Adeguamento alla Direttiva Europea 2022/2555

NIS 2

Allineamento agli Standard Europei per la gestione della Sicurezza in ambito Cyber Security e capacità di Incident Response

Nel dicembre 2022, gli Stati membri dell'UE hanno formalmente emanato una revisione della Direttiva precedente sulla sicurezza delle reti e dei sistemi informatici (Network and Information Systems - NIS), e pubblicata a gennaio 2023 nella Gazzetta Ufficiale Europea con il riferimento 2022/2555.

La **Direttiva NIS2** aggiornata è stata progettata per ampliare il campo di applicazione dell'originale. Concepita in risposta a diversi cyber attacchi ampiamente diffusi e dannosi, la **Direttiva NIS2** rafforza i requisiti di sicurezza, razionalizza gli obblighi di reportistica e introduce misure di supervisione più rigide e requisiti di applicazione più rigorosi.

L'obiettivo è pertanto quello di innalzare e standardizzare il livello di sicurezza all'interno della Unione Europea, coinvolgendo anche la gestione della filiera dei fornitori (**supply chain**), per evitare l'effetto domino degli attacchi ransomware e altre minacce informatiche.

Tutti i 27 Stati membri della UE sono tenuti a ratificare la Direttiva NIS2 entro ottobre 2024

NIS 2

> "Member States shall ensure that **essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems** which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. "

- **Più settori interessati**
- **Più entità coinvolte**
- **Nuovi metodi di selezione e registrazione dei fornitori**
- **Nuovi termini di notifica degli incidenti**
- **Requisiti aggiuntivi per Risk Assessment e Audit**

NIS2, si applica a più settori industriali

La direttiva NIS2 è applicata a un insieme più ampio di entità:

- **Essenziali**
- **Importanti**

Gli obblighi sono gli stessi per entrambe, ma quelle **Essenziali** sono soggette a misure di applicazione e sanzioni più rigorose.

La Direttiva NIS2 si applica a qualsiasi entità che fornisca servizi critici all'interno di un Paese membro UE, indipendentemente da dove si trova tale entità

Le organizzazioni che operano nei seguenti settori sono considerate **Essenziali**

- Sanità
- Energia
- Trasporti
- Finanza
- Approvvigionamento idrico
- Bancario
- ICT
- Acque reflue
- Salute (farmaci, R&S, dispositivi medici critici)
- Spaziale
- Amministrazione pubblica

NIS2 introduce una seconda categoria di entità, denominate **Importanti**

- Servizi postali e corrieri espresso
- Chimico
- Alimentare
- Manifatturiero
- Digital Provider - *(piattaforme di social networking, motori di ricerca, marketplace online)*
- Servizi postali e corrieri espresso
- Gestione dei rifiuti
- Organizzazioni di ricerca

I cambiamenti chiave, dalla NIS alla NIS2

L'articolo 21 del NIS2 obbliga gli Stati membri a garantire che le entità Essenziali e Importanti gestiscano il Rischio implementando sistemi, policy e best practice efficaci che coprano un'ampia gamma di misure e discipline di cybersecurity, tra cui:

- Analisi dei rischi e sicurezza dei sistemi informatici;
- Gestione e reportistica degli incidenti;
- Continuità operativa, come la gestione dei backup e il ripristino di emergenza;
- Gestione delle crisi;
- Sicurezza della supply chain;
- Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi;
- Pratiche di base per la cyber-igiene e formazione sulla cyber security;
- Tecnologie di crittografia e cifratura;
- Sicurezza delle risorse umane, policy di controllo degli accessi e gestione delle risorse;
- Accesso Zero Trust (autenticazione multifattore, autenticazione continua).

Gestione e reportistica degli incidenti

La Direttiva NIS2 impone ad ogni entità critica, obblighi di notifica per gli incidenti che hanno un "impatto significativo" sulla fornitura dei loro servizi. Queste notifiche devono essere effettuate presso l'autorità competente o il **CSIRT** (*Computer Security Incident Response Team*) del proprio Paese di appartenenza.

Nuove definizioni NIS2

Incidente: "qualsiasi evento che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati memorizzati, trasmessi o elaborati, o dei relativi servizi offerti o accessibili tramite i sistemi di rete e di informazione".

Notifiche minacce cyber: "impatto significativo sulla fornitura di servizi, quindi circostanze che:
- hanno causato/possono causare interruzioni operative o perdite finanziarie;
- hanno colpito/possono colpire altre persone causando perdite considerevoli".

Notifica incidenti: "indipendentemente dal fatto che l'entità sia importante o essenziale, la soglia di segnalazione è l'impatto significativo sulla fornitura dei loro servizi".

Obblighi di notifica multi-livello:

EARLY WARNING

È un sospetto atto malevolo con potenziali impatti transfrontalieri?
Dal momento in cui si viene a conoscenza dell'incidente significativo, indicando se si sospetta che l'incidente significativo sia causato da atti illeciti o dolosi o possa avere un impatto transfrontaliero.

OFFICIAL INCIDENT NOTIFICATION

Valutazione dell'incidente, gravità e impatto, oltre a indicatori di compromissione.
Aggiornamento delle informazioni precedentemente fornite, indicando una valutazione iniziale dell'incidente significativo, compresi la gravità e l'impatto, nonché, se disponibili, gli indicatori di compromissione.

INTERMEDIATE STATUS REPORT

Su richiesta del CSIRT o dell'autorità competente pertinente.

FINAL REPORT

Se l'incidente è in corso al momento della relazione finale, verrà presentata una relazione di avanzamento e la relazione finale sarà fornita un mese dopo.

La redazione di una relazione finale comprende

- descrizione dettagliata dell'incidente, compresi la gravità e l'impatto;
- il tipo di minaccia o la causa principale che probabilmente ha scatenato l'incidente;
- le misure di mitigazione applicate e in corso;
- nel caso, l'impatto transfrontaliero dell'incidente.

Gestione e reportistica degli incidenti

Incidente	Tempo	
Primi segnali dell'incidente	0 h	**Indagine e definizione budget**
Installazione agenti endpoint su ampio perimetro	3 h	**Decisione strategica (contenimento/analisi)** 1° notifica ad ACN (obbligatoria)
Collezionamento telemetria dagli endpoint	15 h	**Attivazione e monitoraggio watchlist personalizzate** **+** **Analisi opzioni di contenimento**
	24 h	**Valutazione efficacia del contenimento** **+** **Drop connessioni di rete degli endpoint coinvolti**
	40 h	**Condivisioni della portata della compromissione e Discussione relativa al ripristino di alcuni dei processi principali del cliente in modo sicuro**
Confronto tra TTP osservate e threat intelligence per migliorare profilo avversario	53 h	**Discussioni su ulteriori azioni di mitigazione**
Ripristino sicuro dell'operatività	70 h	**2° notifica ad ACN (obbligatoria) per condivisione di gravità, impatto, IoC**
Formalizzazione rapporto finale con RCA e ulteriori dettagli	1 mese	**3° notifica ad ACN (obbligatoria) per condivisione descrizione incidente, causa, misure di mitigazione, impatto esterno**

ADEGUARSI ALLA NIS 2
GLI ADEMPIMENTI

ART 21.
Le misure di cui al paragrafo 1 sono basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti.

MISURE TECNICHE - IT Department
Predisporre strategie di controllo dell'accesso ai sistemi informativi aziendali:
Garantire la continuità operativa, come la gestione del backup e il ripristino in caso di disastro;
Attivare pratiche di igiene informatica di base;
Implementare l'uso di strumenti per:
- Crittografia
- Autenticazione a più fattori o di autenticazione continua
- Comunicazioni vocali, video e testuali protette;
- Sistemi di comunicazione di emergenza protetti da parte del soggetto anche al proprio interno, se del caso

GOVERNANCE

- **Politiche** di analisi dei rischi e sicurezza dei sistemi informatici e delle comunicazioni digitali
- **Gestione** e la divulgazione delle vulnerabilità
- **Strategie e procedure** per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;
- **Incident Response**
  - *Gestione degli eventi e incidenti di sicurezza;*
  - *Procedure di gestione delle crisi*

ORGANIZZAZIONE

Procurement
- **Valutazione** della qualità complessiva delle pratiche di cyber security della (supply chain, a norma dell'art. 22, paragrafo 1
- **Asseverazione certificata** della catena di approvvigionamento, relativamente alle misure di sicurezza

Human Resources
- **Formazione** in materia di cyber security
- **Sicurezza della gestione** delle risorse umane e dei dati trattati

IT Department
- **Sicurezza** dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete
- **Controllo** delle rispettive misure di sicurezza offerte e certificate dai rispettivi fornitori, dei prodotti e dei servizi

QUADRO SANZIONI
ART. 32

ART.32 RESPONSABILITÀ

ART 32. - MISURE DI VIGILANZA E DI ESECUZIONE
relative a soggetti ESSENZIALI & IMPORTANTI

a) ispezioni in loco e vigilanza a distanza, compresi controlli casuali, effettuati da professionisti formati;

b) audit sulla sicurezza periodici e mirati effettuati da un organismo indipendente o da un'autorità competente

e) richieste di informazioni necessarie a valutare le misure di gestione dei rischi di cibersicurezza adottate dal soggetto interessato, comprese le politiche di cibersicurezza documentate, nonché il rispetto dell'obbligo di trasmettere informazioni alle autorità competenti a norma dell'articolo 27;

g) richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova.

Responsabilità Personali

chiedere che gli organismi o gli organi giurisdizionali pertinenti, secondo il diritto nazionale, **vietino temporaneamente a qualsiasi persona che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale** in tale soggetto essenziale di svolgere funzioni dirigenziali in tale soggetto

Responsabilità dei Soggetti

sospendere temporaneamente o chiedere a un organismo di certificazione o autorizzazione, oppure a un organo giurisdizionale, secondo il diritto nazionale, di **sospendere temporaneamente un certificato o un'autorizzazione relativi a una parte o alla totalità dei servizi o delle attività pertinenti svolti dal soggetto essenziale**

ART.34 SANZIONI ECONOMICHE

SOGGETTI ESSENZIALI

Sanzioni economiche pari a un massimo di almeno 10 Mln/€ o a un massimo di almeno il 2 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto essenziale appartiene, se tale importo è superiore.

SOGGETTI IMPORTANTI

Sanzioni economiche pari a un massimo di almeno 7 Mln/€ di EURO o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto importante appartiene, se tale importo è superiore.

10 MODI PER AFFRONTARE LA NIS 2

Hy.S.A.C. NIS2GO

Hy.S.A.C. NIS2GO è la piattaforma virtuale di servizi e soluzioni tecnologiche per supportare le Organizzazioni nella gestione dell'esposizione informatica e rispondere alla totalità degli obblighi previsti dalla Direttiva NIS2.
A partire dall'analisi in tempo reale di ogni asset critico, alla discovery delle vulnerabilità, al rilevamento delle minacce dall'esterno ed alle informazioni comportamentali degli utenti con il supporto dell'intelligenza artificiale ed informazioni contestuali sugli incidenti, **Hy.S.AC NIS2GO** consente la difesa di infrastrutture e dati, fornendo strumenti di analisi per il controllo costante e la riduzione del rischio informatico.

1. Analisi del rischio – ENDPOINT SECURITY

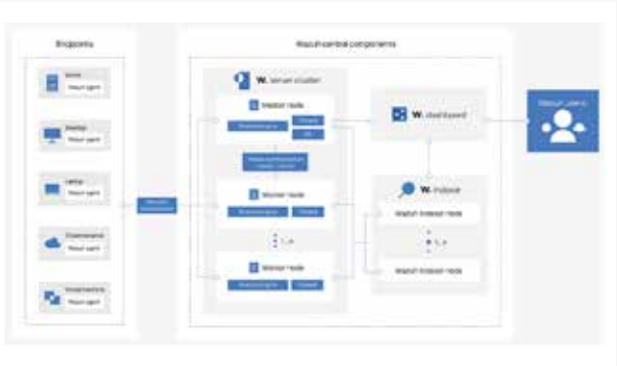
Configuration Assessment - Malware Detection - File Integrity Monitoring

Visualizza, proteggi e gestisci tutti i tuoi beni

Endpoint Security è il primo passo per consentire una maturità informatica per quanto riguarda la gestione degli asset, di cui all'articolo 21.
Al centro di tutti i framework di gestione del rischio c'è l'esigenza di sapere quali asset necessitano di un'analisi del rischio. Conoscere ed avere la visibilità della superficie di attacco dell'Organizzazione è fondamentale affinchè vengano assunte quelle decisioni che per efficacia e priorità siano in grado di mitigarne il rischio fino al suo annullamento, e che le conseguenti capacità di gestione siano sufficientemente adeguate e diligenti per la sicurezza delle informazioni aziendali.

2 Classificare le risorse esposte e rilevare le minacce THREAT INTELLIGENCE

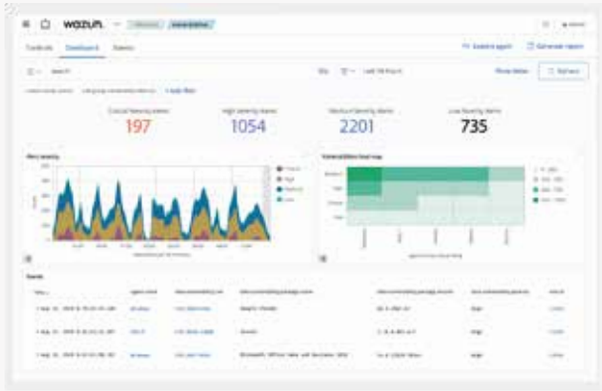
Threat Hunting – Vulnerability Detection – Log Data Analysis



È cruciale sviluppare una profonda comprensione del contesto circostante ogni risorsa all'interno dell'ambiente IT perché aiuta a priorizzare le risorse da proteggere e ad adottare misure di sicurezza proporzionate al rischio, mediante strumenti avanzati per l'analisi dei dati generati dai dispositivi di rete, dagli endpoint e dalle applicazioni.
Wazuh è capace di sfruttare i dati di sicurezza con sufficienti capacità di indicizzazione e interrogazione dei registri, facilitando la ricerca e l'identificazione rapida di potenziali problemi e cause degli incidenti di sicurezza, mappando gli eventi e semplificando le indagini di threat hunting per identificare potenziali minacce e vulnerabilità legate alla mancanza di aggiornamenti sugli endpoint monitorati.
Wazuh assegna una priorità alle vulnerabilità identificate per accelerare il processo decisionale e di ripristino. La capacità di rilevamento delle vulnerabilità di Wazuh garantisce il rispetto dei requisiti di conformità alle normative, riducendo al contempo la superficie di attacco.

3 Evitare costose interruzioni – SECURITY OPERATIONS

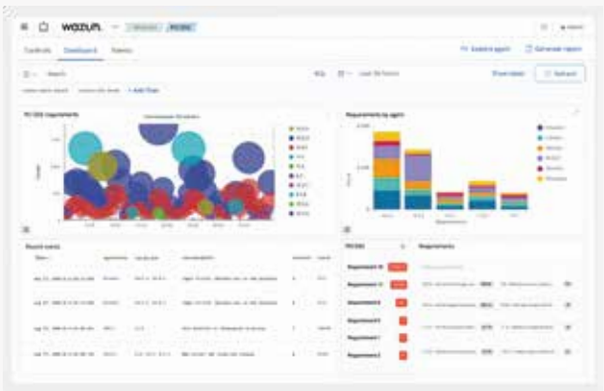
IT hygiene – Posture Management – Cloud Workload Protection – Regulatory Compliance



L'**IT Hygiene** si riferisce alle best practices e misure che aiutano a mantenere la sicurezza, la disponibilità e l'efficienza dell'infrastruttura IT di un'organizzazione; Una cattiva prassi corrisponde alla presenza di utenze, dispositivi, software e configurazioni non più utilizzate, ma ancora presenti nel sistema che possono diventare importanti fattori di accesso e diffusione di attacchi informatici.
Wazuh può aiutare a creare un inventario dei dispositivi in uso, costantemente aggiornato e disponibile, includendo informazioni come sistema operativo, hardware, software installato, configurazioni di rete, porte e processi attivi. In questo modo si può effettuare un monitoraggio attivo della propria infrastruttura, individuando più velocemente anomalie e minacce.

La protezione delle risorse cloud (AWS, Microsoft Azure, Google Platform, Office 365 e altri) è sicuramente uno dei servizi gestiti dalla piattaforma SOC di Wazuh, che permette alle aziende di mantenere la superficie protetta e di assicurare la conformità delle proprie infrastrutture.

4 Semplifica i framework di sicurezza
e la conformità normativa



Wazuh semplifica e supporta l'adempimento degli obblighi di conformità normativa offrendo una soluzione solida che soddisfa i requisiti tecnici degli standard normativi come PCI DSS, HIPAA, GDPR e altri. Sfruttando Wazuh , le organizzazioni ottengono importanti vantaggi chiave, facilitando il processo di conformità mantenendo la focalizzazione sul controllo attivo dell'infrastruttura e degli endpoint, mantenendo attivi gli avvisi qualora non venissero soddisfatti i requisiti di conformità e sicurezza.

5 HySAC iVault MSP
Backup & Disaster Recovery on Cloud

iVault MSP è un Servizio multipiattaforma per il Backup/Restore/Disaster Recovery dei dati, ideato e sviluppato per essere fornito in modalità MSP – Managed Service Provider – , con l'obiettivo di semplificare le attività di salvataggio mediante regole di automazione, ridurre i rischi di usura/perdita dei dati e rientrare nei criteri di una moderna governance aziendale e delle normative sulla sicurezza dei dati che prevedono la delocalizzazione tra gli adempimenti richiesti.

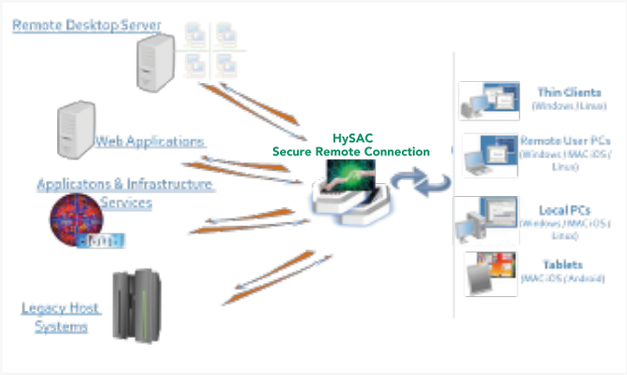
Caratteristiche Tecniche:

- Agent dedicato in ambiente TE5250
- Backup Globale (Object file system, IFS, System)
- Crittografia dei dati *(sessione di lavoro e dati su storage)*
- Compressione dei dati su Storage (8:1)
- Funzionalità incrementale
- Gestione dello storico delle copie
- Consòle centralizzata - in icloud
- Logs reporting
- Conforme al RE 2016/679 (GDPR) per la delocalizzazione delle copie

IVault permette il backup di: MS Windows Server & Workstation- Linux-Unix/AIX.

6 HySAC Secure Remote Connection
connessioni sicure crittografate senza VPN

HySAC Secure Remote Connection è una piattaforma completa per la connessione sicura alle applicazioni aziendali disponibili all'interno della rete privata oppure in cloud, evitando le VPN.
Ogni Utente accede al proprio ambiente di lavoro tramite **HySAC Secure Remote Connection** in modalità crittografata, utilizzando qualsiasi device a disposizione (MS Windows – IOS – Android).



HySAC Secure Remote Connection è pensato per fornire un unico ambiente di lavoro secondo le regole della Cyber Security integrando qualunque infrastruttura esistente (pubblica e privata) con il controllo e la gestione centralizzata delle attività, nonché la registrazione dei log degli accessi.
Il server **HySAC Secure Remote Connection** disponibile per le più importanti distribuzioni di OS Linux, poiché predisposta all'interrogazione degli accessi mediante MFA, è la piattaforma ideale di delivery delle applicazioni aziendali.

7 Multi Factor Authentication (MFA)
la soluzione Trustbuilder

Autenticazione **multifattoriale** universale B2B / B2C. Grazie alla partnership con **TrustBuilder** i vostri utenti possono accedere alle applicazioni in modo sicuro e molto semplice, sia che si trovino in ufficio o in remoto, con o senza connessione, indipendentemente dal dispositivo utilizzato.

È una soluzione "*vendor independent*" ovvero non legata a una tecnologia proprietaria hardware o software e quindi integrabile con qualsiasi applicazione.

Principali caratteristiche: Autenticazione senza password; Deviceless MFA (token browser); Sigillatura delle transazioni, Single sign-on (accesso a diverse applicazioni senza dover rifare l'autenticazione per ogni applicazione).

Certificazione ANSSI: La tecnologia di autenticazione multifattoriale TrustBuilder è certificata dalla National Agency for Information Systems Security.

CYBER SECURITY PACK

CSY Incident Response

È un servizio di "pronto Intervento" disponibile h24/7x7/365 a fronte di incidenti informatici- attacchi da esterno – data breach – Ransomware & CryptoLocker. L'azienda ha a disposizione un tecnico cyber security per identificare la minaccia, bloccarla e ricevere un report di quanto accaduto con indicazioni di remediation.

eMTI - eMail Threat Intelligence

La compromissione ed il conseguente utilizzo di un indirizzo email da parte di terzi (hacker) comporta rischi di attacchi di tipo Phishing per tutti gli utenti aziendali mettendo in serio pericolo la rete aziendale ed esponendola al rischio di Data Breach.

Attività Controllate – Deep web & Dark web: Chat rooms nascoste; Private website; Peer-to-peer Networks; IRC (Internet Relay Chat) channels; Piattaforme Social media e Forum; Black Market; Botnet

DTI – Domain Threat Intelligence

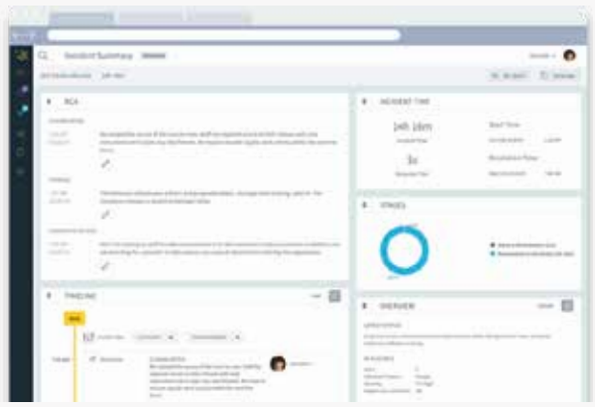
L'attività di "Threat Intelligence gathering" viene effettuata attraverso un processo di ricerca, individuazione e selezione delle informazioni disponibili nel Dark Web e nel Deep Web, relative ad attività illecite legate al dominio aziendale ed alle email compromesse, disponibili in vendita e pronte per essere utilizzate per i tentativi di attacco, mediante le credenziali di accesso. Il servizio non effettua alcun test di sicurezza sul target ed alcuna remediation.

Reporting

Per ogni attività viene consegnata una reportistica dettagliata delle attività in formato PDF.

Incident Response

Organizzare un piano di risposta per un evento di Sicurezza



Correlando i dati provenienti dall'infrastruttura IT, è in grado di avvisare rapidamente i team di sicurezza di comportamenti anomalie che possono segnalare un attacco.

La risposta agli incidenti è l'insieme delle azioni e dei processi che le organizzazioni intraprendono per rispondere alle minacce rilevate nella loro infrastruttura. Aiuta a mitigare l'impatto degli attacchi informatici sulle risorse critiche e sulle operazioni aziendali.

Wazuh aiuta i team di sicurezza a rilevare, analizzare e rispondere rapidamente agli incidenti di sicurezza e attiva automaticamente le azioni appropriate in risposta agli incidenti di sicurezza rilevati. Queste azioni includono l'eliminazione di file dannosi, il blocco delle connessioni di rete sospette, la messa in quarantena degli endpoint compromessi e altro. L'automazione delle azioni di risposta agli incidenti consente di ridurre il tempo medio di risposta (MTTR), riducendo così al minimo il potenziale impatto delle violazioni della sicurezza.

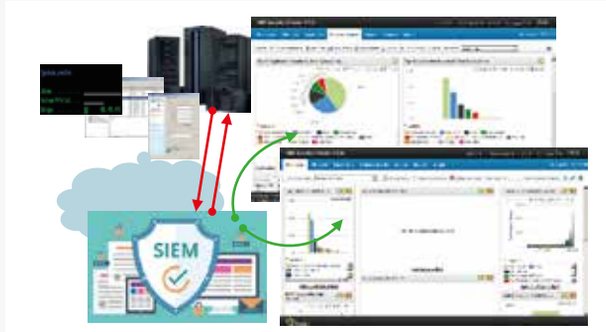
Se abbiamo uno strumento che ci permette di classificare ed analizzare i passi di un attacco svolto nei nostri confronti, allora conosciamo meglio cosa, dove e come siamo stati colpiti. Sappiamo quindi elaborare una risposta migliore, più rapidamente ed efficacemente. I dati di Wazuh permettono di fornire più dettagli alla piattaforma Exigence. Questa offre il pieno controllo degli incidenti critici, affrontando in modo unico ogni aspetto dell'incidente. Trasformando quindi una situazione non strutturata in una strutturata e facile da gestire, è possibile coordinare tutti gli stakeholder e i sistemi in ogni momento, orchestrare i complessi flussi di lavoro dall'innesco alla risoluzione, semplificare l'analisi dei sistemi colpiti e sfruttare le lezioni apprese per migliorare le prossime risposte.
La piattaforma Exigence è capace di affrontare diversi tipi di incidenti, sia per le operazioni tecnologiche, sia per la sicurezza, sia per le esercitazioni e i test di continuità aziendale, sempre con la stessa orchestrazione e l'efficienza del processo.

10

HySAC - DP-iLog 400

Data Providing per il controllo degli accessi ai sistemi IBM/i

La quasi totalità dei sistemi di sicurezza escludono il sistema IBM/i per l'architettura proprietaria della piattaforma ed il sistema operativo che lo caratterizza.



Dp-iLog 400

Arcasafe, mette a disposizione dei Clienti di IBM/i uno strumento software di Data Providing basato su filtri, in grado di leggere i file di log, i journal del sistema e gli eventi relativi alle policy ed alla sicurezza degli accessi degli Utenti – interni ed esterni - al sistema per inviarli al sistema SIEM in formato Syslog, facilitando le attività di controllo della sicurezza dei dati.

Obiettivo della soluzione

La combinazione dell'impiego del modulo Data Providing for IBM/i con i sistemi SIEM pemette di integrare il sistema nei processi di sicurezza già attuati per gli altri sistemi, fornire un supporto pratico alle analisi degli eventi di accesso per individuare schemi sospetti o non autorizzati e quindi mantenere gli asset della Governance e della Compliance.

La gestione del servizio di monitoring e reporting può avvenire anche nei casi di una gestione da parte di un MSP Service Provider o di una struttura SOC – Security Operation Center – esterna al perimetro aziendale

arcasafe
Keeping your Company Safe

ADEGUAMENTO ALLA DIRETTIVA EUROPEA 2022/2555

NIS 2

Allineamento agli Standard Europei per la gestione della Sicurezza in ambito Cyber Security e capacità di Incident Response

SCOPRI DI PIÙ SULLA DIRETTIVA NIS 2
E SUL LIVELLO DI ESPOSIZIONE AI RISCHI DELLA TUA AZIENDA

ENTRA IN CONTATTO CON IL NOSTRO TEAM

+39 0362 14.43.506

info@arcasafe.eu

www.arcasafe.eu

arcasafe s.r.l.
P.IVA 09546870966

Via G. Segantini, 5
20825 Barlassina (MB)

+39 0362 14.43.506
info@arcasafe.eu
www.arcasafe.eu