



kitsune

La **piattaforma** che ***raccoglie, analizza e trasforma***
dati in visione strategica.

MERIDIAN

GROUP

Meridian Group è una società italiana specializzata in Cyber Digital Intelligence che sviluppa soluzioni proprietarie per prevenire, rilevare e contrastare minacce informatiche complesse, integrando tecnologia, intelligence operativa e sicurezza offensiva.

La nostra mission

La nostra missione è trasformare la sicurezza informatica in un processo continuo, strategico e misurabile. Anticipiamo le minacce emergenti attraverso un ecosistema guidato da intelligence proattiva, simulazioni offensive, investigazioni tecniche e automazione orchestrata.

Beyond CyberSecurity.

25+ anni di esperienza
nella cyber security

45+ tecnici altamente
specializzati

87+ clienti

3 tecnologie
proprietarie

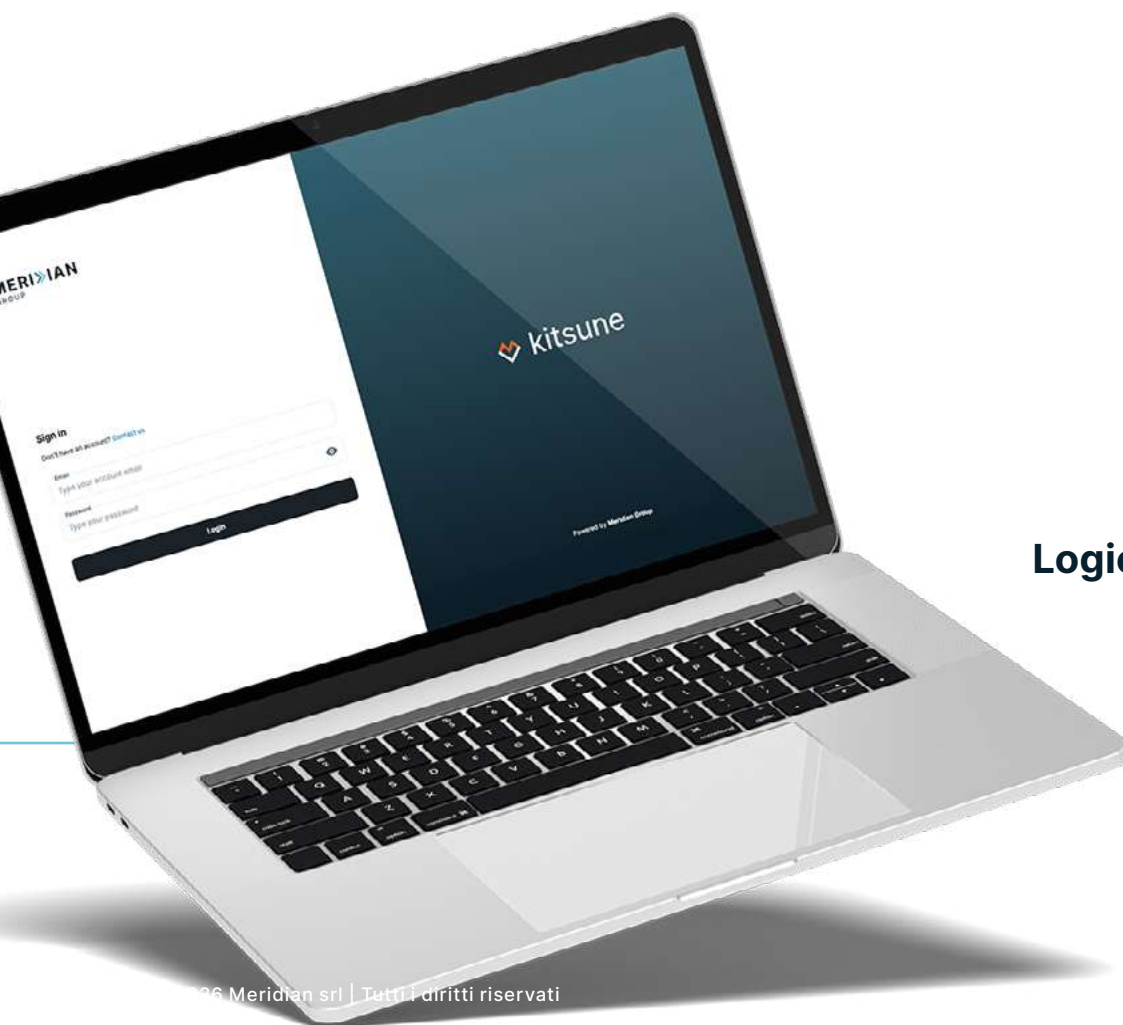
What's coming will **redefine everything.**

Kitsune è una piattaforma di cybersecurity progettata per ambienti critici e altamente regolamentati, che unifica in un'unica soluzione il rilevamento, la gestione e la risposta alle minacce informatiche.

Grazie all'integrazione di intelligenza artificiale e machine learning, consente analisi comportamentali avanzate, correlazione automatica degli eventi e identificazione predittiva delle minacce, riducendo la complessità operativa e anticipando gli attacchi.

Scalabile e modulare, Kitsune si integra facilmente anche nei contesti più complessi, offrendo una visione completa e centralizzata del rischio cyber e una risposta operativa integrata, intelligente e adattiva. Interamente sviluppata in Italia, rappresenta un nuovo standard per la sicurezza digitale.





Rilevamento Automatico delle minacce

Protezione in tempo reale

Difesa Proattiva

Allarmi

Integrazione con i sistemi esistenti

Tecnologia innovativa e scalabile

Roi Sugli investimenti in sicurezza

Logica Semantica per l'identificazione delle minacce

Tecnologia Italiana

HOMEPAGE



VALORE PRINCIPALE

- Cruscotto direzionale per il controllo dell'intero perimetro di sicurezza
- Punto centrale di governo per il SOC

VISIBILITÀ IMMEDIATA

- Indicatori chiave aggregati in widget intuitivi:
 - Eventi
 - Minacce attive
 - Tentativi di compromissione
 - Allarmi
- Informazioni chiare, aggiornate e facilmente navigabili in tempo reale

ANALISI E CONTESTO

- Grafici comparativi e timeline evolutive
- Mappa geografica degli incidenti
- Individuazione rapida di:
 - Aree critiche
 - Trend nel tempo
 - Categorie a maggiore impatto

EFFICIENZA OPERATIVA

- Supporto a decisioni basate sui dati (data-driven)
- Comunicazione più efficace verso management e risk owner
- Riduzione dei tempi di coordinamento tra i team

GESTIONE DEL RISCHIO

- Prioritizzazione immediata delle minacce
- Analisi di dettaglio (drill-down) su:
 - Asset
 - Alert
 - Campagne
- Continuità tra monitoraggio e intervento operativo

BENEFICI

- Trasformazione dei segnali eterogenei in insight operativi
- Allineamento tra detection, response e reporting
- Un unico punto di controllo e governo della sicurezza

LOOK UP

The screenshot displays the Meridian Look Up interface. At the top, there's a search bar and navigation icons. Below it, a table lists various IP addresses and their associated domains. The table has columns for Type, TTL, Value, Name, Status, Refresh, Retry, Expiration, and Notes. The data includes entries for A, NS, MX, and SOA records for domains like 216.239.32.21, 216.239.34.21, and 216.239.34.21. Below the table, there's a sidebar with search filters and a bottom section with detailed analysis results, including a 'Certificate HTTP' section and a 'WHOIS' section.

Type	TTL	Value	Name	Status	Refresh	Retry	Expiration	Notes
A	3600	216.239.32.21						
A	3600	216.239.34.21						
NS	3600	ns1.google.com						
MX	3600	aspm2.googlemail.com						
MX	3600	aspm2.googlemail.com						
A	3600	216.239.34.21						
MX	3600	aspm2.googlemail.com						
MX	3600	aspm2.googlemail.com						
NS	3600	ns1.google.com						
MX	3600	aspm2.googlemail.com						
SOA	3600	ns1.google.com						
NS	3600	ns1.google.com						
A	3600	216.239.32.21						
NS	3600	ns1.google.com						

VALORE PRINCIPALE

- Motore di arricchimento per entità sospette:
 - Domini, Indirizzi IP, Certificati e Hash
- Una singola query consente di ottenere:
 - Evidenze tecniche
 - Contesto OSINT
 - Correlazioni con le knowledge base interne
- Elimina la necessità di operare manualmente su strumenti esterni

WORKFLOW INVESTIGATIVO

- Supporta l'intero processo investigativo end-to-end
- A partire da un indicatore grezzo permette di:
 - Valutarne l'affidabilità
 - Analizzarne la storicità
 - Individuare collegamenti con campagne note
 - Correlare attori e indicatori di compromissione (IOC)

ANALISI AVANZATA

- Correlazione semantica delle informazioni
- Visualizzazione dei risultati non solo in forma di liste, ma anche come:
 - Grafo di relazioni logiche
- Supporta:
 - L'attribuzione delle minacce
 - Un triage più preciso ed efficace

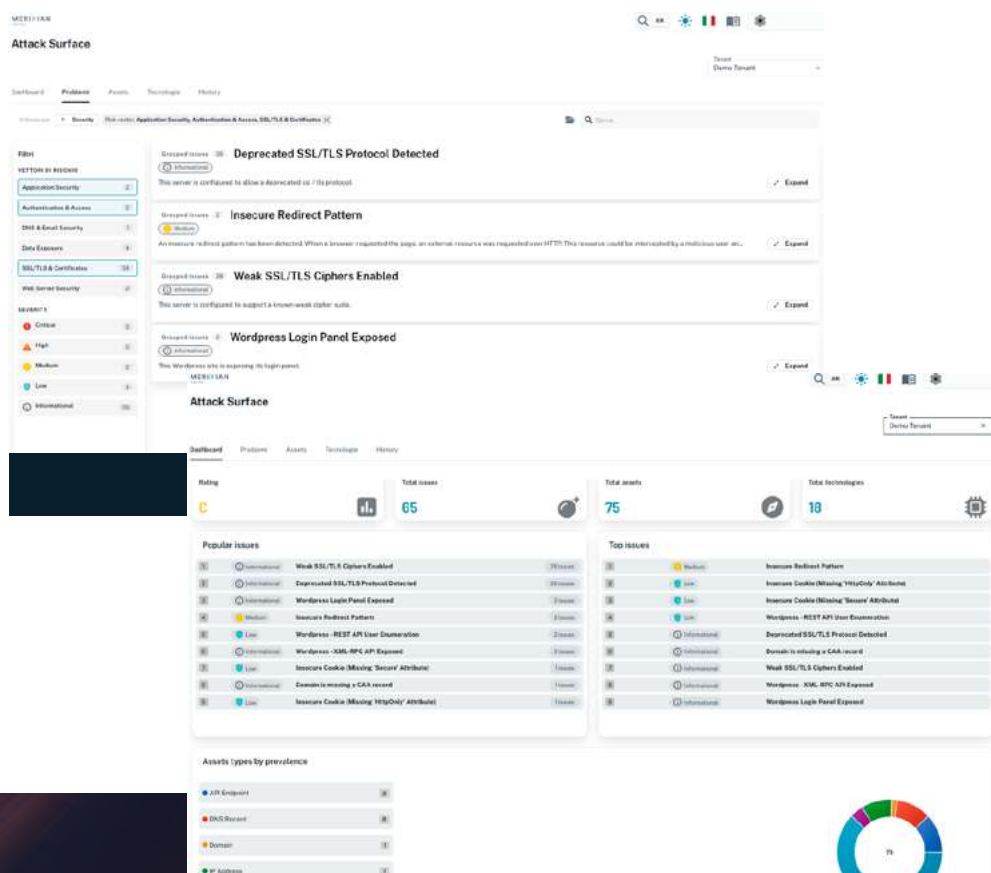
BENEFICI OPERATIVI

- Riduzione del tempo medio di investigazione (MTTI)
- Maggiore tracciabilità delle decisioni
- Riduzione dei falsi positivi

IMPATTO

- Punto di raccordo tra:
 - Raccolta degli indizi
 - Analisi e contestualizzazione
 - Azione operativa
- Migliora la qualità delle analisi
- Aumenta la coerenza e l'efficacia delle risposte

ATTACK SURFACE



VALORE PRINCIPALE

- Vista dinamica e sempre aggiornata della superficie di attacco
- Inventario automatico di tutti gli asset
- Visibilità completa su:
 - Esposizioni
 - Errori o debolezze di configurazione
 - Vulnerabilità associate
- Supporta una gestione del rischio proattiva

GESTIONE DELLE CRITICITÀ

- Le criticità sono classificate per priorità e impatto
- Possibilità di filtrare per:
 - Business unit
 - Tecnologia
 - Livello di gravità
- Attivazione automatica di azioni di remediation

ANALISI BASATA SUL RISCHIO

- Integrazione tra dati tecnici e contesto aziendale
- Supporto a decisioni guidate dal rischio
- Interventi mirati:
 - Dove l'esposizione è realmente sfruttabile
 - Dove l'impatto può essere più significativo

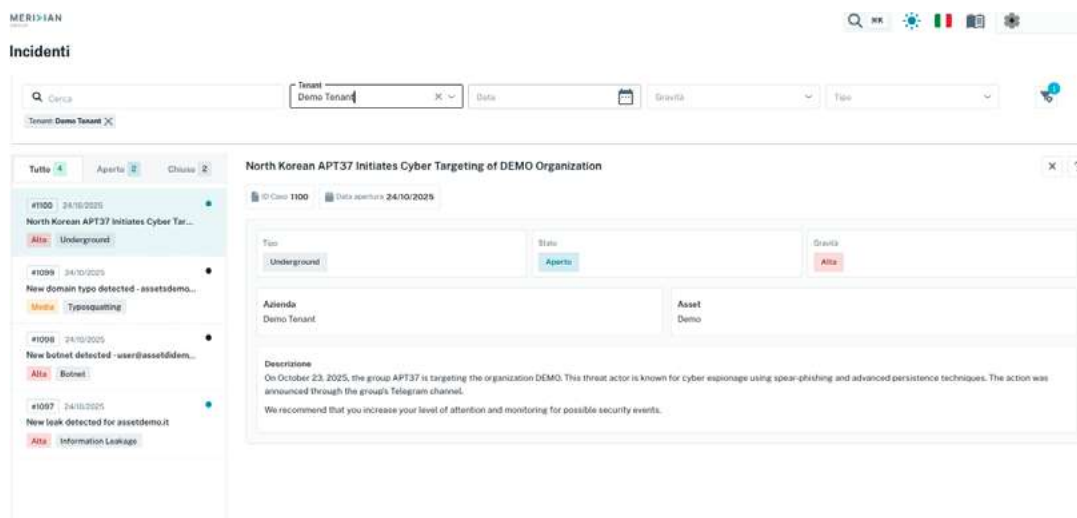
VALORE OPERATIVO

- Prevenzione:
 - Riduzione delle superfici di attacco prima che vengano sfruttate
- Ottimizzazione delle risorse:
 - Focus sulle attività a maggior valore

IMPATTO

- Controllo continuo della postura di sicurezza
- Allineamento tra IT e Security su priorità condivise
- Riduzione del rischio di violazioni:
 - Sia su minacce note
 - Sia su nuovi vettori emergenti

INCIDENTI



VALORE PRINCIPALE

- Vista centralizzata di tutti gli incidenti
- Informazioni principali sempre disponibili:
 - Stato
 - Livello di gravità
 - Responsabile
 - Attività in corso
- Per ogni incidente sono disponibili:
 - Evidenze raccolte
 - Cronologia completa degli eventi
 - Registro delle decisioni prese
 - Azioni eseguite, sia manuali che automatiche

CONTESTO E CLASSIFICAZIONE

- Classificazione degli incidenti secondo standard riconosciuti (es. MITRE ATT&CK)
- Arricchimento con:
 - Tecniche e modalità di attacco
 - Indicatori di compromissione (IOC) collegati
- Maggiore contesto per facilitare analisi e attribuzione

METRICHE E PERFORMANCE

- Monitoraggio continuo delle prestazioni operative:
 - Tempo medio di rilevazione (MTTD)
 - Tempo medio di risposta o risoluzione (MTTR)
- Valutazione dell'efficacia del SOC
- Supporto al miglioramento continuo

FILTRI E ANALISI

- Filtri e viste personalizzabili per analizzare gli incidenti
- Possibilità di segmentare per:
 - Stato, Gravità, Responsabile, Tipologia o categoria
- Navigazione semplice tra incidenti e relative correlazioni

BENEFICI OPERATIVI

- Maggiore controllo e tracciabilità delle attività
- Migliore coordinamento tra i team
- Riduzione dei tempi di rilevazione e risposta
- Decisioni più rapide e basate su dati concreti

TERZE PARTI

MERIDIAN GROUP

Third Parties

Dashboard Problems Assets **Technologie** History

Search

Filtri	TECHNOLOGY	CPE TYPE	TAGS	FIRST SEEN	LAST
IMAP	IMAP IMAP server	cpe:2.3:a:imap:imap_server:	imapserver mailserver	12/01/2025	12/01
Tags	Exim 4.99.1	cpe:2.3:a:exim:exim:4.99.1:	smtpserver mailserver	12/01/2025	12/01
mailserver 4	MariaDB 10.6.20	cpe:2.3:a:maria:maria:10.6.20:	mysqlserver database	12/01/2025	12/01
sshserver 3	Generic SMTP	cpe:2.3:a:generic:smtp:	smtpserver mailserver	12/01/2025	12/01
web server 3	OpenBSD OpenSSH	cpe:2.3:a:openbsd:openssh:	sshserver	12/01/2025	15/01
imapserver 2	SSH 2.0	cpe:2.3:a:ssh:ssh:2.0:	sshserver	12/01/2025	15/01
smtpserver 2	OpenResty 1.27.1.1	cpe:2.3:a:openresty:openresty:1.27.1.1:	web server	12/01/2025	15/01
mysqlserver 1	Microsoft ASP.NET	cpe:2.3:a:microsoft:asp.net:	web framework	12/01/2025	15/01
database 1	Microsoft HTTP Server API 2.0	cpe:2.3:a:microsoft:http_server_api:2.0:	development	12/01/2025	15/01
web framework 1	PureFTPd	cpe:2.3:a:pureftpd:pureftpd:	ftpserver	12/01/2025	15/01
VENDOR	Telecomitalia	cpe:2.3:s:telecomitalia:telecomitalia:		12/01/2025	15/01
Microsoft 5	Microsoft Internet Information Services	cpe:2.3:a:microsoft:internet_information_services:	web server	12/01/2025	15/01
Generic 2	OpenBSD OpenSSH 7.4	cpe:2.3:a:openbsd:openssh:7.4:	sshserver	12/01/2025	15/01
OpenBSD 2	Dovecot	cpe:2.3:a:dovecot:dovecot:	imapserver mailserver	12/01/2025	15/01
IMAP 1	Microsoft Internet Information Services 10.0	cpe:2.3:a:microsoft:internet_information_services:10.0:	web server	12/01/2025	15/01
Exim 1	Generic FTP	cpe:2.3:a:generic:ftp:	ftp	12/01/2025	15/01
MariaDB 1					
SSH 1					

VALORE PRINCIPALE

- Monitoraggio strutturato del rischio legato a fornitori e partner esterni
- Visibilità continua sulla supply chain digitale
- Supporto alla gestione del rischio di terze parti (TPRM)

SEZIONE ASSET

- Inventario completo degli elementi associati ai fornitori:
 - Domini
 - Indirizzi IP
 - Host
 - Email
 - Servizi
- Per ogni asset sono disponibili:
 - Stato
 - Punteggio di affidabilità
 - Data dell'ultima verifica
- Supporto a una due diligence dinamica
- Individuazione rapida di variazioni nell'esposizione

SEZIONE PROBLEMI

- Evidenziazione delle criticità rilevate:
 - Vulnerabilità applicative
 - Errori di configurazione
 - Assenza di header di sicurezza
 - Anomalie DNS
- Per ogni problema:
 - Descrizione dettagliata
 - Contesto
 - Indicazioni per la remediation

ANALISI E GESTIONE DEL RISCHIO

- Integrazione tra TPRM e threat intelligence
- Identificazione rapida dei punti deboli
- Definizione delle priorità di intervento
- Riduzione del rischio di compromissione indiretta

NEWS

The screenshot displays the 'News & Report' section of the Meridian platform. At the top, there are navigation tabs for different threat levels: All (10447 items), TLP-RED (11 items), TLP-AMBER (184 items), TLP-AMBER+STRICT (10 items), TLP-GREEN (240 items), and TLP-CLEAR (19 items). Below these is a search bar and a filter icon. The main content area is a grid of news cards, each with a title, a brief description, a date, and a category tag. The cards are organized by date, with the most recent at the top. The interface is clean and professional, with a focus on delivering timely and relevant security news.

VALORE PRINCIPALE

- Raccolta in tempo reale di contenuti da oltre 50.000 fonti qualificate
- Possibilità di filtrare le notizie per:
 - Tipologia
 - Data
 - Livello di criticità
- Accesso rapido a informazioni aggiornate e rilevanti

ANALISI DEL CONTESTO

- Integrazione tra dati tecnici e informazioni di scenario
- Supporto nell'individuazione di:
 - Tendenze emergenti
 - Vulnerabilità zero-day
 - Nuove campagne
 - Impatti normativi e geopolitici

FUNZIONALITÀ OPERATIVE

- Possibilità di salvare le ricerche
- Creazione di liste tematiche di monitoraggio (watchlist)
- Collegamento degli articoli a:
 - Incidenti
 - Campagne
 - Attori coinvolti
- Creazione di dossier condivisibili con:
 - Figure tecniche
 - Figure non tecniche

BENEFICI

- Riduzione delle informazioni non rilevanti
- Maggiore copertura e completezza delle notizie
- Supporto a decisioni più rapide e proattive, basate su fonti affidabili e verificabili

REPORT

News & Report

Search filter Sort by: Latest

All 10447 Items	TLP:RED 11 Items	TLP:AMBER 104 Items	TLP:AMBER+STRICT 70 Items	TLP:GREEN 248 Items	TLP:CLEAR 19 Items										
Italy Alleged TheGentlemen Ransomware Incident Involving Gaposa S.R.L. #Ransomware A new victim (originally attributed to TheGentlemen reference Gaposa S.R.L., an Italy-based company in Fermo (FM) operating in the metal structure manufacturing sector. Available material associated with the leak... Industrials and Engineer... 03/31/2026	DDoS Aviation Target Update for Today #DDoS #Informational The pro-Russian hacktivist group NullKaw05 (NKG) has updated its DDoS target list with a focus on Danish and Greenlandic public-sector infrastructure. The dataset features a broad range of Danish governmental... Aviation Civil Aviation Transportation 03/31/2026	Morocco Claimed DDoS Activity Targeting Multiple Moroccan Government Ministries #DDoS #Data Breach An actor identifying as legitimate reportedly claimed DDoS activity targeting multiple Moroccan government ministries, including the Ministry of Foreign Affairs, Ministry of Justice, Ministry of Economy & Finance... Government 03/31/2026	Italy Alleged NetRunner Ransomware Incident Involving GEG Telecomunicazioni #Ransomware A listing attributed to NullKaw05 reference GEG Telecomunicazioni a ransomware-related context on the group's leak site, with an initial indicating the status as "Leaked, Estimated" the public... Telecommunications 03	Italy Alleged TheGentlemen Ransomware Incident Involving Zanzi S.p.A. #Ransomware On the leak site belonging to TheGentlemen, a new victim identified as Zanzi S.p.A. was posted. No public details are currently available regarding any ransom demand, and no samples or volume of allegedly stolen... Industrials and Engineer... 03/30/2026	France Alleged Data Sale Involving La Centrale de Financement on Breached #Data Breach An actor using the moniker "Ezio" on the underground forum "Breacher" is advertising an alleged data breach involving La Centrale de Financement. La Centrale de Financement is a French financial services company... Finance 03/30/2026	Italy Alleged SCADA/HMI Compromise Involving a Building Management System #Informational In a post attributed to the Telegram channel "MonsieurG", published on 30 March 2026, the actor claims to have gained unauthorized access to a building management system (BMS) of an unidentified Italian government... Other 03/30/2026	Denmark DDoS Targets Update for Today #DDoS #Campaign The pro-Russian hacktivist group NullKaw05 has updated its target list for Denmark-related assets. The most relevant entries include an initial targets such as Aalborg Airport (Aalborg Lufthavn), Aalborg... Aviation Civil Aviation Government Transportation 03	Uganda Mysterious Team Bangladesh Claims Coordinated DDoS Campaign Against Multiple U.S. Targets #DDoS Mysterious Team Bangladesh has reportedly claimed a coordinated DDoS campaign targeting multiple Uganda-based websites on 29 March 2026 under the operation hashtag #26Uganda. Claimed targets included... Aviation Civil Aviation 03/30/2026	United States Update on Alleged Compromise Involving Lockheed Martin #Data Breach #Informational APT (RAT) previously claimed an alleged breach involving Lockheed Martin, a major U.S. aerospace, defense, and security company, asserting that approximately 375 terabytes of data had been exfiltrated and made... Aviation Industrials and Engineer... 03/30/2026	Italy Alleged SCADA/HMI Compromise Involving an Industrial Generator Control System #Data Breach #Informational In a post attributed to Z Perpetual Alliance, the actor claims to have compromised an industrial generator control system in Italy. The reference and system appears to be an Italy-based industrial power generation... Energy 03/30/2026	Italy BD Anonymous Team Claims DDoS Involving Regione Molise #DDoS BD Anonymous Team has claimed a DDoS attack involving the website of the Regione Molise (regione.molise.it) on March 30, 2026... sectors:GOVERNMENT 03	Italy Alleged SCADA/HMI Compromise Involving an Industrial Diesel Generator Facility #Informational In a post attributed to Z Perpetual Alliance, the actor claims to have gained unauthorized access to the control systems of an Italy-based industrial...	Italy Alleged Compromise Involving ITA Airways #Data Breach #Informational ITA Airways has disclosed a security incident affecting users of its Volare loyalty programme, and stated that internal incident management procedures and technical analysis were activated following the report. IT...	France Alleged ALP 001 Ransomware Incident Involving Iliad S.A. #Ransomware A leak site entry attributed to the ransomware group ALP 001 reference a leak R.A. (leak 01) is a ransomware-related context. Available material...	United Kingdom Alleged ALP 001 Ransomware Incident Involving KYOCERA Document Solutions #Ransomware A leak site entry attributed to the ransomware group ALP 001 is a KYOCERA Document Solutions Europe Management B.V. (ky...

VALORE PRINCIPALE

- Strumenti avanzati di reportistica e analisi storica
- Possibilità di:
 - Consultare report preconfigurati
 - Creare report personalizzati
- Analisi su:
 - Minacce
 - Incidenti
 - Vulnerabilità
 - Correlazioni

ANALISI E METRICHE

- Monitoraggio di indicatori chiave:
 - Efficacia dei controlli
 - Andamento degli SLA
- Supporto alla valutazione delle performance operative

REPORT PER GOVERNANCE

- Produzione di report pronti per audit (audit-ready)
- Supporto a:
 - Comitati rischi
 - Organismi di vigilanza
- Comunicazione semplificata verso stakeholder non tecnici

PERFORMANCE SOC

- Misurazione continua delle prestazioni:
 - Tempo medio di rilevazione (MTTD)
 - Tempo medio di risposta (MTTR)
 - Tasso di falsi positivi
 - Copertura delle regole
- Individuazione di aree di miglioramento
- Ottimizzazione degli investimenti

IMPATTO

- Collegamento tra operatività quotidiana e governance strategica
- Maggiore responsabilità (accountability) nelle decisioni
- Aumento del valore decisionale dei dati

ATTORI

Actors

Search Filter

ALL RED AMBER GREEN CLEAR

TLP-AMBER-STRICT 03/31/2026 UNC6721 UNC6721 is a suspected North Korean financially motivated threat actor that delivers TURTLESNAPE and TURTLESHELL via Cloudflare's pages dev infrastructure. Updated On 03/31/2026	TLP-AMBER-STRICT 03/30/2026 UNC6760 Post-compromise threat group involved after ClickFix style infection vectors or the FAKETREFF JavaScript downloaders, where users are tricked into executing commands via cmd.exe... Updated On 03/30/2026	TLP-CLEAR 03/30/2026 BreachForums Updated On 03/30/2026	TLP-AMBER-STRICT 03/30/2026 UNC4037 UNC4037 is a suspected Belarusian espionage group since at least 2020 that has conducted credential harvest operations exploiting legitimate Zimbra and Roundcube Webmail (ESET) Webmail (S2 Group). Updated On 03/30/2026
TLP-AMBER-STRICT 03/27/2026 UNC6569 UNC6569 is a threat cluster active since at least October 2022 that has conducted multi-cloud intrusions across AWS, GCP, Azure, and GitHub environments for reconnaissance, privilege escalation, and data exfiltration. Updated On 03/27/2026	TLP-CLEAR 03/26/2026 North Korean APT group Updated On 03/26/2026	TLP-CLEAR 03/23/2026 Nasir Security Updated On 03/23/2026	TLP-CLEAR 03/23/2026 GhostClaw Updated On 03/23/2026
TLP-CLEAR 03/20/2026 VoidStealer Updated On 03/20/2026	TLP-CLEAR 03/20/2026 TeamPCP Updated On 03/20/2026	TLP-CLEAR 03/20/2026 Beast Updated On 03/20/2026	TLP-CLEAR 03/20/2026 Perseus Updated On 03/20/2026
TLP-CLEAR 03/18/2026 Runningcrab Updated On 03/18/2026	TLP-CLEAR 03/16/2026 Horabot Updated On 03/16/2026	TLP-CLEAR 03/16/2026 Konni Group Updated On 03/16/2026	TLP-CLEAR 03/16/2026 LeakNet Updated On 03/16/2026

VALORE PRINCIPALE

- Knowledge base sui principali attori di minaccia:
 - APT
 - Cyber crime
 - Hacktivismo
- Vista strutturata del panorama delle minacce

PROFILAZIONE DEGLI ATTORI

- Per ogni attore sono disponibili:
 - Tattiche, tecniche e procedure (MITRE ATT&CK)
 - Motivazioni
 - Obiettivi (target) preferiti
 - Campagne attribuite
- Maggiore comprensione del comportamento degli attaccanti

ANALISI E CONFRONTO

- Identificazione di pattern ricorrenti
- Valutazione delle capacità offensive
- Analisi dell'evoluzione nel tempo
- Supporto a:
 - Prioritizzazione dei controlli
 - Attività di threat hunting

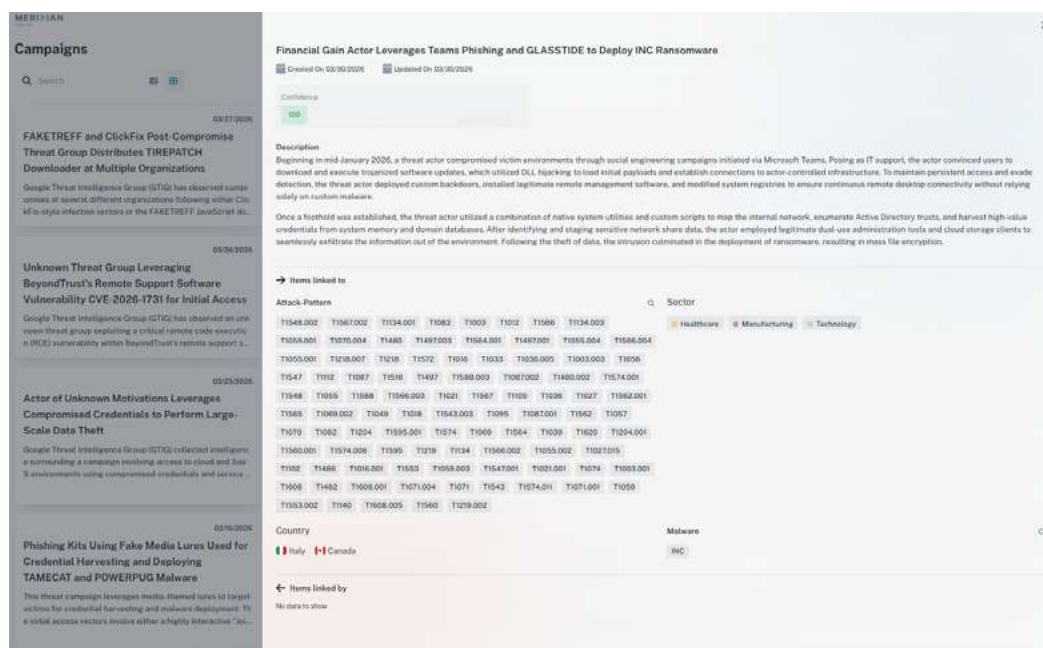
CORRELAZIONE E CONTESTO

- Correlazione tra:
 - Indicatori di compromissione (IOC)
 - Campagne
 - Incidenti
- Accelerazione dei processi di attribuzione
- Definizione di contromisure mirate

BENEFICI

- Maggiore consapevolezza del panorama delle minacce
- Riduzione dei tempi di investigazione
- Migliore allineamento delle regole di detection al rischio reale
- Supporto a decisioni più efficaci in ambito sicurezza

CAMPAGNE



VALORE PRINCIPALE

- Monitoraggio delle principali operazioni avversarie a livello globale
- Sintesi delle informazioni chiave:
 - Obiettivi
 - Tattiche, tecniche e procedure (TTP)
 - Infrastrutture di comando e controllo
 - Indicatori osservati
- Visione strutturata delle minacce in corso

ANALISI E IMPATTO

- Comprensione di come una campagna possa impattare i propri asset
- Supporto a:
 - Azioni preventive (hardening)
 - Aggiornamento delle regole di sicurezza
 - Comunicazioni mirate

FILTRI E PRIORITIZZAZIONE

- Possibilità di filtrare per:
 - Settore
 - Area geografica
 - Tecnica utilizzata
- Allineamento delle priorità difensive al contesto reale

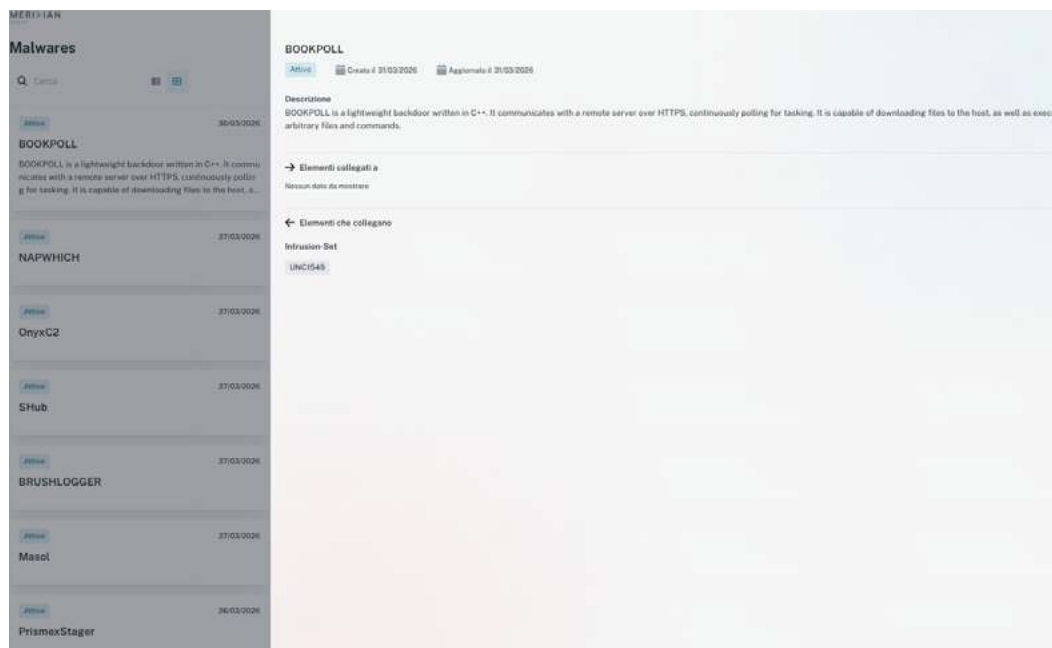
CORRELAZIONE E CONTESTO

- Collegamento con:
 - Attori, Indicatori di compromissione (IOC) e Report
- Creazione di dossier operativi pronti all'uso per:
 - SOC e Management

RISULTATI

- Postura di difesa più dinamica ed efficace
- Capacità di anticipare gli schemi di attacco
- Riduzione del gap informativo rispetto agli avversari
- Migliore capacità decisionale in ambito sicurezza

MALWARE



VALORE PRINCIPALE

- Repository operativo di campioni malevoli
- Classificazione per:
 - Famiglia
 - Tipologia
 - Comportamento osservato

ANALISI E IMPATTO

- Ogni elemento include:
 - Indicatori tecnici
 - Note analitiche
 - Collegamenti a campagne e attori
- Supporto alle attività di:
 - Reverse engineering
 - Triage

AUTOMAZIONE E DETECTION

- Generazione rapida di indicatori di compromissione (IOC)
- Alimentazione delle regole di rilevazione (detection rules)
- Miglioramento continuo delle capacità di difesa

INTEGRAZIONE SANDBOX

- Analisi del comportamento reale dei malware
- Maggiore accuratezza nelle analisi
- Riduzione dei falsi positivi

BENEFICI

- Maggiore copertura di rilevazione (detection)
- Riduzione dei tempi di risposta
- Riutilizzo strutturato dell'intelligence nei playbook

VULNERABILITÀ

MEDIAN

VALORE PRINCIPALE

Gestione completa del ciclo CVE → Remediation

Informazioni disponibili per ogni vulnerabilità

- Severità
- Possibili modi di sfruttamento
- Asset impattati
- Riferimenti a fonti ufficiali

ANALISI E PRIORITIZZAZIONE

Filtri e viste permettono di:

- Dare priorità agli interventi basandosi sul rischio (gravità, esposizione, criticità del business)
- Pianificare patching o mitigazioni alternative

CONTROLLO E MISURAZIONE

Collegando vulnerabilità ad asset e incidenti passati, l'analista può:

- Misurare il debito di sicurezza
- Valutare l'efficacia delle azioni correttive

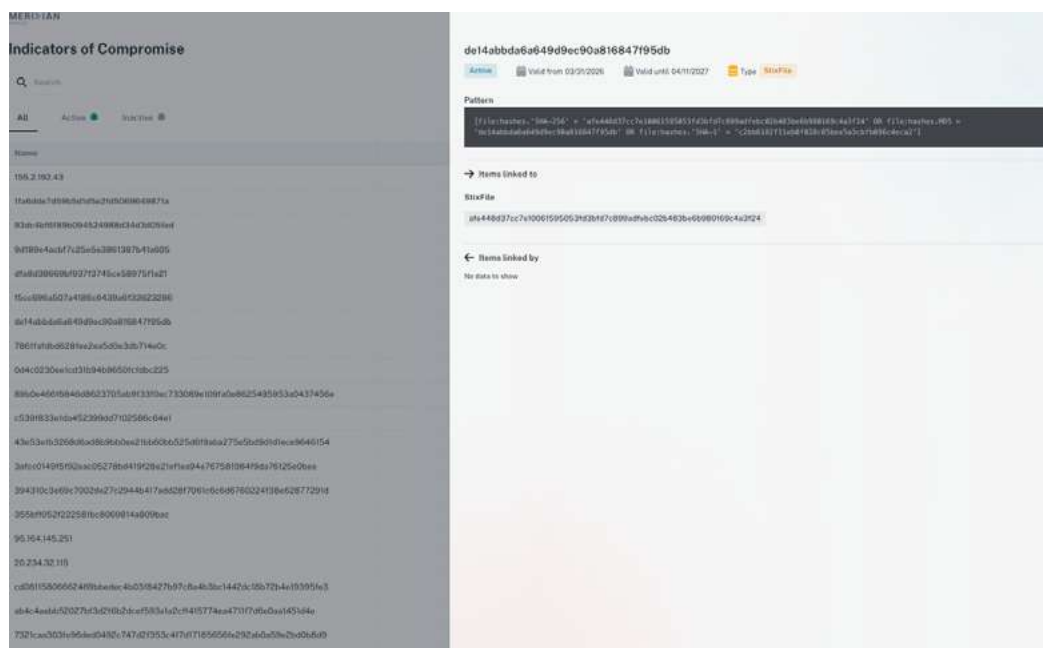
BENEFICI

- Riduzione delle finestre di rischio
- Ottimizzazione delle risorse
- Documentazione della conformità per audit e regolatori

IMPATTO

- Vulnerability management proattivo, più rapido ed efficace
- Miglioramento continuo della sicurezza aziendale

IOC



VALORE PRINCIPALE

Centralizzazione e gestione degli indicatori operativi

Tipologie di indicatori

- Hash
- IP
- Domini malevoli
- Altri indicatori operativi

CONTENUTI E ANALISI

IOC validati e contestualizzati permettono di:

- Correlare immediatamente con i log interni
- Alimentare SIEM, EDR e firewall per blocco e rilevamento automatico
- L'analista può valutare:
 - Freschezza e affidabilità degli IOC
 - Relazione con attori o campagne
 - Impatto potenziale sugli asset aziendali

AUTOMAZIONE E CONTROLLO

- Trasformazione dell'intelligence in controllo tecnico operativo
- Tracciabilità completa e riutilizzo nei playbook di detection e response

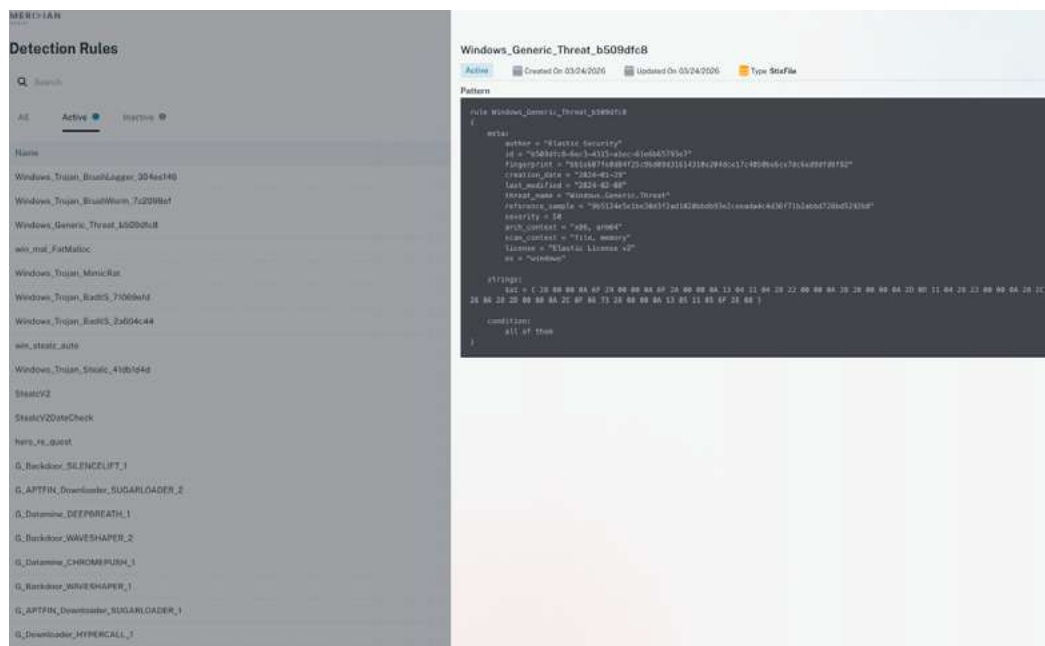
BENEFICI

- Riduzione del tempo tra scoperta e applicazione delle contromisure
- Maggiore precisione nelle regole
- Minori falsi positivi

IMPATTO

- Miglioramento continuo della difesa automatizzata
- Supporto a decisioni rapide e basate su intelligence

DETECTION RULES



VALORE PRINCIPALE

Repository di regole preconfigurate e custom allineate al rischio aziendale

COPERTURA E PRECISIONE

Classificazione per:

- Tipologia (Sigma, YARA, Snort)
- Profilo di rischio aziendale
- Segnale vs rumore

CONTENUTI E ANALISI

Ogni regola include:

- Parametri tecnici e condizioni di attivazione
- Collegamento a IOC, campagne e sandbox
- Possibilità di test e affinamenti incrementali

AUTOMAZIONE E TUNING

- Trasformazione delle minacce in regole attuabili in produzione
- Tuning continuo basato su metriche di efficacia
- Rimozione delle signature obsolete

BENEFICI

- Massimizza copertura e precisione della rilevazione
- Riduce falsi positivi e rumore
- Ciclo integrato minaccia → regola → produzione

IMPATTO

- Detection adattiva e coerente con tattiche avversarie
- Allineamento alle priorità di business
- Capacità di seguire le minacce emergenti

RANSOMWARE

The screenshot displays the Meridian Ransomware interface. On the left, a table lists various victims with columns for Name, Actor, and Organization. On the right, a detailed view for 'Parque Eólico Toabré' is shown, including its creation date (03/31/2026), confidence level (100), organization, country (Panama), and a description of the wind farm.

Name	Actor	Organization
everest has published a new victim: Parque Eólico Toabré	Everest	
ShinyHunters has published a new victim: Hallmark Cards, Inc. & Hallmark Plus	ShinyHunters	Hallmark
everest has published a new victim: PT Brantas Abipraya	Everest	
everest has published a new victim: Straight Line Logistics	Everest	
combassecartel has published a new victim: PG SOFT FRANCE - Lusked data	combassecartel	PG
combassecartel has published a new victim: Net-Sulair	combassecartel	
combassecartel has published a new victim: Prouflex	combassecartel	
combassecartel has published a new victim: Dronera	combassecartel	
combassecartel has published a new victim: Sisco	combassecartel	
combassecartel has published a new victim: Northernft	combassecartel	
combassecartel has published a new victim: Silver Peak	combassecartel	
combassecartel has published a new victim: Buffalo Neuroimaging Analysis Co...	combassecartel	Buffalo
combassecartel has published a new victim: Roshua	combassecartel	
combassecartel has published a new victim: Stubbious Ransom Murchison	combassecartel	
SilentRansomGroup has published a new victim: James Day	SilentRansomGroup	
play has published a new victim: Breks	RECESS SPIDER	
play has published a new victim: Colorado Construction	RECESS SPIDER	
play has published a new victim: Lucky Look	UNCK789	
play has published a new victim: Weber Kracht & Chelone	UNCK789	

Parque Eólico Toabré
Created On: 03/31/2026 | Confidence: 100
Organization: Parque Eólico Toabré | Country: Panama

Description
(AI generated) Parque Eólico Toabré is a wind farm based in Panama operated by Union Eólica Panameña. With a total capacity of 55 MW and 22 wind turbines, it contributes significantly to generating renewable energy. In addition to lowering the country's reliance on fossil fuels, the farm represents a sustainable solution for producing electricity.

VALORE PRINCIPALE

Sorveglianza mirata su gruppi, varianti e campagne in corso

INFORMAZIONI DISPONIBILI

- Sintesi di TTP (Tattiche, Tecniche, Procedure)
- Note tipiche di riscatto
- Vettori iniziali di attacco
- Settori più colpiti
- Collegamenti a IOC e detection rules correlate

ANALISI E EARLY WARNING

La vista consente di:

- Rilevare nuove ondate di attacchi
- Valutare l'esposizione degli asset critici
- Prioritizzare controlli: backup, segmentazione, hardening RDP/VPN, policy di macro

CONTROLLO E MITIGAZIONE

- Preparazione di contromisure efficaci
- Accelerazione del triage
- Allineamento con IT e Business Continuity su piani di risposta e ripristino

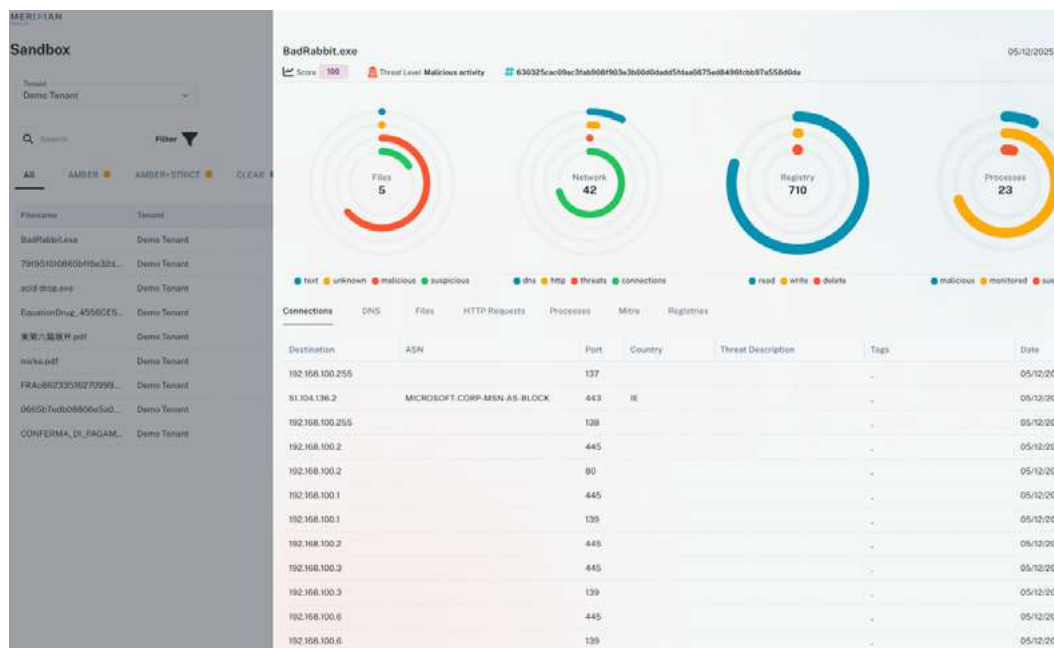
BENEFICI

- Riduzione dell'impatto potenziale di minacce ad alta severità
- Abilitazione di prevenzione e risposta tempestive

IMPATTO

- Maggiore protezione e resilienza del SOC contro attacchi ransomware
- Supporto decisionale rapido e mirato

SANDBOX



VALORE PRINCIPALE

Ambiente controllato e isolato per analisi dinamica di file sospetti

TELEMETRIE E INFORMAZIONI RACCOLTE

- Monitoraggio di processi e connessioni
- Modifiche a file system e registro
- Indicatori comportamentali dei campioni
- Risultati che alimentano IOC e detection rules

ANALISI E VERIFICA

- Conferma o smentita di ipotesi sugli attacchi
- Evidenzia artefatti post-infezione
- Test di contromisure prima della distribuzione

AUTOMAZIONE E TRIAGE

- Chiusura del ciclo tra analisi e enforcement
- Accelerazione del triage
- Miglioramento dell'accuratezza
- Limitazione dell'esposizione a payload sconosciuti

BENEFICI

- Supporto a una postura difensiva evidence-based
- Migliore preparazione e decisioni più sicure per gli analisti

IMPATTO

- Riduzione dell'incertezza nelle analisi malware
- Potenziamento della difesa operativa e della resilienza SOC



Beyond Cyber Security, Meridian group.



info@meridian-group.eu | www.meridian-group.eu | pec: meridiangroup@legalmail.it | Tel: +39 06 9970 6680 | Viale Erminio Spalla 09, 00142 - Roma (RM) | P.IVA/C.F. 13693001003