDOR CERTIFICATION	PROFESSIONAL CERTIFICATIONS	
• SOC Analyst • SIEM Specialist • SOAR Specialist • Cyber Threat Intelligence • Cybersecurity Specialist • Network Security • System Management • Service Management • Project Management	• Fortinet: NSE 4, NSE 5, NSE 6, NSE 7 Checkpoint: CCSA, CCSE, CCSM • Palo Alto: PCNSE, PSE • Qualys: Qualys Certified Specialist, Vulnerability Management • Akamai/Guardicore: GCSA, GCSE • Microsoft Certified: Azure Fundamentals, Azure Security Engineer Associate, Microsoft 365 Certified-Security Administrator Associate • Amazon: AWS Certified Fundamentals • Google: Google Professional Cloud Architect	• **CISSP** • **CISM** • **GIAC (GDAT, GCIH)** • **CEH** • **EC-Counsil E-HA** • **MITRE ATTACK** • **CRISC** • **CGEIT** • **CDPSE** • **CISA** • **Comptia Security+**	• **ISACA CSX Foundation** • **ISO 22301 BCMS** • **ISO 22301 Lead Auditor** • **ISO 27001 Lead Auditor** • **ISO 27001 Foundation** • **ITIL v3** • **ITIL v4** • **COBIT** • **PMP** • **Prince2**

180+ Security Vendor & Professional Certifications

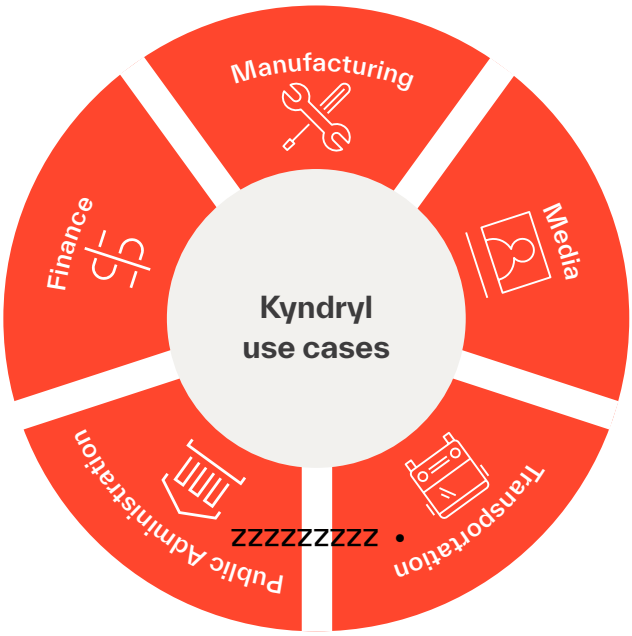
kyndryl

Il piano di formazione e certificazione viene mantenuto aggiornato in relazione alle opportunità tecnologiche più interessanti che vengono approfondite e alle esigenze del mercato.

Il Security Operations Center di Kyndryl Italia ha la sua control room operativa all'interno del Data Center Tier IV (DC) Tecnopolo Tiburtino a Roma, progettato con avanzate facilities in grado di garantire la piena continuità operativa. Le piattaforme gestite sono ospitate presso i datacenter di Pero (Milano) in Business Continuity con il DC di Castelletto (Milano), entrambi DC Tier IV nella zona metropolitana milanese.

La struttura è operativa da marzo 2022 e conta già un importante numero di clienti, migrati in modo efficiente grazie a un approccio alla transition che ha comportato zero rischi per i clienti, con attività e tempi definiti e un'ottimizzazione (in termini di livelli di servizio, review delle regole di correlazione, automazione e proattività) dell'as-is preso in carico già in fase di assessment e avvio del nuovo servizio. L'attività di migrazione massiva eseguita in questi mesi su clienti molto importanti per tipologia di business e per complessità di infrastruttura, ha dimostrato la capacità di analisi, definizione, pianificazione ed esecuzione del Security Operations Center di Kyndryl.

Ad oggi Kyndryl ha in gestione numerose aziende in diversi settori merceologici. I riscontri ottenuti dai clienti, molto positivi in termini di livelli di servizio mantenuti, di capacità di intervento e di attenzione al miglioramento continuo del servizio, hanno permesso anche di arricchire le best practice adottate, di accrescere l'esperienza nella gestione della sicurezza di realtà complesse e di migliorare l'organizzazione, i processi e le procedure operative su cui si basano le attività degli operatori L1/L2.



kyndryl

Visita il sito:

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