Protagonisti della trasformazione digitale

NTT DATA Italia Corporate Presentation

13 novembre 2024

Siamo parte di NTT Group

Una delle più grandi aziende di telecomunicazioni a livello globale

NTT Group

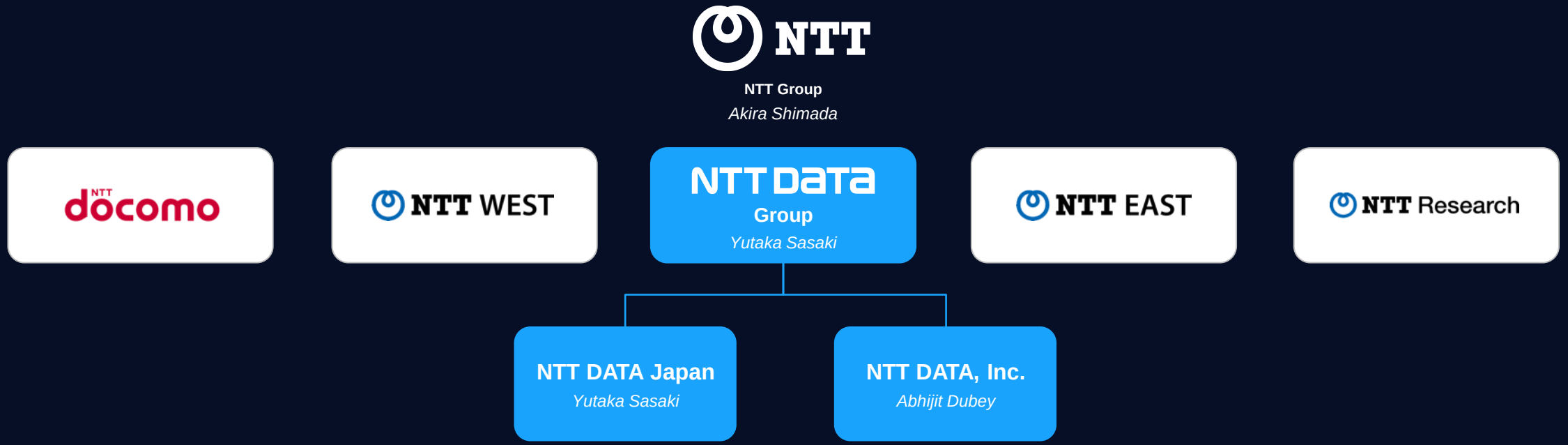
Akira Shimada

Il Gruppo NTT in numeri:

~$100B	**$3.6B+**	**150+**	**75%**	**4th**	**A**	**330K+**
Fatturato annuale	Investimenti annuali in R&D	Anni sul mercato	Della Fortune Global 100 è cliente	Più grande azienda telecom al mondo	Affidabilità creditizia	Professionisti

Siamo parte di NTT Group

Una delle più grandi aziende di telecomunicazioni a livello globale



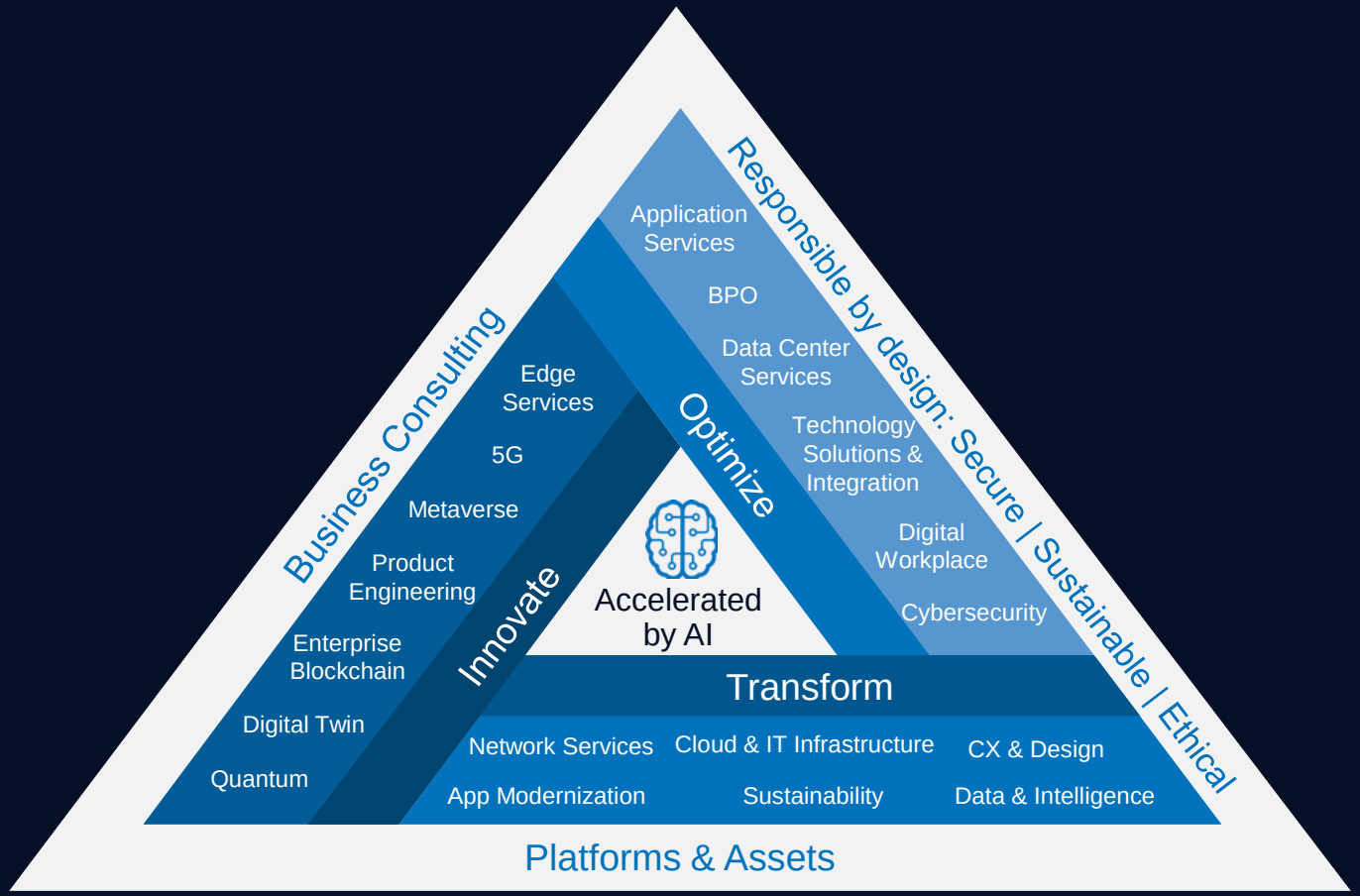
NTT Data Group in numeri:

$30B+	**50+**	**29**	**6th**	**3rd**	**Top 10**	**4th**
Fatturato annuale	Paesi	Paesi dove NTT DATA è riconosciuta Top Employer	Tra i brand IT di maggior valore	Più grande provider di data center al mondo (100 data center in 30 città)	Provider di servizi IT globale	Più grande provider di Backbone IP al mondo

Capacità senza pari a supporto dei risultati dei clienti

Industry expertise & solutions

Financial Services | Healthcare | Insurance | Life Sciences & Pharma | Higher Education & Research | Logistics, Travel, & Transportation | Public Sector | Automotive | Retail & CPG | Telco, Media & Technology | Energy & Utilities | Manufacturing



In Italia/

Siamo acceleratori del cambiamento.
Forti delle migliori competenze,
affrontiamo il futuro con coraggio.

NTT DATA, sempre più grande in Italia

Anticipiamo con intelligenza il futuro, in un ambiente collaborativo dove continuiamo a crescere insieme, come comunità e società.
Supportiamo la crescita digitale del Paese e delle aziende con le quali collaboriamo, in Italia e all'estero, generando sempre più sinergie e collaborazioni per affrontare sfide più importanti, progetti più innovativi, inclusivi, e sostenibili.

6.000+
Dipendenti

~ 600
Milioni (€)
di ricavi

11
Città

Gov & tech

Innovazione in pratica

L'innovazione avviene quando applichiamo la tecnologia e l'esperienza del settore per risolvere importanti sfide aziendali.

Tecnologie globali

Tecnologie avanzate mirate che stimolano la crescita e aumentano il valore

Linguistica digitale & LLM

Elaborare il linguaggio per migliorare la produttività

Web3

Sbloccare il mondo di Web3

Sicurezza zero trust

Utilizzare la connettività e infrastrutture smart per rimodellare la mobilità

Sostenibilità globale

Innovare per un futuro più sostenibile e proteggere il pianeta e la società

Green tech

Verso il net-zero

Supply chain

Tracciabilità con blockchain per garantire supply chain sostenibili

Soluzioni per le emissioni

Aiutare a guidare un'economia a basse emissioni di carbonio

Industry globali

Co-investimento, co-creazione e nuove soluzioni per industry globali mirate

Digital twins & smart robotics

Costruire società migliori e automatizzare i vantaggi di business

5G

Cambiare le regole del gioco con i servizi cellulari

IoT & edge analytics

Migliorare la sicurezza pubblica con IoT avanzato e edge analytics

NTT DATA realtà di rilievo nel mondo nell'ambito della Cybersecurity

Recognition

#2

by revenue in Gartner® Market Share Analysis: Managed Security Services, Worldwide, 2023

**Source: Gartner® Market Share Analysis: Managed Security Services, Worldwide, 2023 – Published May 2024*

Leader

in Everest Group's Cybersecurity Services PEAK Matrix® Assessment 2024 – Europe

**Source: Cybersecurity Services PEAK Matrix® Assessment 2024 – Europe – Oct 2024*

Global Partnerships

132

Soluzioni di cybersecurity in collaborazione con un significativo parco di fornitori in ambito

37,400+

Certificazioni dei vendor

Community

7,500+

Global Cybersecurity specialists

420

Local Cybersecurity specialists in Italy

ISACA

CSA cloud security alliance®

Reali competenze end-to-end per supportare una trasformazione digitale in sicurezza

Security Consulting
Assessment | Roadmap | Architecture

Technical Services
Design | Implement | Automation | Technology

Support Services
Maintenance | Lifecyle | Digital Wallet

Managed Services
UMDR | Manage & Operate

Crisis Response

Threat actors

- Recon
- Exploits
- Cybercrime

Digital assets

- Infrastructure
- Data
- IP

Specialization

End2End

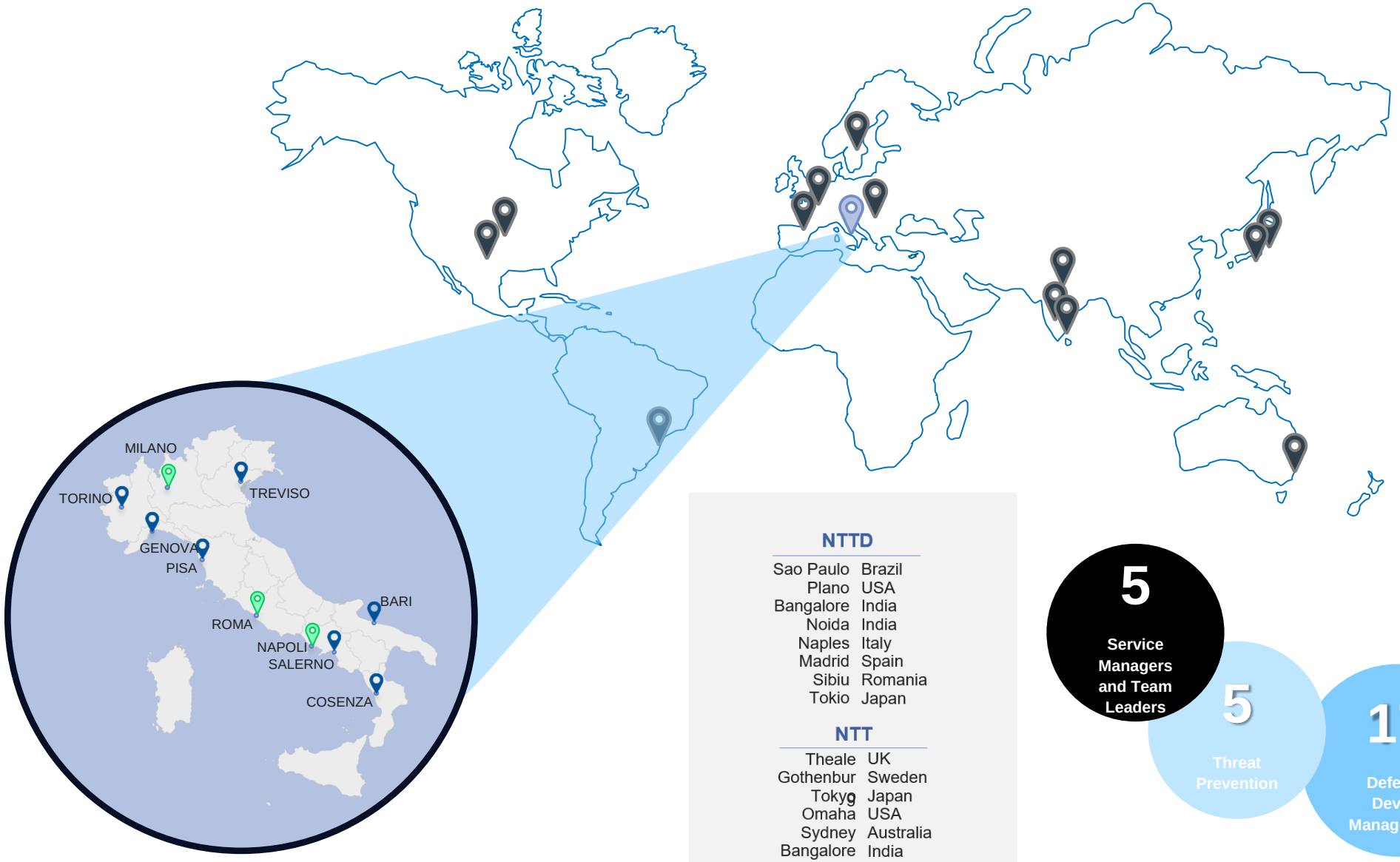
Experience

Glocal Services

NTT DATA

Il 40% del traffico IP mondiale è gestito dall'infrastruttura di rete del Gruppo NTT

Distribuzione dei SOC NTT nel mondo e in Italia



NTTD

Sao Paulo	Brazil
Plano	USA
Bangalore	India
Noida	India
Naples	Italy
Madrid	Spain
Sibiu	Romania
Tokio	Japan

NTT

Theale	UK
Gothenbur	Sweden
Tokyo	Japan
Omaha	USA
Sydney	Australia
Bangalore	India

800 Dipendenti SOC nel mondo

85 Dipendenti SOC in Italia

38 Security Monitoring, Incident Response

20 Threat Intelligence

17 Defence Device Management

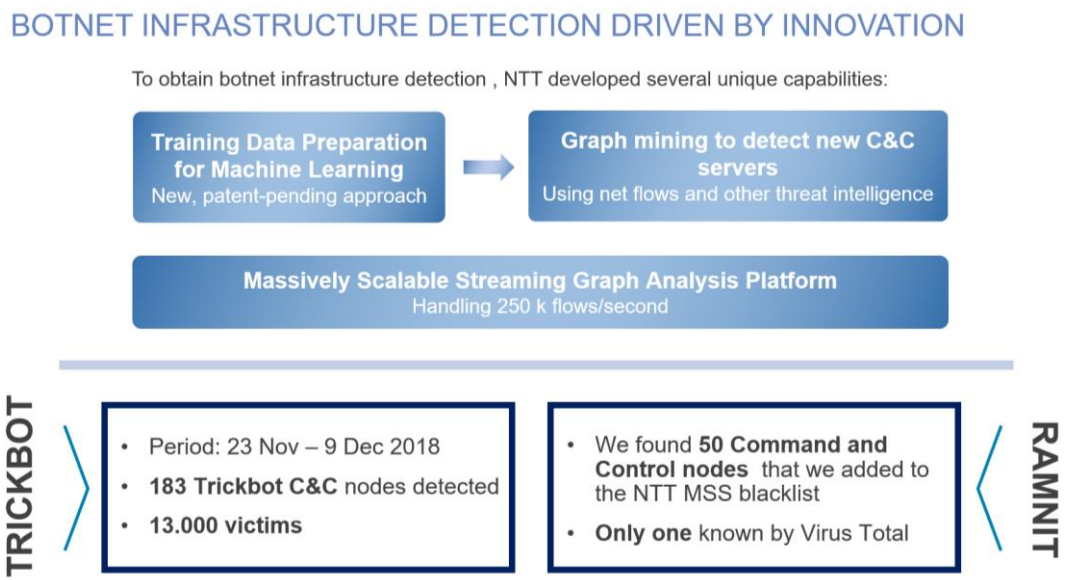
5 Threat Prevention

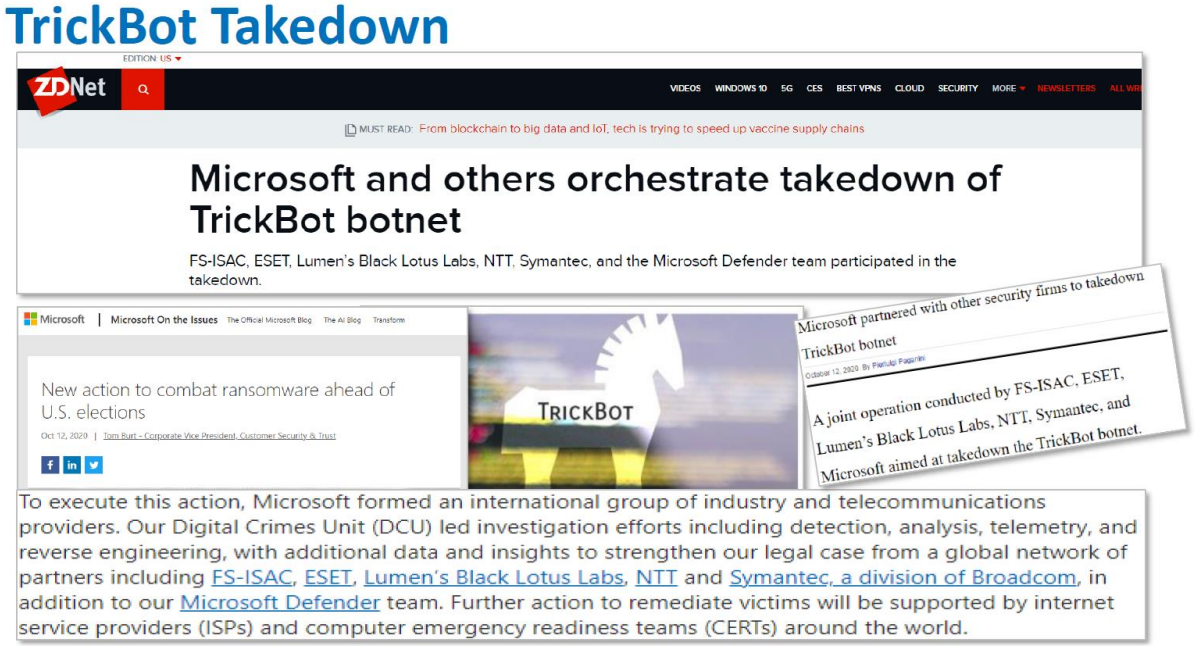
5 Service Managers and Team Leaders

Condivisione di strumenti ed informazioni per la lotta alle minacce presenti su larga scala

- Innovazione
- Disponibilità dei dati e capacità elaborativa
- Threat Intelligence e analisi

- Scambio informativo
- Eccellenza
- Teamworking





Information sharing e partecipazione alle community come elementi cardine della strategia di cybersecurity

BUSINESS COMMUNITY

- CTA (Cyber Threat Alliance)
- Aspen Institute Global Cybersecurity Group
- CSDE (Council to Secure the Digital Economy)
- USTelecom
- International Communication CISO Council
- Tech Accord

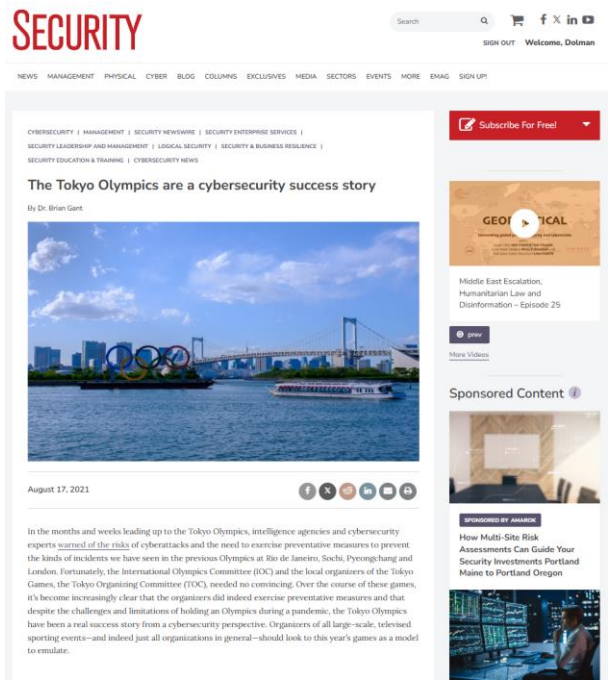
INTERNATIONAL GOVERNMENT

- USFederal: CISA, NSC, NIST, NTIA, etc
- UK: NCSC, NCAB
- Germany: BSI
- Israel: INCD
- Singapore: CSA, HTX
- Czech: Nukib

Importanza della collaborazione cross-sector per la sicurezza del Sistema-Paese

- **Interdipendenza** tra i diversi settori
- **Esercitazioni congiunte periodiche** per mantenere la preparazione

- Il governo giapponese organizza ogni anno una esercitazione congiunta dal 2009
- La prima ha avuto solo 116 partecipanti da 34 organizzazioni
- L'ultima ha avuto oltre **3.000 partecipanti**



- Garantire la sicurezza nei domini fisico e informatico per eventi di alto profilo (es. Tokyo 2020)

Contribuire alla formazione dei professionisti in ambito cybersecurity…

Sostegno ad **Università ed altri enti formativi come gli Istituti Tecnici Superiori** attraverso l'esecuzione di docenze in aula, presentazione di testimonianze, organizzazione di laboratori didattici, individuazione di argomenti sperimentali per le tesi, percorsi di tirocinio e sponsorizzazione delle coorti accademiche

Organizzazione di percorsi formativi interni rivolti ai neoassunti per **fornire nozioni di base** su tutti gli aspetti che caratterizzano il mondo della cybersecurity partendo dagli aspetti normativi, passando dalla conoscenza delle principali soluzioni tecnologiche ed infine arrivare alla conoscenza di processi e pratiche per la cybersecurity

Partnership with Universities

Two of Italy's most prestigious universities, **Bocconi** & **Politecnico di Milano**, have joined forces to prepare an **interdisciplinary path** that combines **technical and managerial competencies**:

- **technical elements** of computer science and **analytical methods** (provided by Politecnico di Milano); and
- a range of topics in the **social sciences** as management, economics, finance law, social engineering, ethics, and behavioral skills (provided by Bocconi).

We have been a partner of the **Master in Cyber Risk Strategy and Governance** since the first year in 2021

Bocconi — POLITECNICO MILANO 1863

Interaction with Students *meeting them during dedicated moments and participating in selected courses providing our experiences with Business Cases*	**Recruiting Activities** *selecting students who impressed us during our interactions with them* **Hired 18 students over 3 years.**
Brand reputation *highlighing our capabilities to students from around the world, strengthening their interest in our brand*	**Research** *discussing areas of cooperation and research with the University involved and Suggesting thesis topics to students*

We support the students we consider most deserving in the **first steps of their careers** and for us it is an honor to experience their **enthusiasm**, brand new **ideas** and a contemporary **vision** on an **ever-evolving field as Cybersecurity**.

NTT DATA

Moving excellence from local to global

NTT DATA
301.504 follower
2s •

Ethical hacking. Cyber risk management. Encryption algorithms. They're just some of the skills 32 Italian junior staffers are leaning at NTT DATA Italia's Cyber Academy.

As the global leader in helping companies transition into the digital world, we're highly aware of the cyber risks that exist out there. We know that one slip-up can have big consequences, exposing your personal information to the internet's shadier characters. That's why we make a point of training our staff to the highest standards to help you keep your data and systems secure.

By the time these students finish the internal course, they'll be cybersecurity pros, ready to help customers handle real-world issues with confidence.

#NTTDATA #NTTDATAItalia #CyberSecurity #CyberAcademy

NTT DATA Italia
71.556 follower
3m •

Al via oggi la #CyberAcademy di #NTTDATA!

32 ragazzi
24 lezioni
Diversi ambiti della cybersecurity: dal Cyber Risk Management all'Ethical Hacking e Red Teaming, dall'Encryption Algorithms & Hash Functions all'Automotive cybersecurity, dalla Privacy Anatomy al Threat Defense e Incident Management.

La Cyber Academy, che nasce con l'obiettivo di coinvolgere i junior della #Cybersecurity sin dal primo giorno in azienda, promuove l'integrazione tra aree di specializzazione differenti e, al tempo stesso, fornisce competenze di base per acquisire una visione d'insieme sul mondo della sicurezza informatica.

...e contribuire a sensibilizzare i future utilizzatori del mondo digitale

OBIETTIVI

- **Sensibilizzare** i ragazzi, dai 9 ai 12 anni, sui **principali rischi** cui si può essere esposti nell'**utilizzo della rete**, dei **social media**, delle **chat** e dei **giochi on line**;
- **Fornire** le **nozioni basilari**, ma essenziali, circa i **comportamenti corretti** da adottare;
- Far **nascere l'interesse** sui temi della **Cyber Security**, sperando di attrarre nuovi talenti verso una delle professioni più ricercate dei prossimi anni;

NUMERI 2024

- **37 esperti** di Cyber Security di NTTDATA
- Circa **4700 ragazzi** coinvolti
  - **120 classi** di scuola primaria
  - **65 classi** di scuola secondaria primaria
- **25 città**
- **460 ore** di lezione e confronto con i ragazzi

Costruzione di un’efficace agenda per la cybersecurity

ASSESS
Progettare la strategia di Cyber Security sulla base dello stato attuale e delle reali necessità

PREPARE
Preparare l’organizzazione per proteggersi dalle minacce del contesto in cui opera

OPERATE
Reagire tempestivamente alle minacce e rafforzare la resilienza mediante una gestione continua della Cyber Security

INFLUENCE
Monitorare le terze parti che potrebbero influire sulla sicurezza aziendale

FORESEE
Guardare oltre i propri confini per rilevare le nuove minacce e ridurre l’esposizione al rischio

MAKE IT SUSTAINABLE
Controllare il livello di rischio coerentemente alla strategia aziendale


NTT DATA

La cybersecurity è un fenomeno di rilevanza sempre più crescente

Aumento dei cyber attacchi: un rischio per il business

Gli attacchi informatici sono aumentati di circa il **75% negli ultimi 5 anni** (nel 2023 sono aumentati del 12% rispetto all'anno precedente).

L'evoluzione tecnologica e il crescente utilizzo dell'AI rendono i **cyber attacchi sempre più complessi ed efficaci**.

Digitalizzazione del settore finanziario

Il settore finanziario dipende sempre più dall'utilizzo delle tecnologie digitali e da fornitori di servizi ICT, aumentando così le vulnerabilità e l'esposizione a rischi informatici.

Nello scorso anno, si è registrato un **aumento del 62% (rispetto al 2022) degli attacchi cyber nel settore finanziario**, con impatto critico nel 50% dei casi.

Fonte: Rapporto Clusit 2024

Allianz Risk Barometer 2024

1° ***Cyber incidents***
Primo rischio più importante per le aziende intervistate

2° ***Business interruptions***
Secondo rischio più importante per le aziende intervistate

- Per il terzo anno consecutivo gli **incidenti informatici** (36% delle risposte complessive) si classificano come il **rischio più importante a livello globale**
- Gli incidenti informatici come attacchi *ransomware*, violazioni dei dati e interruzioni IT sono **la più grande preoccupazione per le aziende di tutto il mondo nel 2024**

ENISA TOP PRIORITY

- **Ransomware** (Top 10 per 9 anni consecutivi)
- **Supply Chain Attacks** (6 anni consecutivi)
- **Internal Fraud** (9 anni consecutivi)

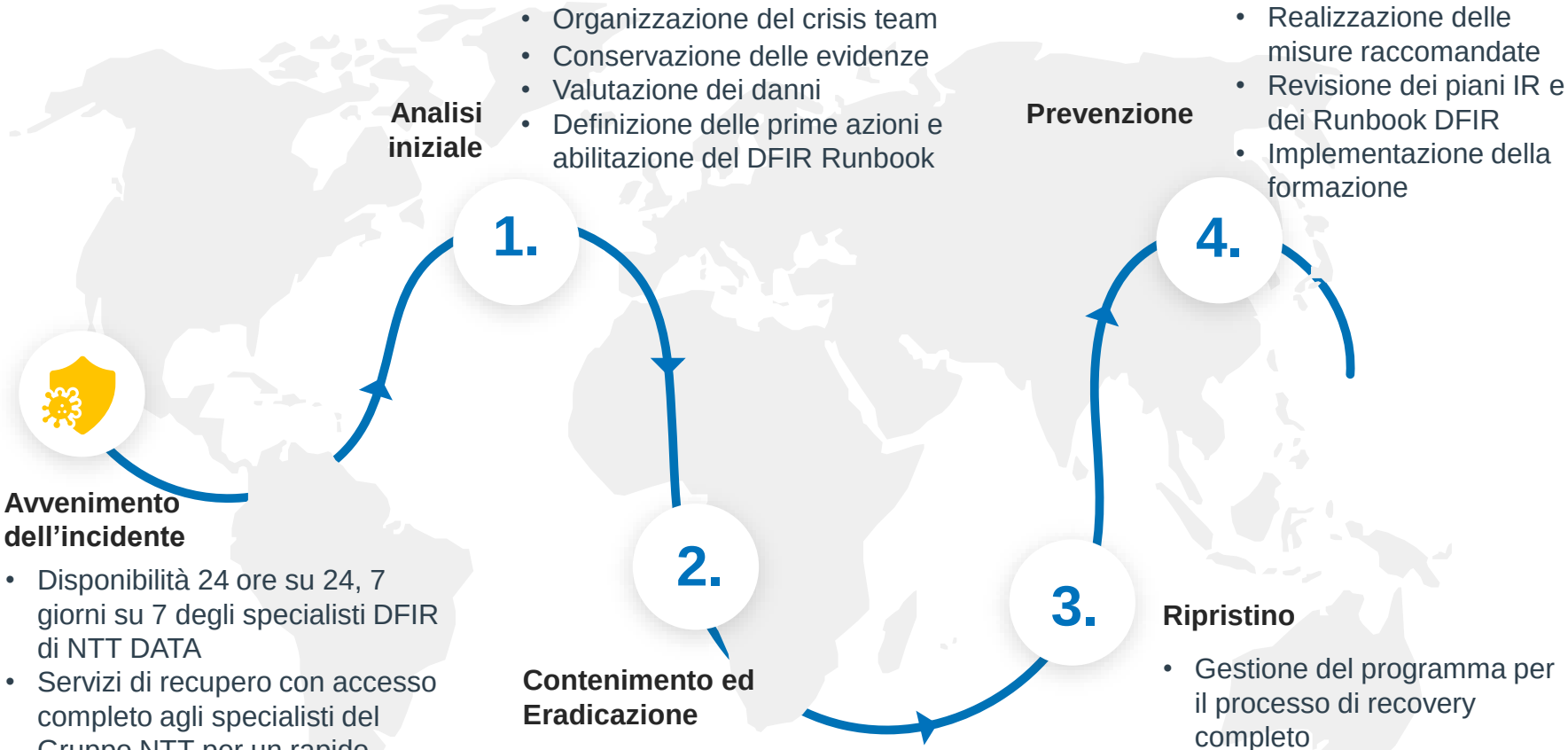
Emergency Response

Ampia **esperienza globale in materia di analisi forense digitale e risposta agli incidenti** per aziende locali e multinazionali

Ridurre al minimo i danni alla sicurezza mediante una risposta tempestiva e misure approfondite per evitare che si ripetano

Crisis Response

Emergency Activities



Avvenimento dell'incidente

- Disponibilità 24 ore su 24, 7 giorni su 7 degli specialisti DFIR di NTT DATA
- Servizi di recupero con accesso completo agli specialisti del Gruppo NTT per un rapido ritorno alle normali operazioni aziendali
- Il Recovery Van di NTT DATA è dotato di hardware per un rapido ripristino

1. Analisi iniziale

- Organizzazione del crisis team
- Conservazione delle evidenze
- Valutazione dei danni
- Definizione delle prime azioni e abilitazione del DFIR Runbook

2. Contenimento ed Eradicazione

- Analisi forense per le indagini
- Reverse engineering del malware
- Isolamento di emergenza di sistemi e ambienti infetti
- Analisi dell'esfiltrazione dei dati

3. Ripristino

- Gestione del programma per il processo di recovery completo
- Distribuzione di hardware di ripristino
- Rapido recupero di sistemi e ambienti

4. Prevenzione

- Realizzazione delle misure raccomandate
- Revisione dei piani IR e dei Runbook DFIR
- Implementazione della formazione

NTT DATA

Ripristino delle infrastrutture critiche

In caso di un incidente grave come un incendio o un attacco informatico, l'infrastruttura di un'organizzazione potrebbe crollare o essere compromessa, interrompendo le operazioni. Ricostruire l'intera infrastruttura può richiedere tempo, ma è fondamentale dare priorità al ripristino dei componenti più critici che supportano le funzioni aziendali principali.

Prepariamo la tua organizzazione per un potenziale incidente grave identificando i sistemi critici, sviluppando un solido piano di ripristino e costruendo un'infrastruttura temporanea che garantisca tempi di inattività minimi. Il nostro servizio si estende anche all'assistenza pratica durante il processo di ripristino, garantendo un ripristino senza interruzioni dei servizi critici e della continuità aziendale.

Outcomes

- Piano di ripristino dettagliato con azioni di risposta immediata per ripristinare i sistemi critici.
- Architettura infrastrutturale completa pronta a gestire scenari di emergenza.
- Supporto pratico al recupero, che garantisce il ripristino con successo delle operazioni critiche.
- Furgone di emergenza mobile con infrastruttura di base per il recupero.

Preparazione pre-incidente

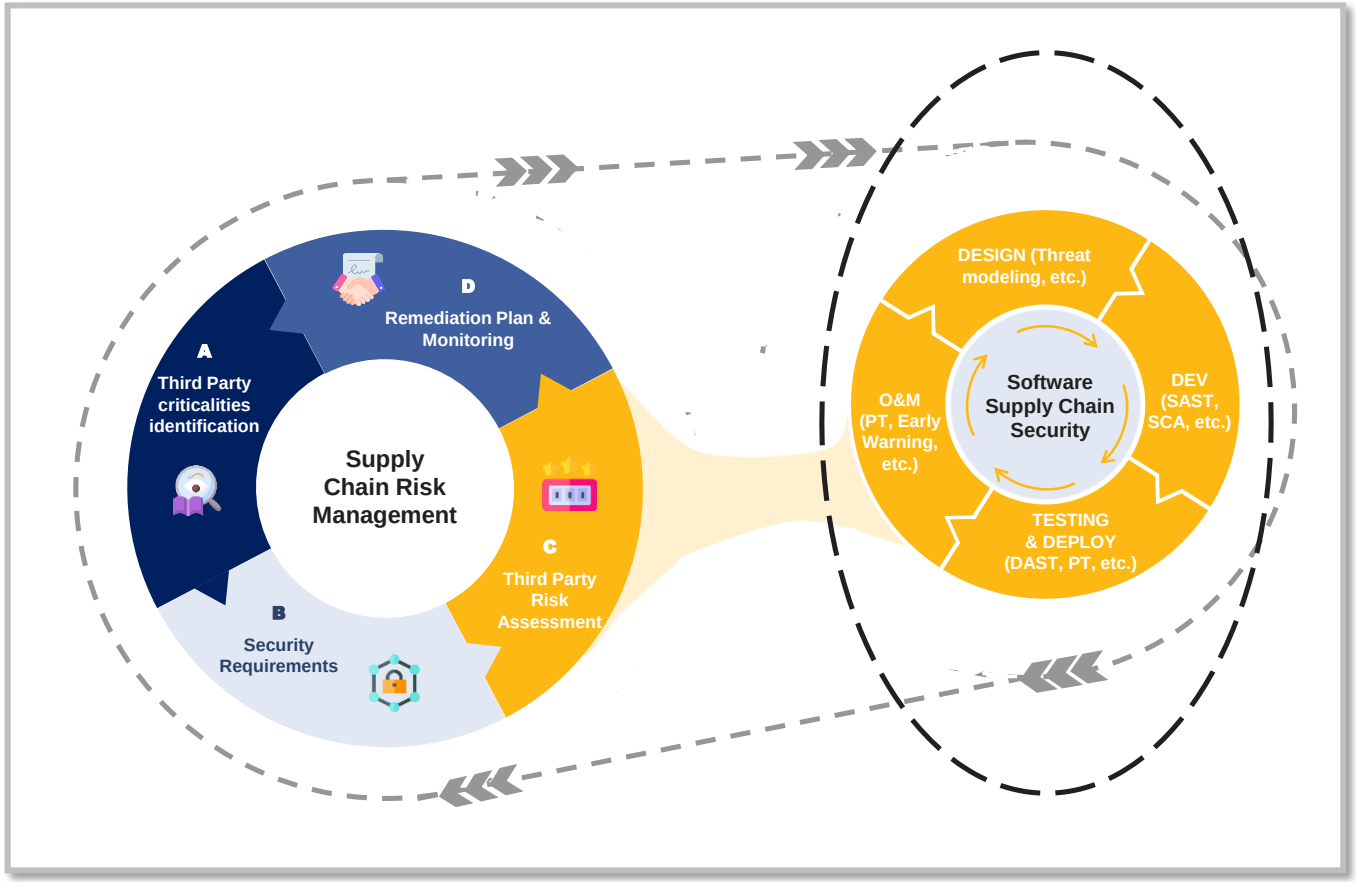
- Identificare i servizi infrastrutturali essenziali (ad esempio, accesso a Internet, firewall, DNS, DHCP) da stabilire come prioritari per il ripristino.
- Mappare i sistemi critici necessari per le operazioni aziendali, come database ed ERP, per garantirne il rapido ripristino.
- Sviluppare un'architettura infrastrutturale progettata per ospitare temporaneamente i sistemi critici durante il ripristino.
- Preparare un inventario delle risorse che includa tutto l'hardware, il software e le configurazioni necessarie per il ripristino.
- Testare i piani di ripristino tramite esercitazioni realistiche, perfezionando continuamente il processo per garantire la preparazione.
- Fornire assistenza e infrastrutture da parte di esperti durante il ripristino per garantire il rapido ripristino dei sistemi e dei servizi aziendali critici.

Visione omnicomprensiva della Supply Chain Security

RISCHI ASSOCIATI ALL'UTILIZZO DI TERZE PARTI

- Fornitori di servizi e componenti vengono attaccati creando un blocco alla fornitura
- Rischio di intrusione nella propria infrastruttura ICT sfruttando le debolezze del business partner
- Sfruttamento di vulnerabilità intrinseche dei dispositivi acquistati
- Fornitori di servizi di ousourcing vengono attaccati, compromentendo il supporto di secondo e terzo livello
- ...

Approccio integrato al Supply Chain Risk Mgmt in grado di supportare sia nella fase di **analisi dei livelli di maturità dei fornitori** nella gestione della sicurezza informatica così come nella **conduzione delle attività di verifica tecnica di quanto viene realizzato dagli stessi**.



Vulnerability Management come elemento chiave per la protezione delle infrastrutture ICT

SW Security Assurance

FORTIFY
VERACODE
CHECKMARX
SYNOPSYS
snyk
HCL SOFTWARE
sonarqube

Vulnerability Detection & Exposure Mgnt

Qualys.
CROWDSTRIKE
tenable
RAPID7
XM Cyber
SKYBOX SECURITY

Vulnerability Prioritization

CISCO | KENNA Security

Vulnerability Response

servicenow
SWIMLANE
CORTEX XSOAR

OSSTMM Open Source Security Testing Methodology Manual www.osstmm.org

DORA Digital Operational Resilience Act

CVSS COMMON VULNERABILITY SCORING SYSTEM

NIST National Institute of Standards and Technology U.S. Department of Commerce

OWASP®

ISO 27001 Certified

GDPR The General Data Protection Regulation

CIS Center for Internet Security®

PCI Security Standards Council®

Technologies and Products

Reference Standards

Process and Compliance

April 2024

NTT DATA

Vulnerabilità recenti in dispositivi utilizzati per la sicurezza delle comunicazioni

Oct 2023, Cisco, 41,983 devices Backdoor installed
- Cisco IOS XE（Switch, Router, AccessPoint)

Feb 2024, Ivanti, Over 2100 devices Backdoor installed
- Ivanti Connect Secure（Pulse Connect Secure）、Ivanti Policy SecureGW

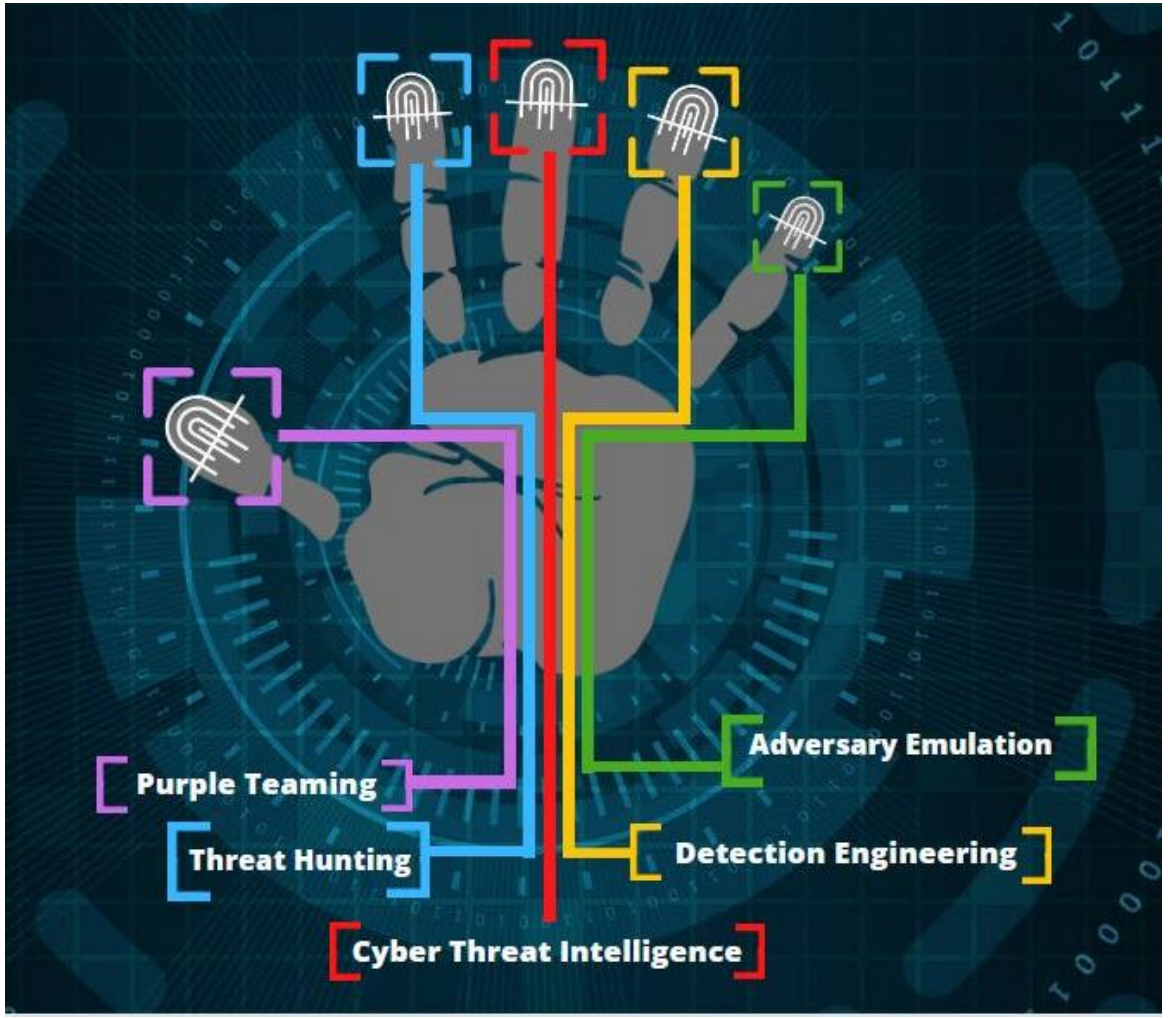
Mar 2024, Fortinet, Observed Attack code and selling them
- FortiOS, FortiProxy

Apr 2024, PaloAlto, Observed Attack code
- Pan-OS Global Protect

Programmi di cybersecurity che da reattivi diventano sempre più proattivi

- Maggiore attenzione verso **minacce** che risultano **realmente critiche**
- Infrastrutture di sicurezza che proteggano gli asset **con maggiore probabilità di subire un attacco**
- **Puntuale valutazione dell'efficacia** delle contromisure messe in campo
- Effettiva **sinergia tra BLUE e RED Team**
- Efficace **allineamento tra Threat e Risk Mgmt**

Threat-Informed Defense



Supportati da servizi gestiti (Managed XDR) per incrementare l'efficacia di risposta a tentative di attacco informatico

Le piattaforme XDR rappresentano **soluzioni di più semplice gestione** per la rilevazione di eventi anomali e la gestione di incidenti informatici grazie alla loro capacità di automatizzare processi che richiedono molto tempo, ridurre i tempi di rilevamento e risposta e generalmente richiedere meno manutenzione

Il valore combinato di NTT DATA con la piattaforma Cortex di Palo Alto Network per l'orchestrazione, l'automazione e la threat intelligence dotata di soluzioni basate sull'intelligenza artificiale porta a una migliore resilienza operativa, finanziaria e del personale in grado di **potenziare la capacità del team di sicurezza**