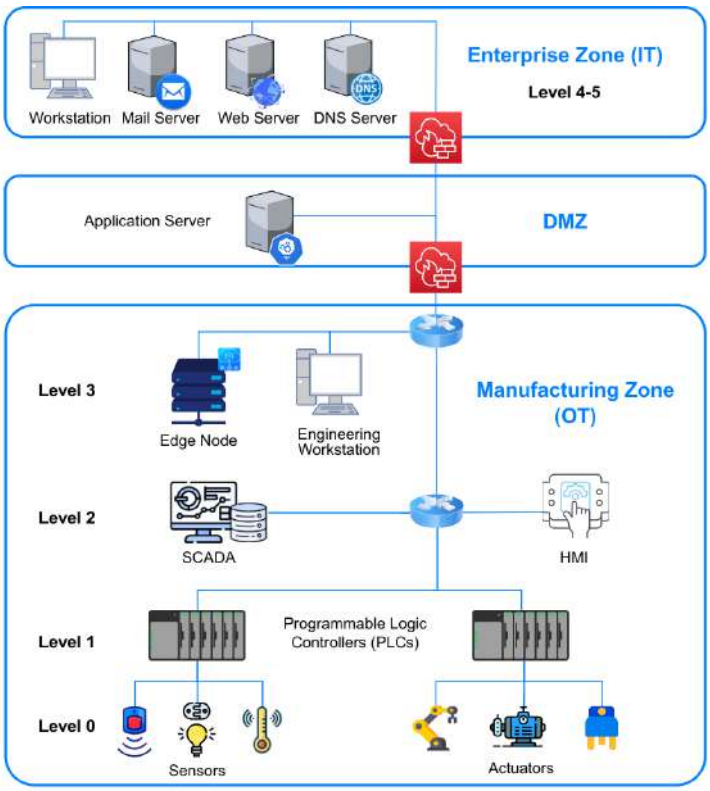
LA SUITE MON5

CARATTERISTICHE TECNICHE

Abbiamo sviluppato una soluzione di cybersicurezza per **ambienti industriali** complessi, applicabile a qualsiasi infrastruttura OT (tecnologia operativa).
Il sistema ideato si colloca tra i livelli 3 e 1 del Modello Purdue, offrendo una serie di vantaggi per la gestione efficace delle reti e l'attività di monitoraggio dei dispositivi.

Funzionalità di Mon5:

- Asset Discovery
- Threat analysis device
- Monitoraggio della rete industriale
- Strumento abilitante per la conformità alla IEC 62443
- Integrazione con gli MSSP



ICS Purdue Reference Architecture

Asset Discovery

Mon5 ASSET DISCOVERY sfrutta tecnologie avanzate di scansione e rilevamento per identificare con precisione ogni dispositivo connesso via IP o Ethernet all'interno della rete di uno stabilimento.

Questo include un'ampia gamma di asset, dai PLC (Programmable Logic Controllers), HMI (Human-Machine Interfaces), sensori e attuatori fino a router, switch e firewall.

Utilizzando metodi di rilevamento sia passivi che attivi, Mon5 garantisce l'identificazione anche dei dispositivi più discreti, senza interferire con i processi operativi.

Informazioni dettagliate sugli asset tramite Context-aware polling

Mon5 ASSET DISCOVERY raccoglie e visualizza informazioni complete per ciascun asset rilevato, inclusi tipo di dispositivo, produttore, modello, versione del firmware e vulnerabilità note.

Queste informazioni sono fondamentali per mantenere un **inventario aggiornato degli asset** dello stabilimento e per condurre valutazioni di sicurezza approfondite.
Comprendendo le caratteristiche specifiche e le potenziali vulnerabilità di ogni asset, le organizzazioni possono adattare le misure di sicurezza e le pratiche di manutenzione alle esigenze uniche del proprio ambiente OT (tecnologia operativa).

L'estrazione di questi dati avviene tramite interrogazione contestuale (Context-aware polling), che consente un recupero efficiente e mirato delle informazioni da PLC, sensori e altri dispositivi da campo.

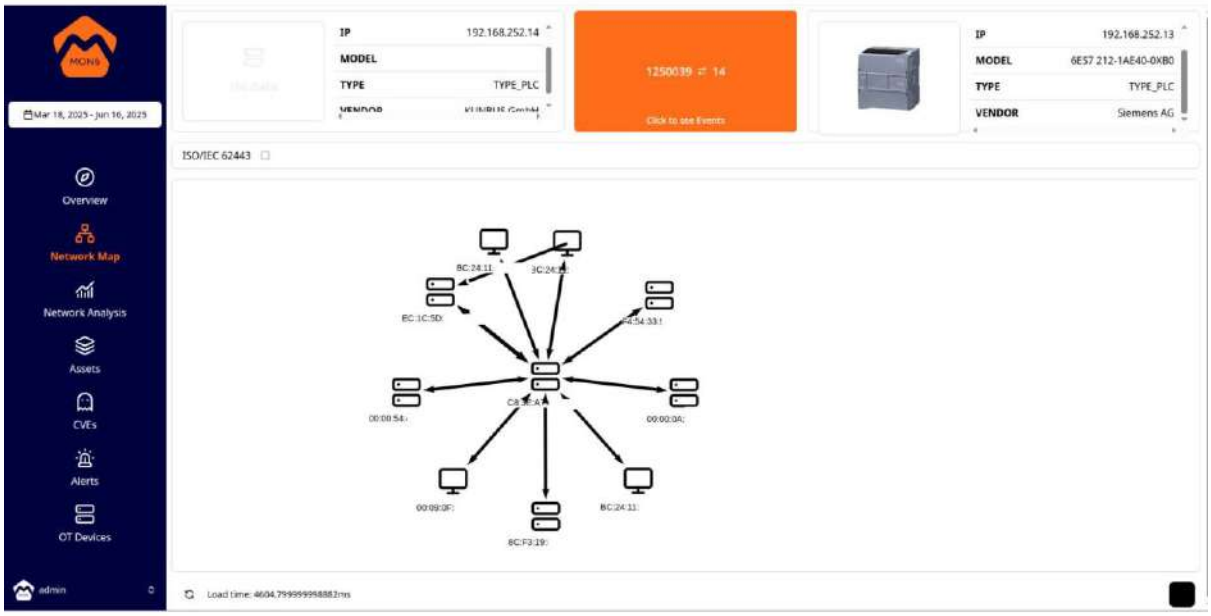
A differenza delle interrogazioni continue o forzate (brute-force), l'interrogazione contestuale **pianifica dinamicamente le richieste in base al tipo di dispositivo**, al suo stato o alla priorità. Questo approccio riduce la congestione della rete e il carico sulla CPU dei sistemi di controllo, migliorando la reattività.
L'interrogazione contestuale aumenta la scalabilità e la resilienza informatica delle reti industriali, minimizzando l'esposizione a traffico non necessario.

MON5 S.R.L.
sede operativa: via Paolo Nanni Costa 20 , Bologna
www.mon5.it - team@mon5.it

Mappatura Dinamica della Topologia dell'Impianto

Al momento del rilevamento, **Mon5 ASSET DISCOVERY** genera una mappa dinamica che rappresenta visivamente la topologia della rete, illustrando come sono interconnessi i dispositivi.

Questa mappa non è statica: **si aggiorna in tempo reale** con l'aggiunta o la rimozione di dispositivi, oppure quando cambiano le connessioni.
La funzionalità di mappatura è progettata per permettere agli utenti di navigare facilmente all'interno di reti industriali complesse.
Evidenzia i percorsi critici, identifica i potenziali colli di bottiglia e individua le vulnerabilità mostrando le relazioni tra i dispositivi.



Assets Map

Real-Time Detection and Updates

Una delle caratteristiche principali del sistema Mon5 ASSET DISCOVERY è la sua capacità di **rilevare in tempo reale le nuove connessioni di dispositivi**.

Ogni volta che un nuovo dispositivo si collega alla rete, Mon5 lo identifica automaticamente e aggiorna di conseguenza la mappa dello stabilimento. Questo

MON5 S.R.L.
sede operativa: via Paolo Nanni Costa 20 , Bologna
www.mon5.it - team@mon5.it

garantisce una visibilità degli asset sempre aggiornata, permettendo di individuare immediatamente connessioni non autorizzate o inattese che potrebbero rappresentare rischi per la sicurezza o problemi operativi.

Threat analysis device

Identificazione Approfondita di Vulnerabilità e Errori di Configurazione

Mon5 ASSET MANAGER analizza ogni asset all'interno della rete, valuta i protocolli di rete, controlla le configurazioni errate più comuni e individua le debolezze di sicurezza.

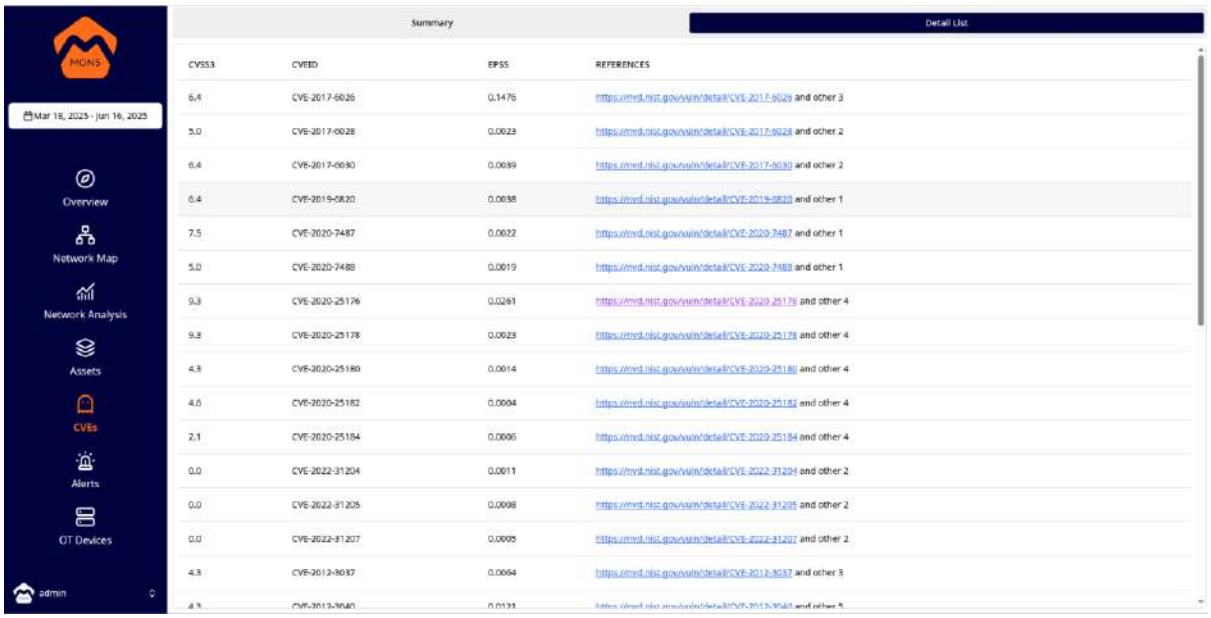
Questa analisi garantisce che le vulnerabilità vengano rilevate non solo in base alla loro presenza, ma considerando anche il contesto specifico in cui sono implementate nell'ambiente industriale.

Allerte di Impatto Basate su CVE e Valore di Esposizione

Per ogni vulnerabilità identificata, **Mon5 ASSET MANAGER genera un alert di impatto**. Queste allerte si basano sul database Common Vulnerabilities and Exposures (CVE), che fornisce un identificatore standardizzato per le vulnerabilità note.

Inoltre, Mon5 valuta il valore di esposizione di ciascuna vulnerabilità, considerando fattori come l'accessibilità di rete, la criticità dell'asset e il potenziale impatto in caso di sfruttamento.
Questo doppio approccio permette una comprensione più precisa della minaccia rappresentata da ogni vulnerabilità, andando oltre il rischio teorico.

MON5 S.R.L.
sede operativa: via Paolo Nanni Costa 20 , Bologna
www.mon5.it - team@mon5.it



Vulnerability and Misconfiguration Analysis

Valutazione del Rischio degli Asset con EPSS

Mon5 ASSET MANAGER integra l'**Exploit Prediction Scoring System (EPSS)** per calcolare un punteggio di rischio per ogni vulnerabilità identificata. EPSS fornisce una stima basata sui dati della probabilità che una vulnerabilità venga sfruttata, combinandola con il valore di esposizione dell'asset per generare un punteggio di rischio completo.

Questo punteggio riflette il rischio reale associato a ciascun asset, dando priorità alle vulnerabilità che rappresentano la minaccia più immediata per l'ambiente industriale.

Miglioramento Security Posture and Prioritized Remediation

Fornendo analisi dettagliate e punteggi di rischio concreti, Mon5 ASSET MANAGER consente alle organizzazioni di **migliorare il loro livello di sicurezza** attraverso decisioni strategiche e informate. I team di sicurezza possono prioritizzare gli interventi di remediation basandosi sui punteggi di rischio, concentrandosi sulle vulnerabilità con il potenziale impatto più elevato.

Questo approccio mirato alla gestione delle vulnerabilità garantisce un'allocazione efficiente delle risorse, rafforzando le difese nelle aree dove sono più necessarie.

MON5 S.R.L.
sede operativa: via Paolo Nanni Costa 20 , Bologna
www.mon5.it - team@mon5.it

Monitoraggio della rete industriale

La funzione di monitoraggio della piattaforma Mon5 migliora la sicurezza e l'integrità operativa degli ambienti industriali grazie alle capacità di rilevamento degli IOC (Indicatori di Compromissione) e delle anomalie.
Questa funzione sfrutta una combinazione di analisi del traffico e dei dispositivi, arricchita da tecniche di intelligenza artificiale (IA), per comprendere in modo completo la baseline operativa normale dello stabilimento.

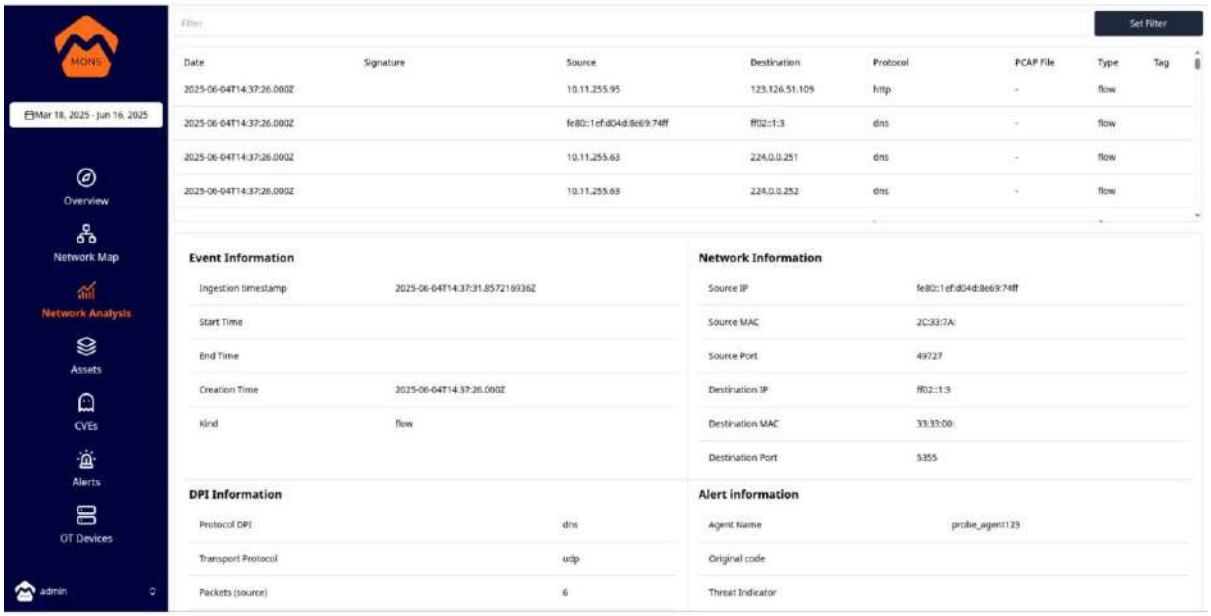
Definizione della Baseline Operativa

Mon5 raccoglie e analizza sistematicamente i dati di tutto il traffico di rete e dei dispositivi connessi per costruire una baseline operativa dettagliata dello stabilimento. Questa baseline rappresenta il comportamento standard delle comunicazioni di rete e delle operazioni dei dispositivi, includendo i flussi di dati tipici, le interazioni tra dispositivi e le attività previste dei protocolli.

Identificazione degli IOC e Rilevamento delle Anomalie

Con una baseline operativa chiara stabilita, Mon5 identifica le deviazioni che possono indicare minacce alla sicurezza o problemi operativi.
Gli Indicatori di Compromissione (IOC) vengono rilevati monitorando le attività di rete e dei dispositivi rispetto alla baseline stabilita.
Allo stesso modo, vengono utilizzati algoritmi di rilevamento delle anomalie per individuare schemi o cambiamenti insoliti nell'ambiente operativo che si discostano dalla baseline.
Questi possono variare da lievi variazioni nel traffico di rete a cambiamenti inattesi nel comportamento dei dispositivi, ciascuno potenzialmente indicativo di minacce informatiche o malfunzionamenti del sistema.

MON5 S.R.L.
sede operativa: via Paolo Nanni Costa 20 , Bologna
www.mon5.it - team@mon5.it

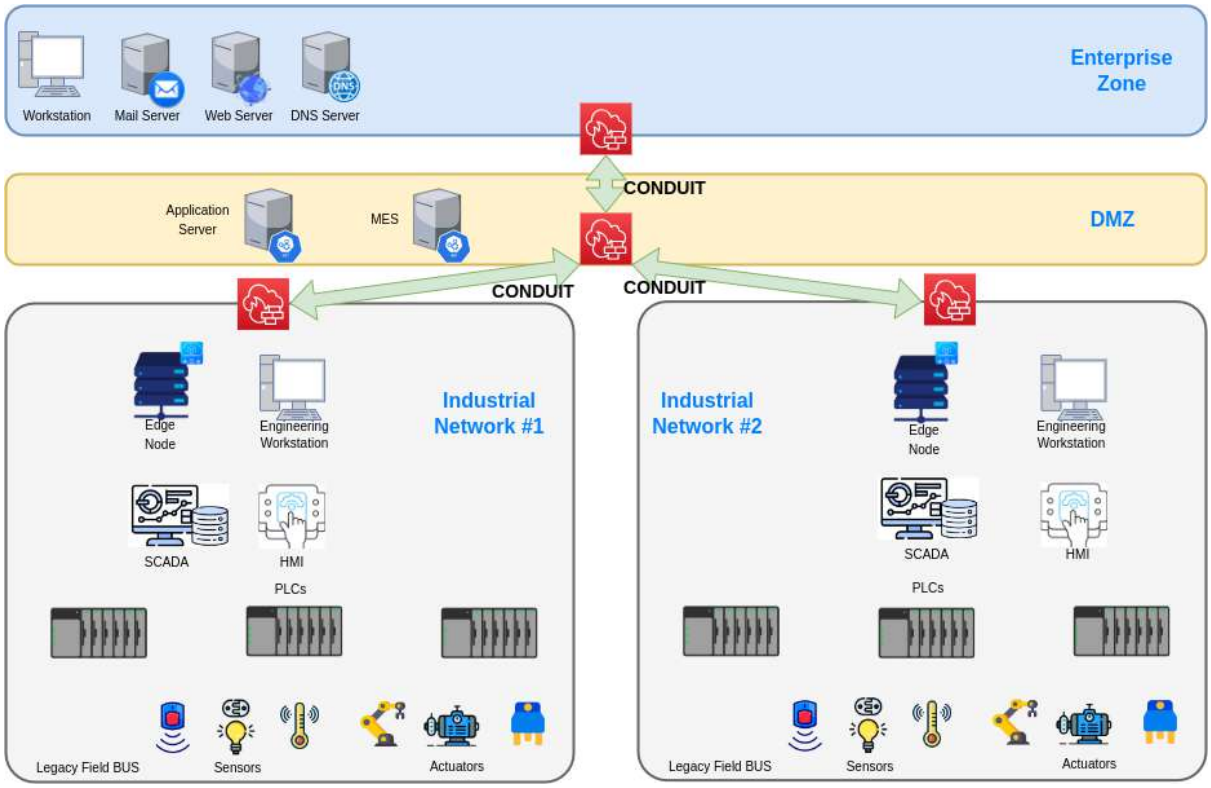


Network Analysis Tab

Strumento abilitante per la conformità alla IEC 62443

La funzionalità di **conformità alla IEC 62443 e alla Direttiva NIS2** della piattaforma Mon5 è progettata specificamente per supportare le realtà industriali nell'aderire a standard e direttive critiche di cybersicurezza.
Attraverso valutazioni e analisi approfondite, la piattaforma Mon5 offre una valutazione dettagliata della rete dello stabilimento rispetto allo standard IEC 62443, garantendo la conformità e migliorando le misure di sicurezza informatica.

MON5 S.R.L.
sede operativa: via Paolo Nanni Costa 20 , Bologna
www.mon5.it - team@mon5.it



IEC 62443 zones and conduit

Gli obiettivi della piattaforma includono:

Valutazione della Conformità allo Standard IEC 62443

Lo strumento di valutazione della conformità della piattaforma Mon5 esamina in profondità l'infrastruttura di rete dello stabilimento, analizzando ogni aspetto per allinearsi agli standard di cybersicurezza IEC 62443.
Questo insieme di standard è fondamentale per la sicurezza delle reti industriali, coprendo dai requisiti generali alle specifiche dettagliate di sistemi e componenti. La valutazione di Mon5 analizza il livello di sicurezza attuale dello stabilimento, identifica le lacune e fornisce indicazioni operative per raggiungere e mantenere la conformità a questi rigorosi standard.

Allineamento alla Direttiva NIS2

Come applicazione concreta della Direttiva NIS2, lo standard ISA/IEC 62443 guida la piattaforma Mon5 nell'estendere le sue capacità di valutazione per garantire l'allineamento ai requisiti di cybersicurezza dell'Unione Europea.

MON5 S.R.L.
sede operativa: via Paolo Nanni Costa 20 , Bologna
www.mon5.it - team@mon5.it

La piattaforma analizza l'efficacia delle pratiche di cybersicurezza dello stabilimento in conformità alla NIS2, con un focus particolare sulla protezione delle infrastrutture critiche.

Report di Conformità Dettagliati

A seguito della valutazione approfondita, la piattaforma Mon5 genera report dettagliati che descrivono il livello di adesione dello stabilimento allo standard ISA/IEC 62443. Questi report sono progettati per essere informativi e operativi, fornendo chiare indicazioni sul livello di conformità, evidenziando le aree di non conformità e raccomandando azioni di remediation. Questo reporting dettagliato facilita interventi mirati per migliorare le pratiche di cybersicurezza, garantendo il rispetto di tutti gli standard e le direttive necessari.

Miglioramento delle Misure di Cybersicurezza

L'obiettivo finale della funzionalità di conformità IEC 62443 e Direttiva NIS2 della piattaforma Mon5 è potenziare le misure di cybersicurezza negli ambienti industriali. Fornendo un quadro chiaro per la conformità e offrendo approfondimenti dettagliati sul livello di sicurezza dello stabilimento, Mon5 consente alle organizzazioni di implementare strategie robuste di cybersicurezza che proteggono contro le minacce in evoluzione, assicurando al contempo il rispetto delle normative e degli standard internazionali.

Integrazione con gli MSSP

L'implementazione della piattaforma Mon5 include un cruscotto completo e pienamente operativo, progettato per migliorare la visibilità e la gestione della cybersicurezza negli ambienti industriali.

Questo cruscotto ricco di funzionalità è supportato dall'architettura software modulare di Mon5, che facilita l'integrazione fluida con i Security Operations Center (SOC) esistenti e i sistemi di Security Information and Event Management (SIEM).

MON5 S.R.L.
sede operativa: via Paolo Nanni Costa 20 , Bologna
www.mon5.it - team@mon5.it

Ecco una panoramica dettagliata di questa funzionalità, con l'evidenziazione dei suoi componenti principali e delle capacità di integrazione:

Dashboard Operativa Completa

Il cruscotto della piattaforma Mon5 è progettato per offrire una vista centralizzata del livello di cybersicurezza della rete, garantendo un accesso intuitivo a diversi punti dati critici:

- **Mappa dei Dispositivi**
  Una rappresentazione visiva di tutti i dispositivi presenti nella rete, con dettagli sulle loro connessioni e stato. Questa mappa viene aggiornata dinamicamente, assicurando una visibilità in tempo reale dell'architettura di rete.

- **Eventi e Rilevamento Allerte**
  Il cruscotto aggrega e mostra eventi di sicurezza e allerte, permettendo una rapida identificazione di potenziali minacce e anomalie.

- **Report sulle Minacce**
  Questo report presenta un'analisi dettagliata delle minacce identificate, includendo natura, asset coinvolti e strategie di mitigazione consigliate.

- **Regole Personalizzabili**
  Gli utenti possono definire e personalizzare regole per il rilevamento delle minacce, consentendo misure di sicurezza su misura che rispondono a specifiche esigenze operative.

Architettura Modulare per una Facile Integrazione

L'architettura software modulare della piattaforma Mon5 è una caratteristica chiave che consente una facile integrazione con i framework di cybersicurezza esistenti:

- **Compatibilità con SOC**
  La piattaforma Mon5 può essere integrata senza soluzione di continuità nei Security Operations Center (SOC), migliorandone la capacità di monitorare e rispondere agli incidenti di sicurezza nelle reti industriali. Questa integrazione facilita la condivisione delle informazioni di cybersicurezza, aumentando la

MON5 S.R.L.
sede operativa: via Paolo Nanni Costa 20 , Bologna
www.mon5.it - team@mon5.it

consapevolezza situazionale complessiva e l'efficacia della risposta dei SOC.

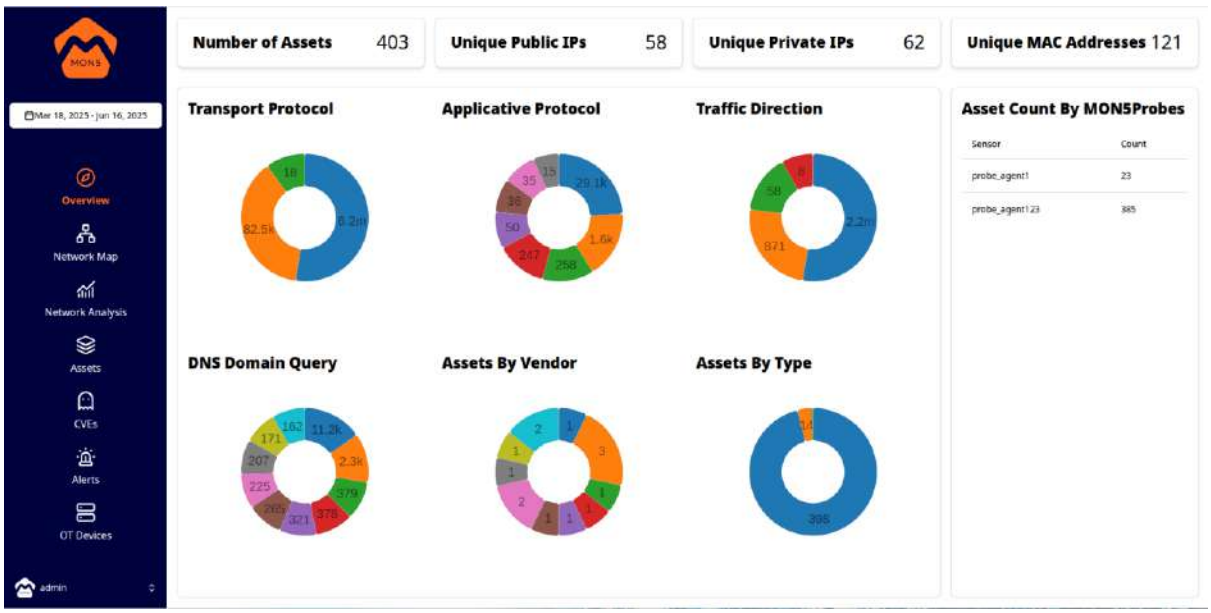
- **Sinergia con SOC**
  L'integrazione con i sistemi SOC è semplice, permettendo la correlazione dei dati di sicurezza dettagliati della piattaforma Mon5 con le più ampie analisi di sicurezza. Questa sinergia arricchisce il dataset del SIEM, fornendo una comprensione più approfondita degli eventi di sicurezza e facilitando un rilevamento e una risposta alle minacce più precisi e tempestivi.

Streamlined Integration and Operations

Il design della piattaforma Mon5 pone l'accento sulla facilità di integrazione, garantendo che la sua implementazione rafforzi le operazioni di cybersicurezza esistenti senza richiedere modifiche sostanziali.

La piattaforma offre API personalizzate per comunicare con i sistemi SOC e semplifica i flussi di lavoro legati alla sicurezza informatica, migliorando l'efficienza e l'efficacia delle operazioni di sicurezza.

Questa capacità di integrazione è fondamentale per le organizzazioni che desiderano potenziare le proprie difese informatiche con un impatto minimo sui processi già in atto.



Dashboard Data Report

MON5 S.R.L.
sede operativa: via Paolo Nanni Costa 20 , Bologna
www.mon5.it - team@mon5.it