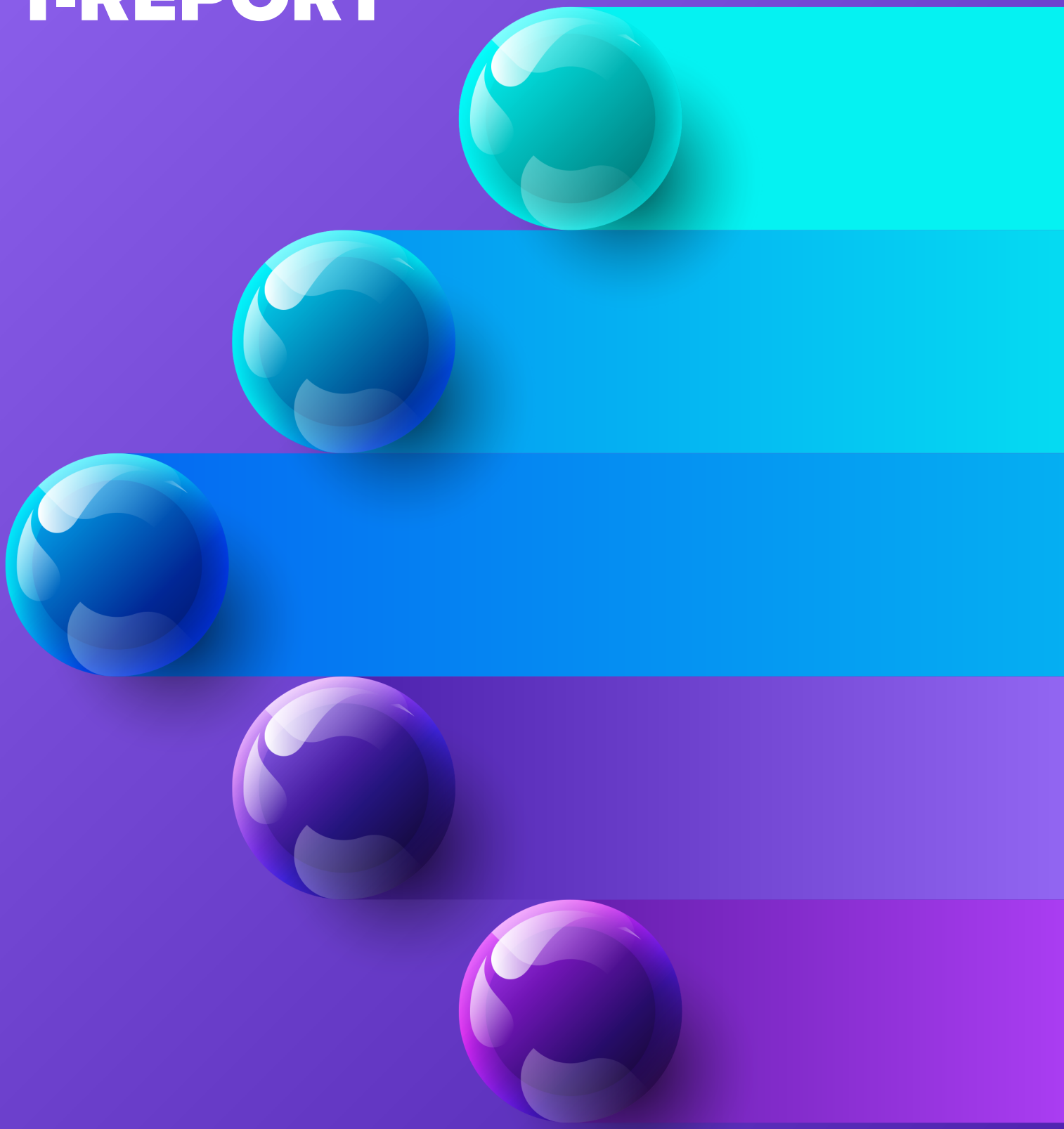
YARIX
a vargroup company

2024 Y-REPORT



Sommario

Sommario

Introduzione

Novità 2023

Lo scopo di questo documento è quello di **tracciare una panoramica accurata e attuale dello scenario delle minacce informatiche** che hanno colpito il nostro paese e altri player internazionali nel corso del 2023, al fine di elaborare un'analisi e una valutazione delle tendenze e delle azioni di mitigazione necessarie a ridurre l'impatto dei cyber attacchi.

Il report, presentato per la prima volta nel 2019 e ormai giunto alla sua settima edizione, **nasce per offrire un'elaborazione dei dati ricevuti e analizzati dal Security Operation Center e dei principali ambiti di competenza della linea di business Digital Security di Var Group**, e fornire una visione complessiva e completa sull'andamento del 2023 in termini di sicurezza informatica.

Una novità rispetto all'anno precedente è rappresentata dall'**introduzione di un'appendice dedicata alla cyber security in ambito Automotive**.

Questa sezione, riservata ai nuovi trend nelle regolamentazioni, rispondenti alla ratio di applicare protocolli sempre più stringenti ed efficaci anche al campo del settore automobilistico, è stata implementata grazie contributo di CYRES Consulting, azienda tedesca di Var Group Digital Security.

Chi siamo: Digital Security Var Group

Digital Security è la business unit di Var Group dedicata all'universo della sicurezza informatica.

Un centro di eccellenza con sedi in Italia e in Europa, impegnato a garantire una difesa avanzata in ogni settore della cybersecurity, offrendo competenze specializzate per affrontare con determinazione e agilità le sfide della sicurezza digitale.

A capo della business unit Digital Security, **Yarix** esprime una leadership riconosciuta nel campo della cyber security, avendo orientato la propria missione allo sviluppo di soluzioni specifiche per imprese ed enti governativi, aziende sanitarie, scuole e università.

È stata la prima azienda privata in Italia ammessa al **FIRST**, la rete di protezione globale che riunisce player come Nasa, Apple e Google con l'obiettivo di contrastare le minacce emergenti.

Parte di Var Group GMBH nella divisione Digital Security dal 2022, **CYRES Consulting** è un pilastro nella consulenza per l'implementazione della cyber security nell'ingegneria e nello sviluppo, in particolare nel settore automotive.

Un team interdisciplinare di esperti, con sede principale a Monaco, in Germania, unito a una rete di partner di cooperazione e consulenti indipendenti, che fornisce servizi di consulenza e formazione all'avanguardia sempre aggiornati alle normative vigenti.

Introduzione

Il metodo

Il report offre uno studio dei dati ricevuti e analizzati da parte di Yarix durante il 2023, considerato come periodo di riferimento. **Le informazioni provengono da un panel specifico di aziende monitorate dal Security Operation Center** e corrispondono alla base clienti di Yarix, che comprende una vasta gamma di settori dell'economia nazionale. Vengono inoltre **inclusi i dati relativi alla gestione di incidenti informatici di aziende** che non erano precedentemente clienti. Le imprese rappresentate nel panel analizzato hanno in media oltre un migliaio di dipendenti e generano fatturati superiori ai 50 milioni di euro.
I dati sono stati normalizzati statisticamente e resi omogenei al fine di poterli utilizzare come output quantitativo affidabile e in grado di supportare valutazioni qualitative. **Tutti i dati raccolti sono stati automaticamente resi anonimi e aggregati per garantire la privacy**, eliminando qualsiasi associazione tra le informazioni e le aziende coinvolte.

Il report è strutturato in quattro sezioni e un'appendice, ognuna dedicata all'analisi e alla valutazione dei dati raccolti ed elaborati da parte del team di riferimento. I dati provengono da un panel rappresentativo dei diversi settori economici italiani ed europei, di cui i seguenti comparti:

- Automotive
- Banking and finance
- Chemical
- Critical Infrastructure
- Energy and Utilities
- Food and beverage
- Gaming
- GDO
- Healthcare
- Information Technology
- Manufacturing
- Naval Industry
- Retail
- Transportation

Il report analizza in modo obiettivo e informato i dati raccolti al fine di evidenziare indicatori di tendenza e anomalie, identificare i principali trend del periodo esaminato e suggerire le relative contromisure per mitigare le problematiche individuate.

Inoltre, viene condotto un approfondimento sugli attacchi informatici che rappresentano un aspetto significativo del panorama attuale nazionale e internazionale della sicurezza informatica.

I team

Il SOC

Il **Security Operation Center** è il team dedicato alla gestione della sicurezza informatica. Il suo compito principale è quello di **monitorare e analizzare costantemente le reti informatiche per individuare e rispondere tempestivamente a minacce di sicurezza e altri eventi che possano compromettere la sicurezza dei dati e delle risorse dell'azienda cliente**.
Il Cognitive Security Operations Center di Yarix (YCSOC) rappresenta uno dei più evoluti in Italia: una cyber control room dotata di misure di sicurezza fisica e biometrica di ultima generazione, basata su forme computazionali predittive e cognitive. **Attivo 24x7x365**, permette alle aziende di proteggere gli asset aziendali strategici, rispondendo efficacemente alla rapida evoluzione dei rischi informatici.
Nel 2023, **l'efficacia del SOC di Yarix è stata potenziata dall'implementazione di Egyda, la piattaforma sviluppata internamente che, grazie all'utilizzo di Intelligenza Artificiale e Machine Learning**, supporta l'analista nella fase di raccolta e categorizzazione delle informazioni, rendendo più rapido ed efficiente il processo di risposta alle minacce.

YIR - Incident Response

Il team di **Incident Response** di Yarix (YIR) affronta e risolve tutti gli aspetti legati alle **violazioni informatiche**, a partire **dall'indagine fino alla gestione delle crisi**, fornendo una risposta efficace agli incidenti di sicurezza. I nostri esperti gestiscono le **azioni di contenimento**, analizzando e utilizzando le informazioni disponibili per determinare l'ambito e la gravità delle minacce, al fine di avviare le azioni necessarie a interromperle e neutralizzarle. **Dal momento dell'ingaggio, il team YIR supporta gli operatori di sicurezza che presidiano l'infrastruttura sotto attacco**, fornendo consulenza in ogni fase del processo di risposta: rilevamento, contenimento, eradicazione e gestione della crisi.

YCTI - Cyber Threat Intelligence

Il **Cyber Threat Intelligence Team** di Yarix (YCTI) è composto da analisti specializzati che, grazie a particolari skill ed esperienza maturati nel settore della cyber security, **interpretano le informazioni disponibili in rete** (Clear, Dark e Deep Web) **per prevenire e contrastare minacce quali cybercrime, hacktivism, operazioni pianificate per la sottrazione di dati o il blocco dell'operatività aziendale**. Questi esperti sono in grado di muoversi nel dark web con profili sotto copertura, infiltrandosi in black market e forum dove vengono scambiati e distribuiti malware, exploit e altri strumenti di attacco così da interagire direttamente con i Threat Actor.

YRT - Red Team

Il **Red Team** di Yarix (YRT) è una squadra di professionisti certificati, dotati di competenze elevate e pluriennale esperienza, in grado **di mettere realmente alla prova il livello di sicurezza di un'azienda**. Adottando la mentalità e le modalità operative messe in atto dagli attaccanti, mediante l'impiego di strumenti e tecniche avanzate e l'applicazione di metodologie internazionalmente riconosciute, riesce a misurare il livello di rischio reale a cui è soggetta un'organizzazione di fronte ad un attacco informatico simulato, **consentendo di identificare i punti deboli e mettere a punto un piano di remediation adeguato.**

CYRES Consulting

Parte di Var Group GMBH, nella linea di business Digital Security, **CYRES Consulting è composta da un team interdisciplinare di esperti**, supportato da una rete di partner e consulenti indipendenti, **la cui missione è di assistere i clienti nell'integrazione strategica e nell'attuazione operativa della cyber security nel settore automobilistico, sia a livello organizzativo che di progetto**. Oltre alla consulenza personalizzata, CYRES può contare sulla sua **Academy**, che offre una vasta gamma di programmi formativi sulla sicurezza informatica, **affermatasi come il più grande database di apprendimento al mondo nel settore della sicurezza informatica applicata all'industria automobilistica**, grazie ai suoi corsi di formazione, video on-demand e certificazioni.

Sezione 1

SECURITY OPERATION CENTER

Security Operation Center

311 mila eventi di sicurezza

I dati analizzati in questo report sono relativi ai circa **311 mila eventi di sicurezza** (**+78%** rispetto all'anno precedente) **rilevati dai sistemi di monitoraggio** messi in opera dal Security Operation Center (YSOC) di Yarix, parte della business unit Digital Security di Var Group.

Gli analisti hanno esaminato questa base di dati, **integrandola e correlandola con ulteriori informazioni di Threat Intelligence** derivanti da fonti interne e da collaborazioni con istituzioni, enti e altre aziende. Non da ultimo, questo documento **tiene conto delle notizie provenienti dal circuito FIRST** (Forum for Incident Response and Security Teams), la comunità internazionale più estesa e autorevole per la prevenzione e la gestione congiunta di incidenti di sicurezza.

Definizioni

Quella tra evento e incidente di sicurezza è una differenza sottile che può talvolta generare confusione e fraintendimenti circa i dati in analisi. Per completezza riportiamo di seguito le definizioni utilizzate per i due termini, che saranno valide per tutto il report.

// Evento di sicurezza

Un evento di sicurezza informatica è **un'occorrenza identificata dello stato di un sistema**, di un servizio o di una rete informatica, **che indica una possibile violazione dei livelli di sicurezza definiti**, oppure una situazione sconosciuta che può essere rilevante per la sicurezza del patrimonio informativo e degli asset aziendali.

// Incidente di sicurezza

Evento, o una catena di eventi, conseguente a un'azione, intenzionale o accidentale, svolta nell'ambito del Sistema Informatico controllato, **che può causare la perdita di riservatezza, integrità o disponibilità dei dati aziendali e dei servizi** erogati dagli asset informatici protetti, nonché l'utilizzo di asset **al fine di commettere illeciti o arrecare danni verso terzi**, in violazione a disposizioni aziendali o legislative.

A titolo esemplificativo e non esaustivo, gli eventi di sicurezza analizzati consistono in:

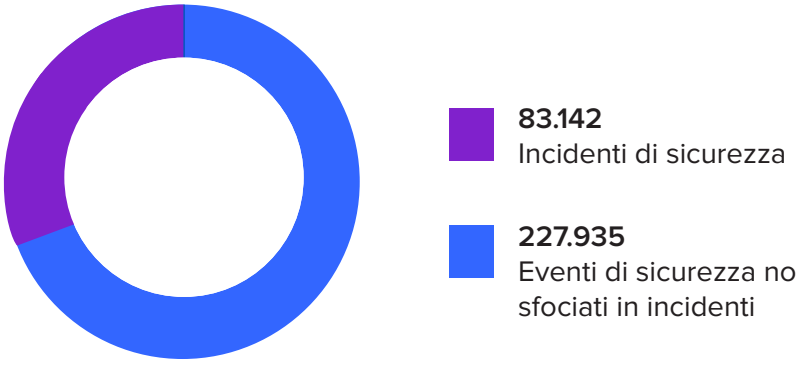
- eventi riconducibili a codici malevoli/malware;
- sfruttamento di vulnerabilità note;
- presenza di sistemi collegati a Botnet;
- esfiltrazione di dati;
- intrusioni;
- compromissione di sistemi e/o applicazione e/o servizi;
- attacchi DoS/DDoS;
- modifica o cancellazione non autorizzata di dati;
- invio di mail di phishing;
- comunicazione con IP, domini, URL riconducibili ad attività malevole.

Gli eventi analizzati in totale sono 311.077, di cui 83.142 si sono evoluti in incidenti di sicurezza, di diversa criticità (fig. 1).

Security Operation Center

Eventi totali analizzati

Figura 1

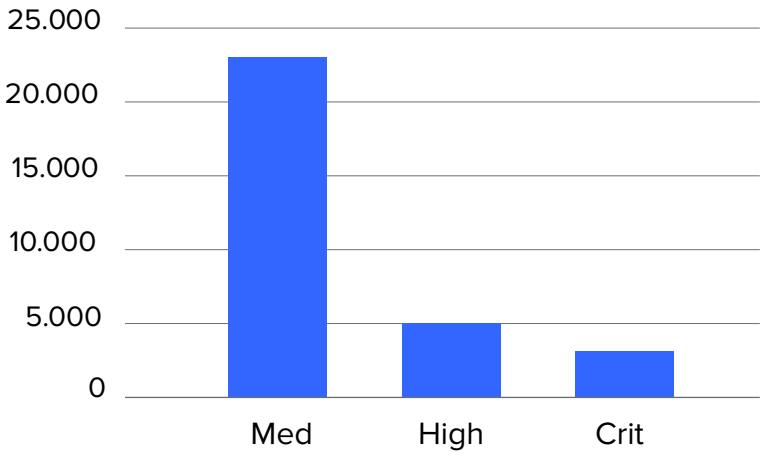


La criticità degli eventi e degli incidenti viene calcolata sulla base delle indicazioni contenute nel manuale operativo dei singoli clienti del servizio, definita secondo le metriche e le procedure concordate, basate su standard nazionali e internazionali.

Questa classificazione permette di **allineare le tipologie e le criticità degli incidenti rilevati** per i singoli clienti nella seguente infografica (fig. 2)

Eventi suddivisi per gravità

Figura 2



Per gli **eventi di gravità "critica"** (fig. 2) è stato riconosciuto il passaggio a incidente di sicurezza e in questi casi **alle attività di analisi sono seguite anche attività di Emergency Response compiute dal team YIR (Incident Response) di Yarix**.

Il team ha supportato il cliente nella gestione dell'incidente, nella risoluzione e nella successiva analisi post-incidente, al fine di rilevare l'origine della compromissione o dell'attacco, i possibili danni collaterali e attività persistenti messe in campo dall'attaccante.

Security Operation Center

Le attività di Emergency Response consistono nel fornire supporto al cliente durante la gestione dell'incidente di sicurezza. L'obiettivo è identificare, analizzare e classificare gli eventi di sicurezza secondo priorità, nonché definire le procedure da adottare in risposta alla conferma di avvenuto incident, fino al ripristino della normale operatività. Questo processo assicura la possibilità di effettuare un'analisi forense dettagliata in un secondo momento. Inoltre garantisce **un miglioramento dei controlli, grazie alla lesson learned**, prevenendo o limitando le conseguenze in caso si verificasse nuovamente lo stesso tipo di incidente.
In particolare, a fronte di una segnalazione di incidente informatico, vengono eseguite una serie di azioni:

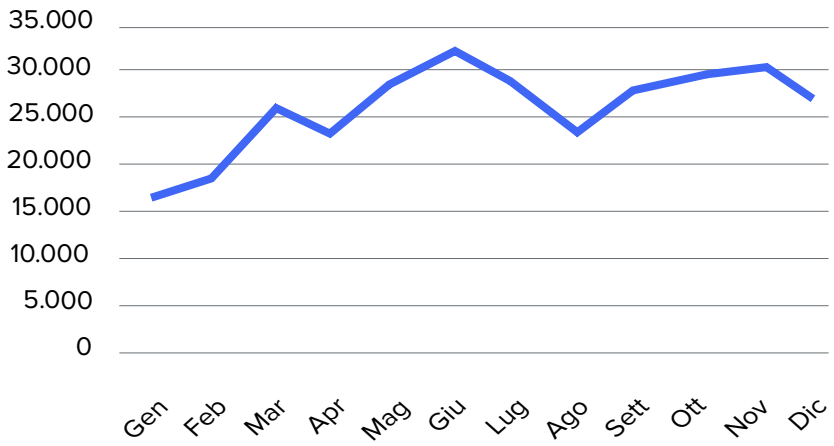
Assistere i soggetti coinvolti nella gestione degli incidenti di sicurezza;

- **Rispondere alle segnalazioni di incidenti**, avvertendo i soggetti coinvolti e seguendone gli sviluppi;
- **Diffondere informazioni sulle vulnerabilità** più comuni e sugli strumenti di sicurezza da adottare;
- **Assistere i soggetti coinvolti** nella realizzazione di misure preventive ritenute necessarie per la riduzione a livelli accettabili del rischio di incidenti;
- **Emanare direttive sui requisiti minimi di sicurezza** per le macchine con accesso alla rete, verificandone il rispetto;
- **Gestire corsi di aggiornamento tecnico**, a tutti i livelli, e in particolare per gli utenti finali;
- **Mantenere aggiornati allo stato dell'arte gli strumenti e le metodologie** per la sicurezza;
- **Testare metodologie e strumenti esistenti**, oltre che svilupparne di nuovi per esigenze specifiche.

Nel corso del 2023, si è registrato un notevole aumento del numero totale di eventi analizzati e gestiti, quasi raddoppiando (**+87%**) la quantità di eventi riscontrati mensilmente rispetto al 2022. (fig.3)

Distribuzione eventi 2023

Figura 3

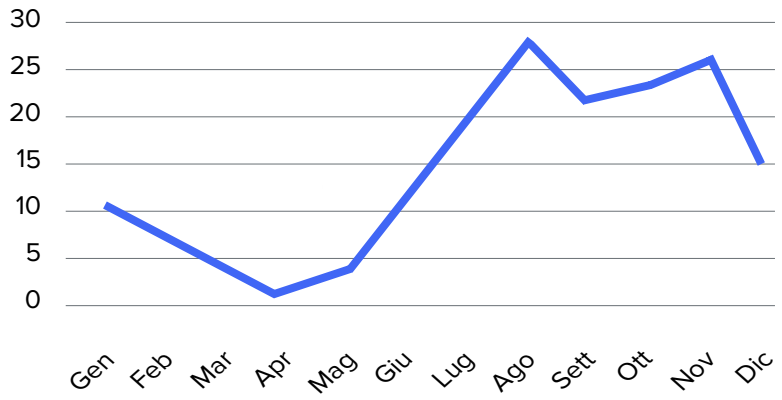


Security Operation Center

Si è registrato un incremento significativo (+**300%**) anche per quanto riguarda gli **eventi di gravità critica**. Ciò è conseguenza delle numerose vulnerabilità critiche emerse in applicativi di largo consumo e dello sviluppo di nuovi scenari di monitoraggio, che hanno portato a una maggiore efficacia nell'identificazione delle minacce da parte del team SOC (fig. 4).

Distribuzione eventi critici 2023

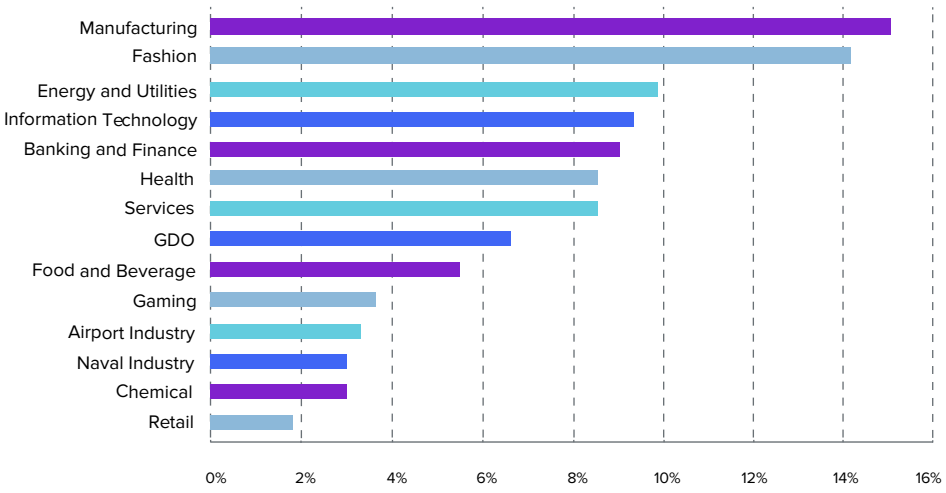
Figura 4



In seguito, l'analisi si è concentrata sulla tipologia di settore industriale impattato.
Tale categorizzazione è fortemente condizionata dal campione preso in esame che, come anticipato, è composto da clienti che usufruiscono del servizio SOC di Yarix. Per questo motivo sono state fatte delle considerazioni di tipo statistico mirate a minimizzare l'impatto di eventuali settori con una presenza più numerosa o di aziende di dimensioni più significative rispetto alle altre. (fig. 5).

Eventi di sicurezza per settore industriale 2023

Figura 5



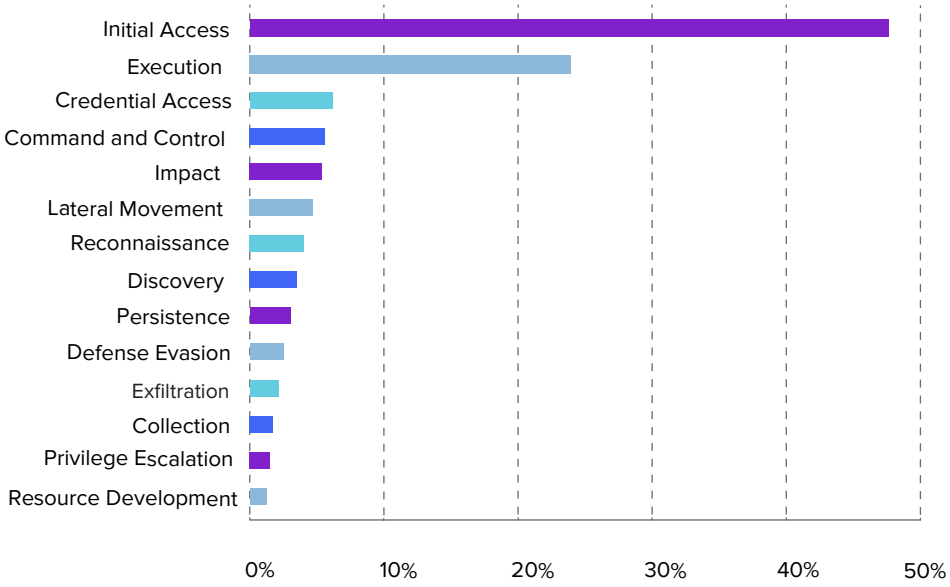
Security Operation Center

Si evidenzia che i due settori per i quali **è stato registrato un numero maggiore di attacchi**, con un'incidenza superiore al 10%, sono quello del **Manufacturing e del Fashion, rispettivamente 15% e 14%**. Questo trend è dovuto a fattori diversi: se per il Manufacturing vi è una situazione legata alla presenza di ambienti produttivi in cui con più frequenza possono essere presenti dispositivi fuori supporto, stante la difficoltà ad intervenire sugli stessi, per il fashion la determinante principale è collegata all'elevata esposizione degli shop online e alla presenza globale, con sedi estere sulle quali le policy possono essere meno restrittive e di conseguenza possono essere soggette ad un più elevato volume di eventi di sicurezza.

Dall'analisi degli eventi di sicurezza è poi stata eseguita una categorizzazione degli stessi secondo le tattiche identificate dal Mitre ATT&CK. (fig. 6)

Tattiche Enterprise Mitre ATT&CK 2023

Figura 6



Il grafico mostra come **la famiglia principale sia legata alle fasi iniziali dell'attacco (accesso iniziale)**. Questo discende direttamente dal fatto che i dati provengono da clienti con un servizio SOC attivo, che ha permesso di identificare e bloccare tali attività prima di raggiungere fasi più critiche dell'attacco.

Security Operation Center

Egyda

Nel corso dell'ultimo anno abbiamo sviluppato il progetto **"Egyda"**, che ha visto protagonisti **l'utilizzo dell'automazione in diverse fasi** (hyper-automation), **del machine learning** (ML) **e dell'intelligenza artificiale** (AI) all'interno del Security Operation Center, migliorando sostanzialmente i nostri meccanismi di difesa contro le minacce informatiche.

Questa iniziativa sottolinea il nostro impegno nell'**utilizzare tecnologie all'avanguardia per migliorare la sicurezza e l'efficienza delle nostre operazioni**.

L'**hyper-automation è stato uno dei pilastri di questo progetto**, grazie al quale abbiamo implementato un'estensiva automazione dei processi di raccolta e analisi dei dati, procedimento che in precedenza veniva eseguito manualmente dai nostri analisti SOC. Questo cambiamento ottimizza non solo il rilevamento e la gestione degli incidenti di sicurezza, ma **libera anche i nostri analisti dai task ripetitivi permettendo loro di concentrarsi sugli scenari più complessi**.

Ad esempio, il nostro sistema ora aggrega e correla automaticamente i dati da fonti diverse, applicando algoritmi avanzati per rilevare schemi e anomalie in tempo reale. Questa capacità è fondamentale per gestire efficacemente l'enorme volume di dati elaborato dal SOC.

Il nostro strumento di machine learning, YUBA, esemplifica il nostro approccio proattivo alla cybersecurity. YUBA è specificamente progettato per analizzare i modelli di autenticazione degli utenti verso i vari servizi cloud, identificando deviazioni dal comportamento usuale che possono significare una violazione della sicurezza. Imparando continuamente da dati storici e in tempo reale, il motore di YUBA diventa sempre più abile nel prevedere e rilevare accessi non autorizzati o potenziali compromissioni.

Questo sistema opera su un principio di apprendimento non supervisionato, dove forma cluster di comportamenti di login tipici e segnala come sospetta qualsiasi attività che si discosti da questi modelli. Questo innovativo strumento, congiuntamente all'applicazione di feed d'intelligence specifici, **non solo ha migliorato i nostri tassi di rilevamento delle minacce, ma riduce l'incidenza di falsi positivi migliorando così l'efficienza operativa**.

L'intelligenza artificiale in Egyda è stata focalizzata sul supporto ai nostri analisti nella prioritizzazione e gestione delle minacce rilevate. **Abbiamo sviluppato un framework decisionale guidato dall'AI che valuta la gravità e il potenziale impatto di ogni minaccia**.

Questo sistema **utilizza dei modelli supervisionati addestrati sui dati passati, che forniscono un punteggio numerico indicante la probabilità che una minaccia sia da sollevare all'attenzione dell'analista**.
Questo punteggio aiuta gli analisti a dare priorità agli eventi urgenti, concentrandosi sulle questioni più critiche, per garantire una risposta rapida ed efficace.

Egyda

Inoltre, l'**AI migliora le capacità di risposta agli incidenti suggerendo i passi ottimali di rimedio e automatizzando i processi decisionali di routine, accelerando così la risposta generale alla sicurezza**.

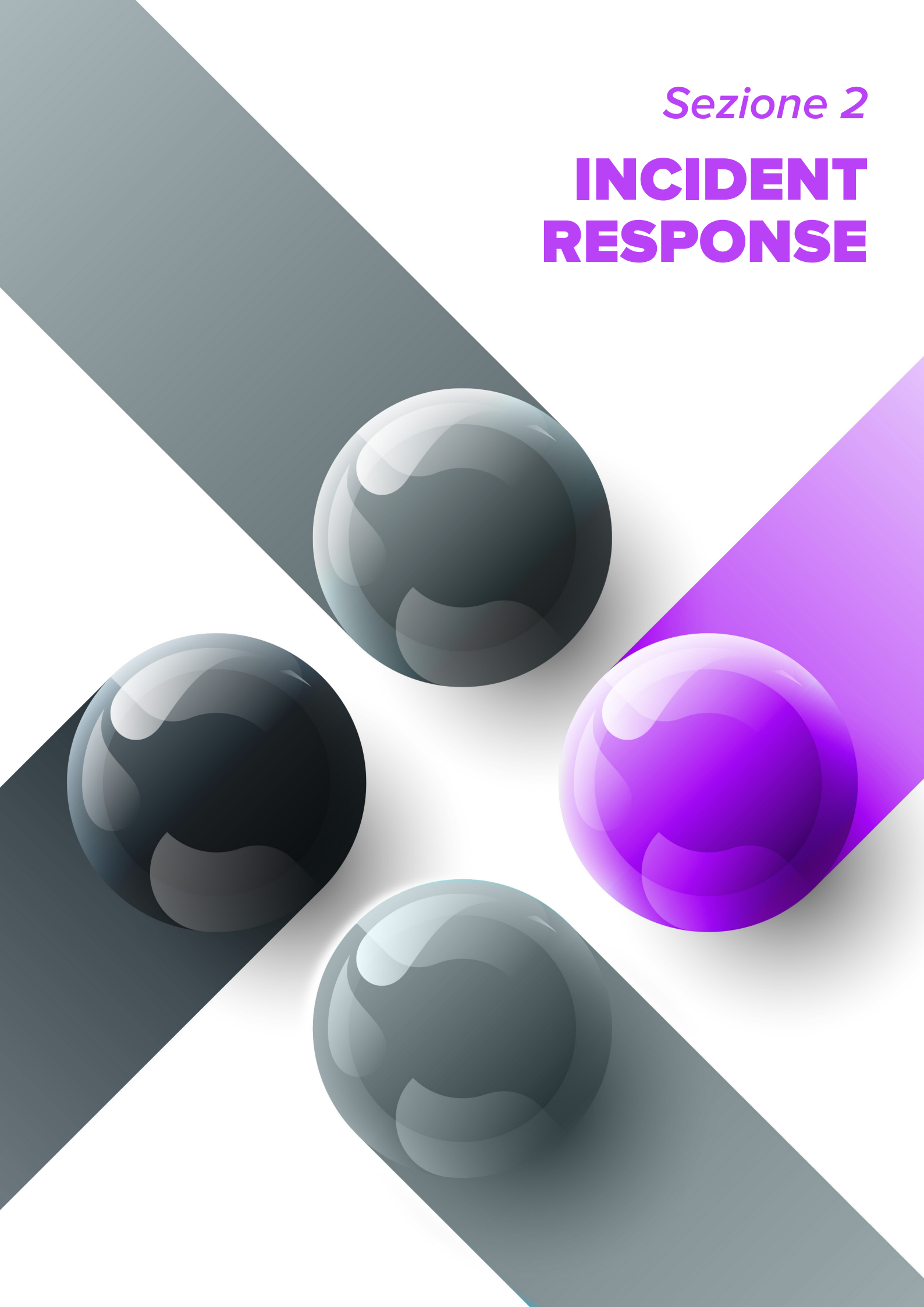
In conclusione, il progetto Egyda ha trasformato il nostro approccio alla cybersecurity nel contesto del SOC, integrando hyper-automation, machine learning e intelligenza artificiale per creare un ambiente di sicurezza più robusto, efficiente e proattivo.

Questi progressi ci hanno spinto in prima linea nell'innovazione tecnologica in materia di cybersecurity, **pronti a fronteggiare le sfide di un panorama di minacce digitali sempre più complesso**. Le nostre soluzioni non solo rilevano, ma prevedono e prevengono le violazioni di sicurezza prima che possano impattare sull'operatività.

Le prospettive future riguardano l'adozione di strumenti di intelligenza artificiale ancora più sofisticati quali l'introduzione, in alcune fasi, degli LLM (Large Language Model) che permetteranno una flessibilità ancora maggiore nell'amministrazione della mole di dati gestita dal SOC.

Sezione 2

INCIDENT RESPONSE



Incident Response

83 major incident

In questa sezione è riportata **un'analisi dei dati relativi agli incidenti di sicurezza gestiti dal team di Incident Response di Yarix** (YIR).

Nel 2023, il team YIR ha operato nella risposta e risoluzione di 83 major incident (**+18%** rispetto al 2022), molti dei quali, in linea con gli anni precedenti, hanno richiesto capacità tecniche molto elevate. In molti di questi casi la risoluzione ha coinvolto elementi tecnici non documentati e l'elaborazione di metodologie personalizzate.

Questa tendenza è in linea con l'incremento esponenziale delle skill relative alle Tecniche, Tattiche e Procedure (TTP) che i Threat Actor (TA) stanno introducendo per l'inserimento di persistenze, movimenti laterali ed exploiting di vulnerabilità.

Le attività del team di Incident Response (YIR) prevedono diverse fasi per la gestione di un incidente di sicurezza che coinvolge realtà parzialmente o totalmente compromesse da un attacco informatico, in cui sono a rischio le informazioni riservate e confidenziali della struttura IT, la loro integrità o la loro disponibilità.

Attività di Emergency Response

La gestione di eventi di questo tipo richiede un approccio organizzato e strutturato. Questo si traduce nell'adozione di **una metodologia di Incident Handling ricavata dalle best-practice internazionali e consolidata con l'esperienza pregressa** nell'ambito specifico. In particolare, le attività di Emergency Response consistono in:

- **raccolta di informazioni precise**, utilizzando tecniche di comunicazione che consentono di comprendere l'attuale stato percepito dal cliente al momento dell'ingaggio;
- **assessment dell'impatto dell'incidente sulle risorse IT**, classificando gli asset impattati per importanza di servizio e criticità di business;
- **identificazione, raccolta e analisi secondo priorità degli artefatti** ed eventi di sicurezza riconducibili all'attacco, al fine di delineare come si è svolto l'attacco e identificare gli indicatori di compromissione (IOCs);
- **contenimento dell'attacco** e messa in sicurezza del perimetro, mediante analisi e bonifica dei sistemi con rimozione di tutti gli elementi malevoli identificati all'interno dell'infrastruttura;
- **supporto al ripristino** della normale operatività di business;
- **implementazione di lesson learned** per limitare le conseguenze in caso del ripetersi dello stesso evento.

Per gestire correttamente l'incidente, **l'analisi di log** e altri artefatti presenti nei sistemi all'interno dell'infrastruttura attaccata rimane **cruciale per ricostruire le attività malevole** e identificare il punto d'ingresso sfruttato dal TA. Questo compito è diventato più complesso a causa delle sempre più frequenti **attività di eliminazione delle tracce operate dal TA** che spesso rendono indisponibili la maggior parte degli elementi necessari per le analisi.

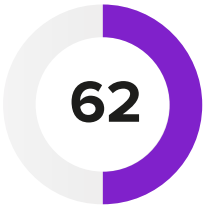
Incident Response

Per fornire una maggiore velocità ed efficienza nelle fasi di containment ed eradication, il team di Incident Response ha sviluppato già dall'anno precedente un ampio set di automazioni utili alla rimozione delle minacce più persistenti e alla messa in sicurezza dei dispositivi utilizzati per le attività di lateral movement e privilege escalation.

Quest'anno, l'evoluzione più significativa è stata osservata nel campo della ricostruzione dell'attacco, processo altamente automatizzato in modo da fornire rapidamente i dati fondamentali agli Incident Response Leader, che si trovano a dover prendere decisioni importanti per il business compromesso.

Overview dati YIR 2023

Nel corso del 2023 **il Team YIR ha gestito complessivamente 83 casi**, di cui:



Incidenti con gravità "alta" o "critica" (IR)

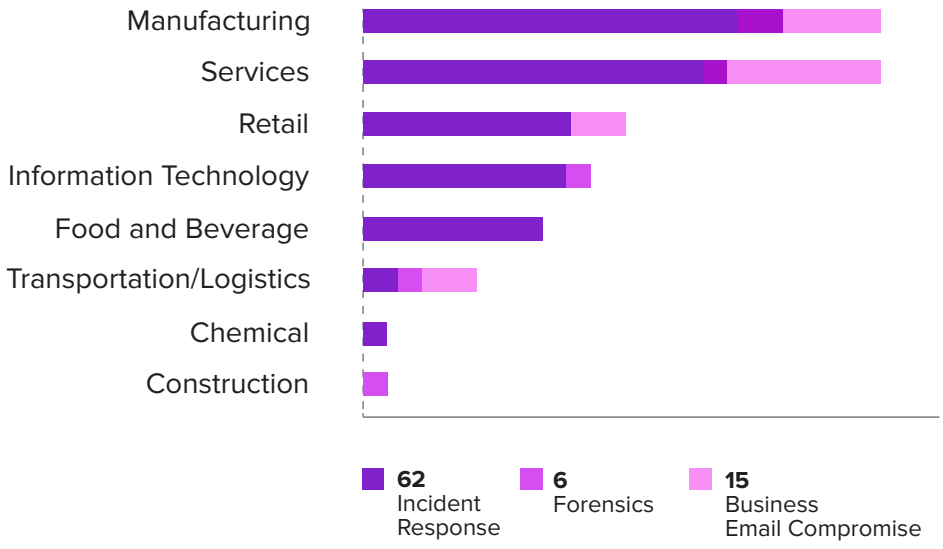
Indagini forensi (FOR)

Business E-mail Compromise (BEC)

L'analisi si è poi concentrata sulla tipologia di **settore industriale** impattato:

Analisi per settore industriale

Figura 7



I settori più colpiti risultano essere quelli del **Manufacturing (24 casi - 28,92%), Services (22 casi - 26,5%) e Retail (11 casi - 13,25%)**.

Incident Response

Vettori di ingresso

Sulla base di quanto emerso dalle analisi degli incidenti, **i vettori di ingresso che hanno permesso la compromissione dei sistemi** si suddividono in:

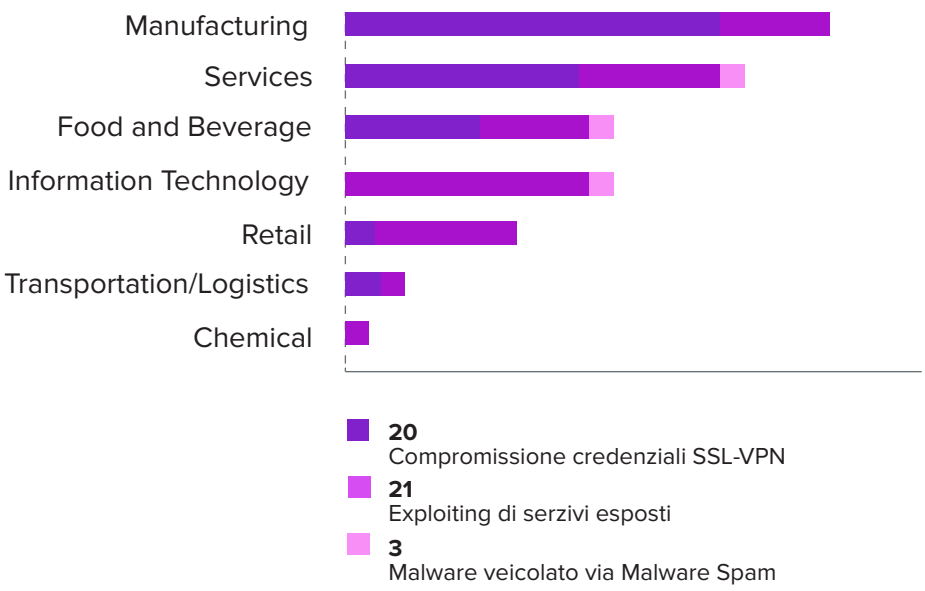
- Compromissione credenziali SSL-VPN
- Exploiting di servizi esposti
- Malware veicolato via Malware Spam (Campagne Mail)

Analizzando i precedenti punti si rileva quanto segue:

- i servizi SSL-VPN maggiormente sfruttati risultano essere quelli sprovvisti di una autenticazione multi-fattore;
- altre vulnerabilità sfruttate dagli attaccanti sono relative a pubblicazione di servizi come interfacce amministrative dei firewall, Citrix, RDP, Exchange e servizi personalizzati e basati su tecnologie opensource;
- tra i servizi più utilizzati per ottenere accesso remoto all'infrastruttura risulta la posta elettronica; nello specifico sono stati analizzati diversi attacchi che, come punto d'ingresso, fanno leva sul fattore umano.

Vettori di ingresso per settore industriale

Figura 8



TTPs e Threat Actor

Per gli incidenti non riportati nella tabella precedente, non è stato possibile identificare con certezza il punto d'ingresso. Pertanto, anche se il team di Incident Response è riuscito comunque a identificare la dinamica dell'incidente, il dato non è stato riportato a statistica.

Incident Response

Threat Actor 2023

Tramite l'**analisi delle Tattiche, Tecniche, e Procedure** (TTPs) è stato possibile **profilare i vari Threat Actor** (TA) **che hanno agito sulle infrastrutture delle aziende colpite**.

In particolare, la parte di analisi delle "tattiche" ha permesso di delineare il modo in cui un TA sceglie di effettuare il suo attacco dall'inizio alla fine. L'**approccio tecnologico** per ottenere risultati intermedi durante l'attività malevola **è descritto dalle "tecniche"** che l'attaccante usa. Infine, **l'approccio organizzativo dell'attacco è definito dalle "procedure"** utilizzate dall'attore della minaccia.

Nell'immagine seguente vengono riportati i Threat Actor identificati durante le analisi, classificati in base al numero di attacchi effettuati.

Threat Actor

Akira Hive Ransom House
Noescape **Find0m** Phobos
BlackBasta Prometei Botnet
Alfa team **Lockbit 3.0** **Babuk**
DeepBlueMagic BlueSky
Rhysida **Play** Royal
Vice City

Totale identificazioni	**27**
Sconosciuti	**35**

Incident Response

Evoluzione degli attaccanti

Dall'analisi si nota che, come l'anno precedente, **LockBit resta in vetta alle classifiche riguardanti i TA più attivi ed efficaci**. Infatti, nonostante il recente intervento delle forze dell'ordine all'infrastruttura Lockbit, soprannominato "Operazione Cronos" [1] , il Threat Actor sembra aver colto l'occasione per una riorganizzazione interna di asset e affiliati, per poi, risorgere ancora più forte.
Negli attacchi osservati dal team Incident Response, **LockBit ha mostrato capacità elevatissime nel campo delle tecniche utilizzate per la gestione del lateral movement ed esfiltrazione, adottando diversi set di strumenti personalizzati per velocizzare i propri affiliati nelle attività di compromissione**.

A differenza dell'anno precedente, l'attività di cifratura eseguita dai Threat Actor più attivi risulta essere abbastanza diversificata nello stile. Sono infatti stati rilevati attacchi che adottano **la cifratura dei file VMDK presenti negli host fisici**, con una frequenza simile a quelli che prevedono la cifratura dei file presenti nei filesystem.

Questo tipo di comportamento mostra che la gang sta rendendo disponibili ai propri affiliati payload funzionali ed efficaci, da utilizzare in qualsiasi caso di compromissione.

In linea con l'anno precedente, gli strumenti principalmente utilizzati rimangono i più celebri, come Mimikatz, Cobalt Strike, Lazagne, ecc., unitamente a strumenti personalizzati verosimilmente sviluppati dai singoli affiliati al fine di semplificare le attività di compromissione.

A differenza dei periodi precedenti, **il team di Incident Response rileva che lo skill set utilizzato dagli affiliati dei major Threat Actor, come Lockbit, Play, BlackBasta e Akira, risulta molto vario**. Questo indica un minor grado di selezione nel processo di affiliazione, in modo da aumentare sensibilmente il numero di attacchi e, di conseguenza, dei pagamenti delle richieste di riscatto.

[1] https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

Sezione 3

CYBER THREAT INTELLIGENCE

Cyber Threat Intelligence

Overview dati YCTI 2023

In linea con quanto riportato dai team di Security Operation Center (YSOC) e Incident Response (YIR), viene ora proposto il punto di vista del reparto **Cyber Threat Intelligence (YCTI) di Yarix** e delle proprie analisi mirate relative all'anno 2023.

Nel 2023, il team YCTI ha riportato un totale di **2.571 eventi significativi**, di cui:

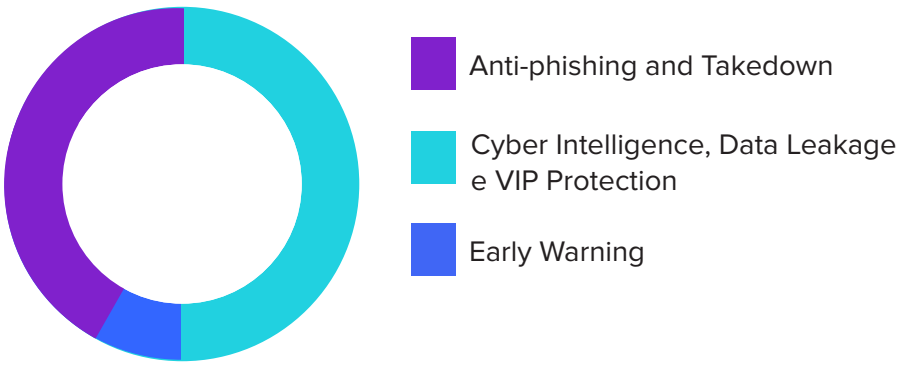
- 1.093 eventi di Cyber Intelligence, Data Leakage e VIP Protection;
- 189 eventi di Early Warning;
- 1.289 eventi di Anti-Phishing e conseguenti attività di contrasto.

A titolo esemplificativo e non esaustivo, gli eventi CTI analizzati consistono in:

- eventi riconducibili a **vendita di credenziali o accessi compromessi** su Deep Web e Dark Web;
- eventi su **vulnerabilità critiche e vulnerabilità 0-day** attivamente sfruttate dai TA (Threat Actor);
- eventi riconducibili a **data breach, data leak o vendita di informazioni e dati confidenziali** su Deep Web e Dark Web;
- **eventi di impatto importante o critico** emersi a seguito di attività OSINT / HUMINT;
- **eventi riconducibili a individuazione e contrasto di domini o siti web fraudolenti** (fake shops, phishing bancario, mobile apps fraudolente, spear-phishing...).

Overview dati YCTI 2023

Figura 9



Cyber Threat Intelligence

Per ogni evento Cyber Threat Intelligence, il team ha fornito un **report di segnalazione specifico, supportando il cliente nella gestione dell'incidente**, fornendo le evidenze raccolte **e suggerendo le corrette contromisure** e le azioni di mitigazione e remediation suggerite.

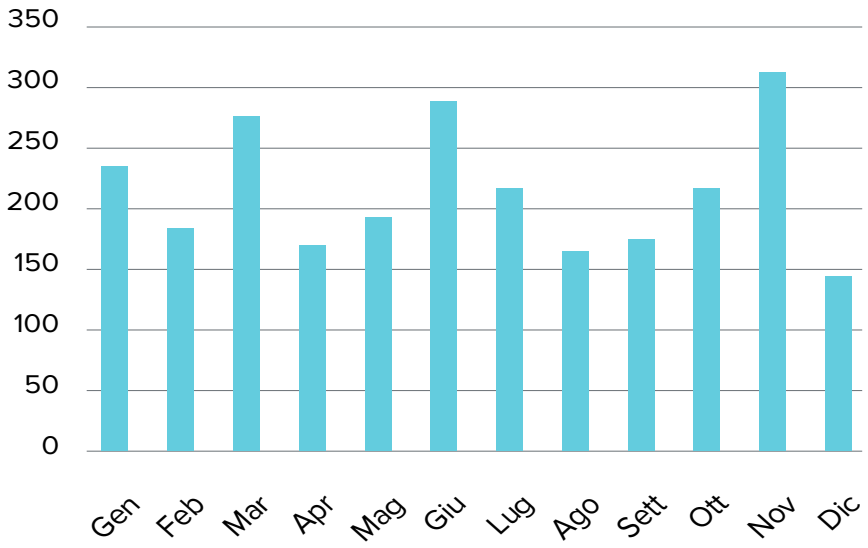
79 eventi con severità critica

Durante il periodo di riferimento, gli analisti del team YCTI hanno identificato **79 eventi con severità critica**. Questo ha permesso di evitare proattivamente incidenti che avrebbero potuto compromettere l'intera organizzazione vittima di potenziali attacchi ransomware o di esfiltrazione di informazioni critiche.

Nel grafico si mostra la **distribuzione temporale degli eventi significativi (2.571) gestiti dal team YCTI**.

Distribuzione temporale

Figura 10



Trend Ransomware

In riferimento agli **incidenti ransomware a livello globale**, il team YCTI ha mappato e **analizzato durante il 2023 un totale di 4.474 eventi condotti da 65 gruppi ransomware**. Di seguito viene riportata la lista relativa alla Top 10 dei gruppi ransomware più attivi:

- LockBit (22%)
- AlphV/BlackCat (9%)
- Cl0p (9%)
- Play (7%)
- 8base (5%)
- Malas (4%)
- Akira (4%)
- Bian Lian (3%)
- Medusa (3%)
- BlackBasta (3%)

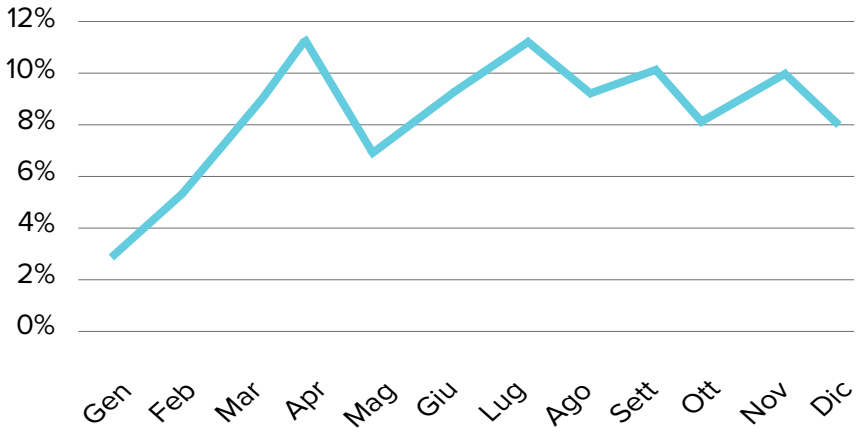
Cyber Threat Intelligence

LockBit si conferma il gruppo ransomware più attivo durante il 2023, contribuendo da solo al 22% degli attacchi totali, seguito da AlphV/ BlackCat e Cl0p (9%), Play (7%), 8base (5%), Malas e Akira (4%), Bian Lian, Medusa e BlackBasta (3%). **Queste 10 gang ransomware hanno contribuito al 68% degli attacchi totali registrati dal Team YCTI**.

Di questa lista Top 10, fanno parte anche 8base, Akira, Malas e Medusa, quattro gruppi ransomware apparsi nell'ultimo anno. Insieme, queste quattro gang criminali hanno contribuito al 16% degli attacchi totali monitorati durante il 2023.

Andamento mensile Ransomware 2023

Figura 11



Guardando all'andamento mensile degli eventi, si può notare una **tendenza crescente della minaccia ransomware durante il primo quadrimestre del 2023**, per poi assestarsi e registrare alcuni picchi durante i mesi di aprile, luglio, settembre e novembre.

Le statistiche riguardanti i paesi bersaglio delle gang ransomware sono altrettanto significative. **L'Italia si posiziona al quinto posto nella lista dei cinque paesi più bersagliati**.

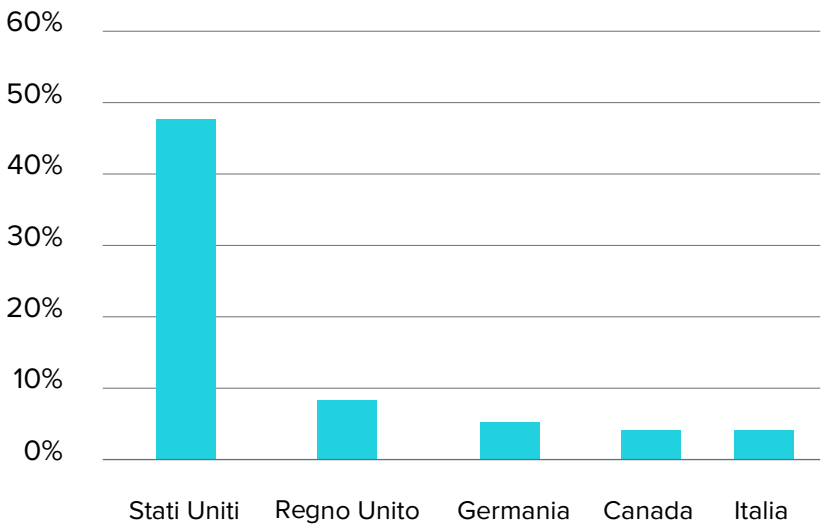
Di seguito la **Top 5** dei paesi le cui organizzazioni, a livello globale, **hanno subito più attacchi ransomware nel 2023**:

- Stati Uniti
- Regno Unito
- Germania
- Canada
- Italia

Cyber Threat Intelligence

Top 5 Paesi - Eventi Ransomware 2023

Figura 12



Le organizzazioni con sede negli Stati Uniti sono risultate le più colpite nel 2023, avendo subito il 48% degli attacchi totali.

Seguono le organizzazioni del Regno Unito (7%), Germania (5%), Canada (4%) e Italia (4%). Il totale degli attacchi subiti dai paesi inseriti nella lista Top 5 ammonta al 68% degli eventi totali registrati nel 2023.

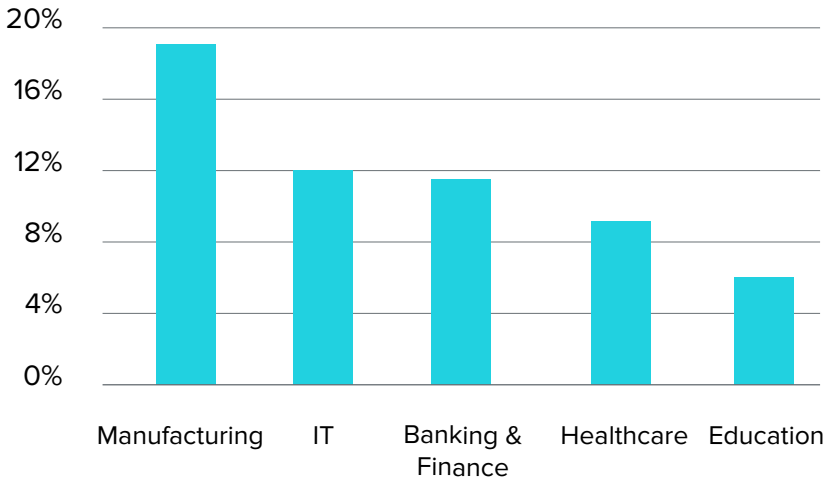
Da segnalare che la classifica dei paesi nella Top 5 del 2023 mostra una situazione analoga a quanto già riportato lo scorso anno.

Per quanto concerne **i settori maggiormente colpiti da attacchi ransomware durante il 2023**, di seguito la Top 5:

- Manufacturing
- IT
- Banking & Finance
- Healthcare
- Education

Top 5 Settori - Eventi Ransomware 2023

Figura 13



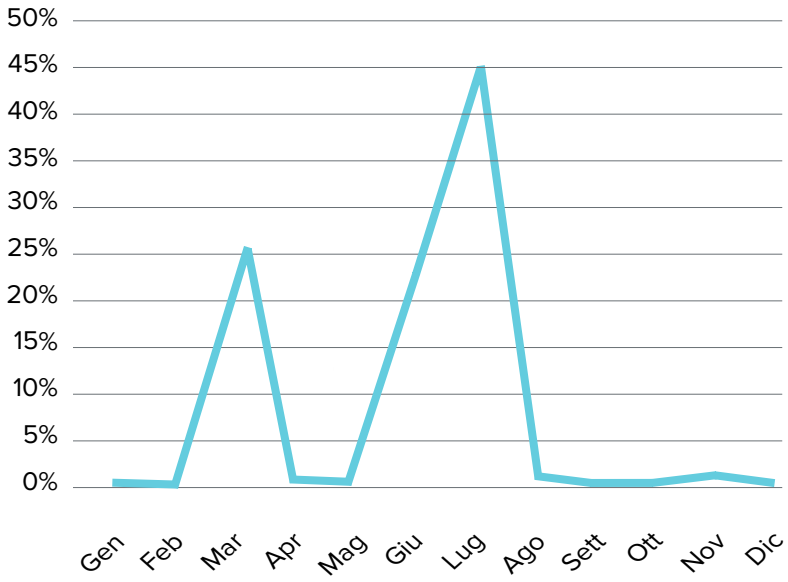
Il settore del Manufacturing risulta al primo posto nella lista, con il **19%** degli attacchi totali del 2023. Seguono il settore IT (12%), Banking & Finance (11%), Sanitario (9%) e quello Educativo (6%). L'insieme degli attacchi ai danni dei settori presenti nella Top 5 si attesta al 57% del totale degli eventi registrati nel 2023.

Approfondimento Cl0p

Come per l'anno passato, anche durante il 2023 si è potuto osservare **lo sfruttamento di particolari vulnerabilità** da parte di alcuni gruppi ransomware. In particolare, il team YCTI ha osservato un **picco di attacchi effettuati dal gruppo criminale Cl0**p a seguito della scoperta e dello sfruttamento attivo di due vulnerabilità ai danni di specifiche applicazioni di trasferimento file. Dai dati analizzati dal team YCTI, la scoperta e lo sfruttamento di tali vulnerabilità avrebbero coinciso con picchi di attacchi effettuati dalla gang ransomware e osservati in particolare a marzo 2023 (26% degli attacchi totali) e nei mesi di giugno e luglio 2023 (rispettivamente il 24% e il 44% degli attacchi registrati).

Panoramica vulnerabilità

Figura 14



Di seguito viene riportata una panoramica delle vulnerabilità sopracitate.

GoAnywhere

A febbraio 2023, **Fortra ha notificato una vulnerabilità denominata CVE-2023-06691** presente nell'applicazione di trasferimento file GoAnywhere Managed File Transfer (MFT), **che ha consentito agli attaccanti l'esecuzione di codice da remoto sulle istanze con consolle amministrativa esposta**. La patch è stata successivamente rilasciata il 7 febbraio, mese in cui Cl0p ha confermato di aver sfruttato la vulnerabilità riuscendo a esfiltrare dati da più di 100 organizzazioni.

Cyber Threat Intelligence

MOVEit

MOVEit: A fine maggio 2023 Progress Software ha notificato la vulnerabilità CVE-2023-343622 presente nei prodotti MOVEit Transfer e MOVEit Cloud. Si tratta di una **vulnerabilità di tipo SQL injection (SQLi) che interessa le applicazioni web MOVEit** esposte su internet, **permettendo agli attaccanti di accedere ai database ospitati dalle applicazioni interessate**. Microsoft ha osservato e attribuito lo sfruttamento della vulnerabilità al gruppo ransomware Cl0p che, a sua volta, ha rivendicato l'utilizzo di tale exploit all'interno del proprio Data Leak Site (DLS).

Non è chiaro se il threat actor Cl0p abbia utilizzato le vulnerabilità solo per sottrarre i dati ed estorcere denaro alle organizzazioni vittima per evitare il rilascio dei file o se abbia anche cifrato i sistemi colpiti. È tuttavia indubbio il grande impatto derivato dallo sfruttamento delle vulnerabilità, considerata la presenza diffusa a livello globale delle applicazioni di trasferimento colpite, utilizzate sia da enti privati che governativi.

Credenziali compromesse

Nel 2023 il team YCTI ha osservato una **crescita dell'interesse e del mercato relativo alle credenziali compromesse da malware Infostealer** all'interno degli ambienti underground. **Questa tipologia di malware**, distribuito principalmente attraverso campagne di phishing e software piratati, **ha il compito di prelevare informazioni sensibili** (tra cui credenziali salvate sul browser, carte di credito, cookies, wallets) dal sistema infettato e trasmetterle al cybercriminale. **Le credenziali esfiltrate**, specialmente se associate a servizi critici e ancora valide, **possono essere sfruttate per ottenere l'accesso iniziale a un sistema aziendale**. Questo modus operandi è comunemente utilizzato dalle gang ransomware.

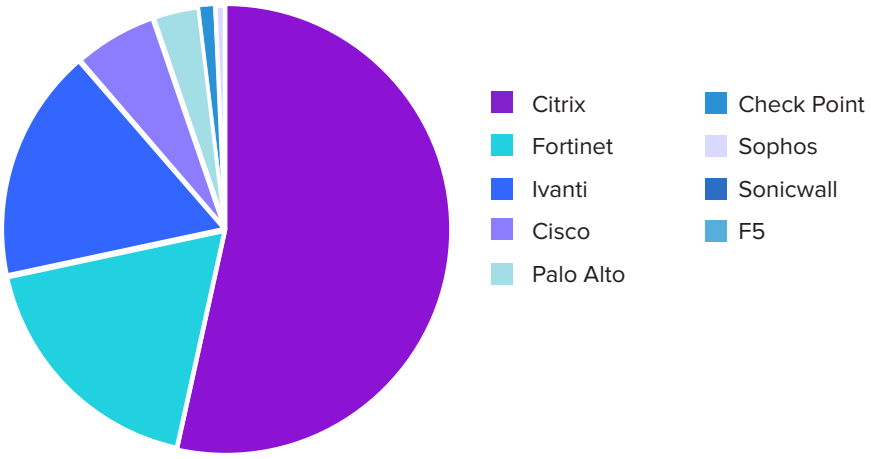
Nel corso del 2023 il team YCTI ha identificato oltre **193 milioni di credenziali compromesse da Infostealer** (+180% rispetto al 2022) esfiltrate da oltre 2.8 milioni di sistemi compromessi differenti. **Tale crescita è dovuta**, oltre al maggiore mercato e interesse menzionato in precedenza, **alla distribuzione nel corso del 2023 di nuovi malware Infostealer e all'aggiunta di nuove fonti ottenute attraverso le continue attività di ricerca sotto copertura condotte da parte del team YCTI**.

Cyber Threat Intelligence

Credenziali compromesse critiche per vendor

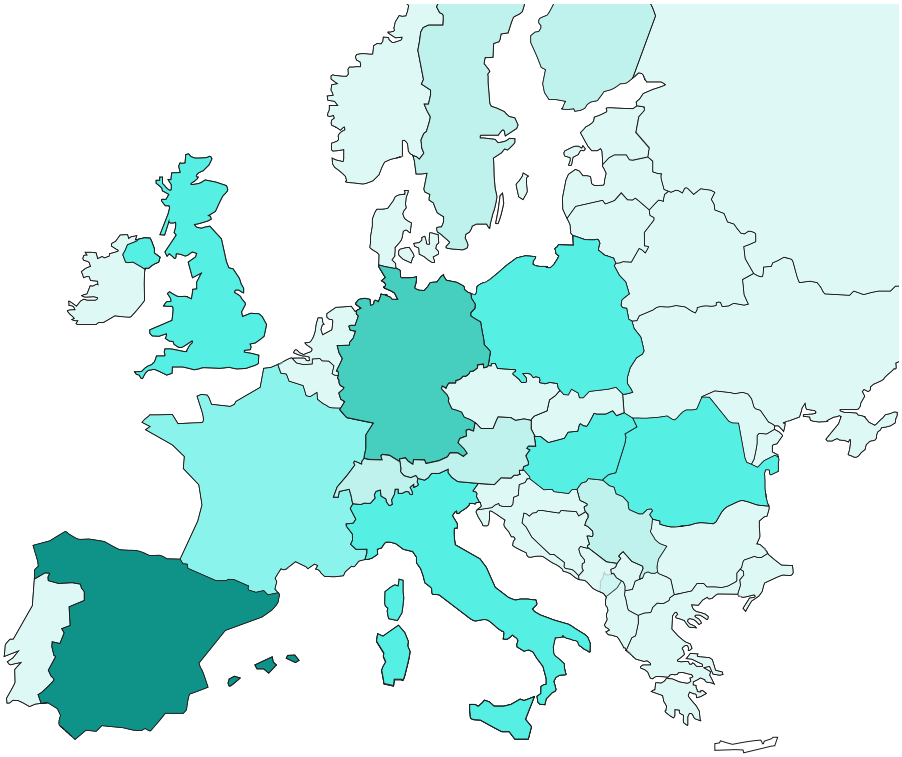
Oltre **60 mila credenziali identificate sono riconducibili a portali aziendali critici**, come ad esempio VPN e Firewall, relativi a diversi vendor:

Figura 15



Nel contesto dei sistemi compromessi identificati, **l'Italia si posiziona al 20esimo posto su scala mondiale con un totale di oltre 38 mila dispositivi infetti** (+123 % rispetto al 2022), e **al terzo su scala europea**, preceduta da Spagna (60 mila) e Germania (47 mila), e seguita da Francia (36 mila), Polonia (32 mila) e Regno Unito (29 mila).

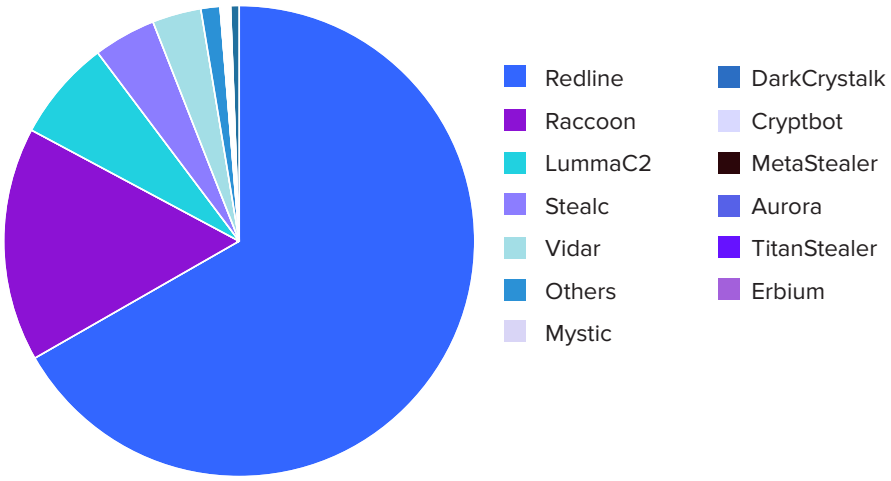
Infezioni da Infostealer in Europa



Infezioni da Infostealer in Italia

Il **2023 è stato inoltre caratterizzato dalla presenza di una grande varietà di malware Infostealer**. In particolare, per quanto riguarda il territorio italiano si osserva Redline al primo posto con oltre 25 mila infezioni (67%), seguito da Raccoon (16%) e LummaC2 (7%). Di seguito sono rappresentate le diverse tipologie di malware Infostealer identificate in Italia:

Figura 16



La crescita del mercato delle credenziali compromesse è stata inoltre osservata nei black market sotto monitoraggio da parte del team YCTI, dove è stata **identificata la messa in vendita delle credenziali esfiltrate da oltre 82 mila host italiani** (+ 11,5% rispetto il 2022).

Fraudolent shops e operazione #fashionmirror

A inizio 2023 il team **YCTI ha condotto un'investigazione che ha portato alla luce un'infrastruttura e una rete di oltre 13 mila shop fraudolenti**.

L'operazione denominata **#fashionmirrror che ha coinvolto oltre 48 brand del fashion con grandi marchi del Made in Italy e internazionali** è stata prontamente segnalata alla Polizia Postale e delle comunicazioni e sono state condotte le operazioni di contrasto e smantellamento dei domini fraudolenti identificati.

Dalle indagini condotte è emerso che il 90% dell'infrastruttura appariva collocata negli USA, Panama e Turchia; analisi più approfondite sulla posizione reale dei server hanno permesso di rilevare delle tracce dell'infrastruttura criminale anche in Europa.

L'investigazione **#fashionmirror è stata inoltre citata nel corso del 2024 da parte della testata giornalistica Le Monde**[2], che ha condotto un indagine che ha portato alla luce ulteriori shop fraduolenti, di cui una buona parte già individuati e investigati dal team YCTI durante l'operazione svolta nel 2023.

Il team YCTI, tramite la propria divisione di brand abuse **ha l'obiettivo di monitorare e contrastare attivamente siti fraudolenti, studiando e mappando costantemente i Threat Actor** che sono dietro a queste operazioni e a queste infrastrutture criminali.

Nel corso del 2023, oltre all'operazione citata #fashionmirror, **il team ha tracciato e identificato oltre 5 cluster differenti di Threat Actors**, la maggior parte di origine cinese che hanno lo scopo di mantenere attive infrastrutture legate ad e-commerce fraudolenti.

[2] https://lnkd.in/eJ4Z8TjA

Sezione 4

RED TEAM

Red Team

Commento Trend YRT

Dal punto di vista dell'offensive security, si potrebbe definire il 2023 come un anno di transizione: **i framework TIBER-IT[3] e DORA[4]**, con il loro prossimo obbligo di implementazione, cominciano ad comparire in maniera sempre più insistente. Per questo motivo, sono diverse le aziende italiane che si stanno preparando al meglio in maniera proattiva, impostando progetti di security assessment a tutto tondo in modo più strutturato.

Il numero di singole progettualità gestite nell'anno da parte del Red Team di Yarix (YRT) risulta leggermente inferiore dell'anno precedente, **230 contro 275 del 2022, per un numero di giornate sostanzialmente equivalente**. Questo è sintomo di un aumento di task più corposi, nonché di un incremento di commitment e budget da parte delle aziende presenti in questo tipo di analisi, fattore non così scontato.

Tra tutte risalta l'**aumento di richieste di assessment di tipo Social Engineering**, in particolare tramite campagne di Spear Phishing (+50%). Evidentemente per le aziende è sempre più importante lavorare sulle proprie difese umane, stimolando la consapevolezza e la reattività dei propri dipendenti tramite simulazioni realistiche. Per questo motivo YRT ha costruito nel tempo un servizio sempre più sofisticato, che porti al cliente **l'esperienza di un attacco costruito su misura da un Threat Actor intenzionato a prendere di mira specificatamente l'azienda e i suoi dipendenti**. In questo scenario, per creare un'esperienza realistica, il Red Team mette in campo creatività e improvvisazione, invece di fare affidamento su scenari preconfezionati.

Grazie alle campagne di Spear Phishing svolte durante il 2023, YRT è in grado di delineare il profilo dell'azienda media italiana e della relativa awareness:

[3] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.htmlhttps://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

[4] https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act

Red Team

500 Dipendenti dotati di caselle e-mail

41,4% Apertura mail di phishing

21,9% Interazione con link o pulsante contenuto

13,4% Inserimento una o più credenziali valide

Weak Strong

Robustezza media delle credenziali

12,7% Segnalazione dell'email malevola dai parte dei dipendenti

Come già evidenziato nel corso del 2022, **prosegue la richiesta di progetti avanzati di Red Teaming, con un occhio di riguardo alle fasi preliminari di Threat Intelligence**, proprio come da dettami di **DORA (con il Threat-Led Penetration Test) e TIBER (che sta per Threat Intelligence Based Ethical Red teaming)**. Sebbene a ritmo misurato, emerge in diversi settori la necessità di mettere sotto la lente di ingrandimento le proprie capacità difensive e di reazione a un evento avverso. In generale, stanno aumentando la coscienza e la cultura generale, che rendono gli investimenti e le scelte strategiche in termini di sicurezza informatica meno focalizzate sulla tecnologia, ma più sul servizio e sulla gestione armoniosa degli eventi nel suo complesso.

Red Team

Proprio in quest'ottica, il 2023 segna il recepimento su larga scala di progettualità di tipo Purple Team Exercise. Questo approccio formativo consiste in una aperta collaborazione proficua tra attacco e difesa, per arrivare a un tuning meticoloso di sistemi e configurazioni di monitoraggio e risposta in ottica di copertura, efficienza ed efficacia.

Va qui menzionato il ritorno di fiamma degli scenari on-premise: se negli ultimi anni vi è stata un'esplosione degli attacchi conducibili da qualsiasi parte del mondo, nel 2023 si può dire siano tornati di moda quelli svolti fisicamente presso sedi, impianti o magazzini allo scopo di sottrarre informazioni, dispositivi aziendali o entrambi. **Nuove tecniche di Physical Hacking e la diffusione di strumenti easy-to-use**, come Flipper Zero, **hanno puntato nuovamente i riflettori su questa tipologia di scenario, che con buona probabilità subirà un'ulteriore impennata se inclusa nei test obbligatori DORA**. La grande differenza con gli approcci del passato consiste nella richiesta di un maggiore focus sugli scenari di minaccia (approccio Threat-based) rispetto a una semplice lista di problematiche fini a sé stesse, come ad esempio riguardanti alcune lacune sulle reti Wi-Fi non sfruttabili in un contesto realistico.

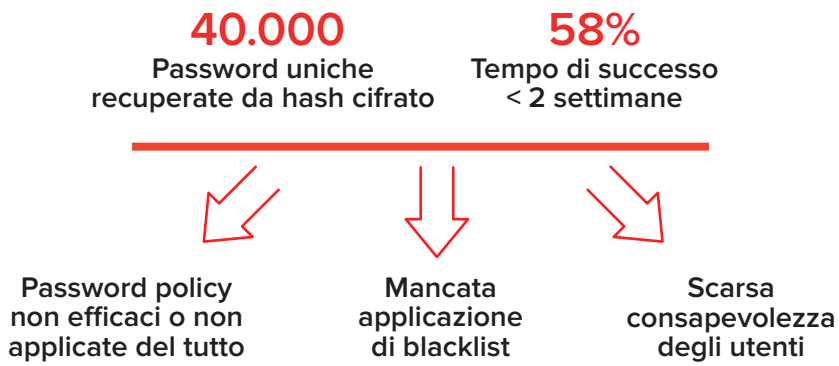
Active Directory

In questa sede, troviamo necessario spendere qualche parola anche sul tema della **Active Directory (AD)**. Il livello di attenzione su questo ambiente è drasticamente lievitato negli ultimi anni, grazie a ricerche e vulnerabilità pubblicamente diffuse (con occhio particolare al lavoro svolto da Specter Ops) e, di conseguenza, a una serie di tool di offensive security che ne sono derivati (tra tutti, proprio Bloodhound). Non si può dire che il livello di sicurezza delle implementazioni presente presso le aziende abbia però tenuto il passo. Cresce quindi curiosità sul tema e **la necessità di ricevere valutazioni di sicurezza su AD che vadano al di là di mere checklist di problematiche, ma che mostrino gli effettivi rischi, specie in contesti di attacco reale** (ad esempio, furto di credenziali di un utente di tipo X). Come ulteriore approfondimento, spesso collegato proprio a cattive pratiche in ambito **Active Directory, si vuole proporre quello degli assessment della robustezza delle proprie credenziali**. Infatti, sempre più realtà richiedono un'analisi pratica del livello di maturità delle proprie password policy, che vada al di là della semplice intervista o analisi della policy stessa e che metta sotto scacco le credenziali, simulando il comportamento di un Threat Actor che tenti di risalire e quindi decifrare le password per proprio tornaconto.

Come si potrà intuire, accedere alle credenziali di dominio di un'azienda è un'operazione molto delicata, che deve rispettare precisi vincoli di confidenzialità. Per questo motivo, **nel corso del 2023 YRT ha costruito una propria infrastruttura fisica di cracking off-line, che ha permesso di ricostruire un numero considerevole di credenziali in ambiente controllato**. La parte focale di quest'attività è rappresentata dal valore aggiunto della creatività del Threat Actor, in grado spesso di cogliere e ricostruire determinate cattive abitudini aziendali e quindi organizzare Dictionary Attack estremamente mirati ed efficaci.

Red Team

Grazie alle **attività di cracking svolte durante il 2023**, YRT ha ottenuto i seguenti risultati:



Per chiudere, infine, proponiamo un commento sui trend del 2023, tra i quali emerge la volontà di estendere concetti di cybersecurity a tecnologie e servizi innovativi quali LLM (Large Language Models), Deep Fake, Automotive e Web3 Security, sui quali YRT sta investendo in termini di formazione, ricerca e sviluppo, così come per i Threat Actor.

Focus su CVE e pubblicazioni

Nel corso del 2023 **YRT ha pubblicato, su YLABS[5], il blog online di Yarix dedicati ad approfondimenti di cyber security**, i seguenti articoli:

- **SIRI WI400: XSS on Login Page – CVE-2022-48111**: ovvero la prima CVE riconosciuta ad YRT nel corso dell'anno, grazie alla proficua collaborazione con Siri Informatica
- **PrivEsc on a production-mode POS**: esposizione tecnica di una catena di vulnerabilità note adattata e sfruttata nel contesto dell'analisi di un POS di produzione
- **Vade Secure Gateway Multiple XSS (CVE-2023-29712, CVE-2023-29713, CVE-2023-29714)**; ovvero 3 ulteriori CVE legate al software francese un anno dopo la loro individuazione durante un'attività di assessment
- **GIS3W**: Persistent XSS in G3WSuite 3.5 – CVE-2023-29998; quinta e ultima CVE assegnata ad YRT nell'anno, frutto della collaborazione con GIS3W
- **Pizza, Pasta and Red Teaming**: insights and ideas for an Italian-style report: approfondimento legato ad una possibile via per strutturare la complessa reportistica di Red Teaming

[5] https://labs.yarix.com/

È importante aprire una duplice riflessione. Da un lato, le eventuali vulnerabilità non note rilevate da YRT emergono durante reali engagement autorizzati, all'interno dei quali spesso ci si imbatte in problematiche non ancora risolvibili ufficialmente, aumentando il valore aggiunto del test stesso. Dall'altro, se inevitabilmente emerge come in Italia si sia sempre più propensi a seguire un processo di Coordinated & Responsabile Disclosure, vi è comunque molta la strada da fare: in diversi casi si applica ancora l'algoritmo dello struzzo o si arrivano a imbastire processi burocratici così complessi e intricati da scoraggiare un sano processo di ricerca delle vulnerabilità. Questo, a lungo termine, potrebbe però tradursi in un boomerang fatto di zero-day taciute e sfruttate in contesti reali di attacco. Per dovere di cronaca, questo vale in particolar modo per l'Italia, ma riguarda in alcuni casi anche importanti player internazionali.

Il valore aggiunto di un Red Team al giorno d'oggi

Prima di passare al capitolo conclusivo riguardo la YRT Top 10 2023, si vuole proporre un'ultima riflessione. **Strumenti commerciali di "Penetration Test automatizzato" e l'avanzare di implementazioni innovative di Artificial Intelligence**, stanno sollevando alcuni dubbi e paure all'interno della community: Il ruolo dell'analista verrà rimpiazzato?

Se ci si approccia a progettualità come Vulnerability Assessment, Penetration Test o attività di Red Teaming rendendoli task di sicurezza meccanici basati su checklist e semplici "copia-incolla" ottenuti da innovativi scanner, sarà opportuno porsi qualche domanda. Oggi risulta più importante che mai **rimettere al centro la competenza, l'esperienza e il valore aggiunto che può portare l'Offensive Security in quanto Proactive Security**. Se il tutto si traduce nella gestione in outsourcing di un prodotto commerciale, cosa impedisce a quel punto all'azienda stessa di risparmiare, utilizzando da sé gli stessi strumenti "che fanno tutto da soli"?

Qui sta la chiave di lettura. È necessario rompere le barriere del passato e **avvicinare quanto più possibile il Red Team al Blue Team, in un'ottica di miglioramento a 360 gradi** (e oltre). Si deve puntare al perfezionamento continuo della reportistica e delle informazioni strategiche che ne possono derivare. In questo modo da "carta accumulata in un cassetto" si ottiene non solo un piano di lavoro prioritizzato, ma anche, in taluni casi, input a ragionamenti che possono andare oltre il perimetro di azione e importanti investimenti atti a proteggere il business e tutto ciò che ne deriva. "L'attacco è la miglior difesa" è forse una frase fatta, ma tutt'altro che priva di significato. Se a questo aggiungiamo la possibilità di "intervistare" l'attaccante per conoscere nel dettaglio le operazioni svolte, sapendo quanto sia poco praticabile in un contesto reale di minaccia, probabilmente il valore aggiunto prende corpo in maniera più nitida. Ecco che **strumenti di Penetration Test automatizzato e innovazioni nel campo dell'Intelligenza Artificiale** non diventano il nemico da scongiurare, ma **un'incredibile arma da sfruttare**. Ovviamente, se si hanno le competenze per farlo.

Red Team

YRT TOP 10 2023

Torna anche nel 2023 la **TOP 10 delle bad practice** identificate e sfruttate durante le attività di Red Teaming da parte di YRT.

In prima istanza si riporta un confronto tra le classifiche 2022 e 2023.

TOP 10 2022		TOP 10 2023	
1	Sistemi critici fuori supporto	**1**	Active Directory e inadeguata gestione degli account
2	Applicazione approssimativa della Two-Factor Authentication	**2**	Copertura parziale o inefficiente da parte dei sistemi di protezione
3	Scarsa consapevolezza da parte degli utenti	**3**	Bad practice a livello sviluppo applicativo da parte dei fornitore - NEW
4	Gestione non conforme di informazioni confidenziali	**4**	Gestione non conforme di informazioni confidenziali
5	Active Directory e inadeguata gestione degli account	**5**	VPN mai configurate - REVIEW
6	Copertura parziali da parte dei sistemi di protezione	**6**	Inefficienze nei processi di decection - REVIEW
7	Inefficienza nei processi difensivi	**7**	Ricostruzioni dell'evento di sicurezza incomplete o non accurate - REVIEW
8	Password policy inefficaci	**8**	Password policy inefficaci
9	Vulnerabilità in sistemi critici esposti	**9**	Scarso controllo della superficie di attacco pubblica - REVIEW
10	Segregazione logica mai applicata	**10**	Applicazione incompleta della two-factor authentication

Come esercizio di stile, l'ordine della classifica di quest'anno rappresenta anche un **tentativo di rappresentarne una pericolosità**, similarmente alle celeberrime TOP 10 OWASP.

Sono 5 le new entry (totali o parziali) del 2023:

- **Bad Practice a livello di sviluppo applicativo da parte di fornitori** - NEW
- **VPN mal configurate** - REVIEW
- **Inefficienze nei processi di detection** - REVIEW
- **Ricostruzioni dell'evento di sicurezza incomplete o non accurate** - REVIEW
- **Scarso controllo della superficie di attacco pubblica** - REVIEW

Per ognuna delle voci, si riporta una rapida descrizione o nota di aggiornamento rispetto ai nuovi trend osservati.

Red Team - 2023 | YRT TOP 10

01 - Active Directory e inadeguata gestione degli account

Una volta giunti in rete interna, emergono solitamente una serie di problematiche che le aziende ignorano da decadi e che risulta tendenzialmente risultano troppo onerose. In assoluto, **Active Directory risulta il terreno più fertile, in quanto molto critico dal punto di vista della disponibilità dei servizi**, e contestualmente spesso mal gestito e mai sottoposto a hardening o monitoraggio mirato. Sono quindi innumerevoli i percorsi che possano agilmente permettere l'elevamento dei privilegi a ruoli di amministratori di dominio o amministratori locali in gran parte dell'infrastruttura gestita raggiungibile.

Update 2023: nonostante non siano più così recenti, le tecniche di attacco su Active Directory colgono spesso impreparate le infrastrutture avversarie e altrettanto i sistemi di monitoraggio.

02 - Copertura parziale da parte dei sistemi di protezione

Numerose aziende hanno investito in maniera importante sul tema del monitoraggio continuo o nell'adozione di sistemi avanzati di difesa. Tuttavia, anche in questo caso emergono spesso delle zone d'ombra, come ad esempio s**istemi che non vengono monitorati perché troppo "fragili" o troppo critici per subire un'interferenza esterna; per non parlare del possibile errore umano in fase di deploy o disallineamento tra perimetro esistente e perimetro di monitoraggio**. Eccezioni nella copertura, specialmente nel momento in cui si ritiene di avere tutto sotto controllo, portano a un falso senso di sicurezza e sono occasioni ghiotte per muoversi sottotraccia.

Update 2023: le simulazioni di attacco nel corso del 2023 hanno posto il focus su una fascia di aziende che hanno investito in termini di soluzioni e servizi di monitoraggio, optando per la strada più economica per rispondere a una necessità (ad esempio open source), ma spesso incompleta e non affidabile.

03 - Bad Practice a livello di sviluppo applicativo da parte di fornitori - NEW

Il tema della gestione sicura delle terze parti è sicuramente di grande attualità, con nuovi e importanti vincoli anche a livello normativo all'orizzonte. Di fatto, sono diversi gli attacchi noti in cui questo tipo di dinamica è effettivamente cruciale: dopo aver indirizzato la sicurezza del proprio perimetro, è fondamentale che nessun fornitore rappresenti un abbassamento del livello di qualità standard e quindi un possibile entry-point o bypass alle misure di sicurezza previste.

Con questa voce si vuole in particolar modo evidenziare come sia **fondamentale affidare lo sviluppo di soluzioni applicative a fornitori che seguano accuratamente un S-SDLC (Secure Software Development LifeCycle) e che siano in grado di dimostrarlo**. Non è quindi tollerabile per le aziende appoggiarsi a fornitori che non abbiano mai svolto un'analisi del codice o organizzato un Penetration Test applicativo. Ciò che ne emerge spesso sono quindi bad practice allarmanti, sintomo di come per alcuni fornitori, la sicurezza delle informazioni sia un tema nemmeno lontanamente sfiorato.

04 - Gestione non conforme di informazioni confidenziali

Ancora troppo spesso la cattiva gestione di informazioni confidenziali rappresenta una enorme fonte di dati per il Threat Actor. Questo punto copre in primis **una cattiva gestione della propria casella mail, spesso utilizzata come archivio per documenti critici e password, fino ad arrivare a file di configurazione, backup, manuali, script non protetti e da nomi esageratamente evocativi** (Password.*).

Update 2023: nel corso dell'anno scorso, questa voce vede come ulteriore peculiarità l'utilizzo non conforme di share di rete aziendali, spesso mal protette, come fonte di accesso ad informazioni estremamente appetibili per un Threat Actor.

05 - VPN mal configurate - REVIEW

Questa voce, new entry del 2023, vuol rappresentare un'ulteriore verticalizzazione della precedente "Segregazione logica mal applicata".
Specialmente in caso di accessi VPN, **non è ancora sufficientemente sentita la necessità di dover assegnare con granularità estrema le reti e i servizi raggiungibili dal singolo utente o host**. Al contrario, spesso gli utenti remoti hanno tutti la stessa visibilità nella rete interna, che include server contenenti informazioni confidenziali o critiche per il business come i backup.

Update 2023: il dettaglio che si vuole mettere in luce nella rivisitazione corrente sta nella mancanza di hardening e di test di determinati meccanismi. Le aziende hanno colto la necessità di restringere i privilegi forniti tramite gli accessi VPN, ma molto spesso non hanno considerato l'importanza di testare la possibilità di bypassare determinati vincoli in maniera agile. Per meglio chiarire, ad esempio, se l'azienda impone ai propri dipendenti l'uso del "Client X" cui ha applicato quindi una serie di restrizioni ben fatte, deve anche preoccuparsi non sia possibile accedere anche tramite "Client Y", nel quale magari tutte le restrizioni di cui sopra risultano non applicate e quindi bypassate in toto.

06 - Inefficienza nei processi di detection - REVIEW

Questa voce, new entry del 2023, rappresenta una prima verticalizzazione della precedente "Inefficienza dei processi difensivi".
Che si tratti della presa in carico di alert critici o di una scarsa correlazione di eventi singoli, **è poi la qualità del servizio, e non dello strumento, che spesso fa la differenza in situazioni critiche**. In questi casi, come dimostrato, gli attaccanti utilizzano tecniche elusive avanzate, ancora una volta sfruttando buchi o inefficienze nei processi di gestione degli eventi.

Update 2023: il focus che vuole rappresentare questa voce è dato dalla mancanza di tuning delle soluzioni di sicurezza implementate. Molto spesso si ritiene che una volta acquistata la licenza di un IDS/IPS, di un SIEM o di un XDR, si risulti quindi inattaccabili e in grado di bloccare qualsiasi minaccia. Tuttavia, come per qualsiasi tecnologia difensiva, è necessario calare la stessa nel proprio contesto di utilizzo, nei confronti degli scenari di minaccia più plausibili e, oltretutto, nei confronti delle più recenti modalità di attacco. Risulta quindi necessario pianificare attività di Purple Team Exercise a cadenza periodica (ad esempio annuale) allo scopo di portare la propria capacità difensiva a un livello superiore rispetto a un'infrastruttura di default che potrebbe risultare non adatta a tutte le casistiche, specialmente se il Threat Actor più plausibile contro cui ci si può trovare a competere non sia uno script kiddie, ma qualcuno con abilità superiori e capace di bypassare le capacità di detection di default.

07 - Ricostruzioni dell'evento di sicurezza incomplete o non accurate - REVIEW

Questa voce, new entry del 2023, rappresenta un'ulteriore **verticalizzazione della precedente "Inefficienza dei processi difensivi"**.

Update 2023: gli attacchi condotti nel corso dell'anno hanno portato alla necessità di meglio dettagliare la categoria, trattando specificatamente di processi di detection. Ciò che si vuole mettere in luce è la differenza tra ciò che si è rilevato e ciò che effettivamente risulta il perimetro di attacco interessato. Ad esempio, se la ricostruzione del Blue Team di un attacco Password Spraying in ambito Office365 individua correttamente l'attacco, segnalando il coinvolgimento di 10 account cui forza il cambio password, si avrà in qualche modo il falso senso di sicurezza di aver bloccato l'evento e risolto prontamente il caso. Se il vero attacco però avesse riguardato anche un solo utente in più effettivamente compromesso, ma fuori dai radar della ricostruzione, ciò resterebbe comunque una vittoria per il Threat Actor. Da qui emerge la necessità di testare, tramite attività di Red Teaming o Purple Team Exercise, nel profondo le proprie capacità difensive e di ricostruzione dell'evento malevolo.

08 - Password policy inefficaci

Specialmente guardando al dominio interno, coinvolgendo inevitabilmente tutti i servizi esposti, emerge una preoccupante cattiva gestione delle password aziendali. **La tendenza è quella di fare il minimo sforzo possibile per soddisfare i requisiti di password policy di default, spesso troppo generiche e totalmente inadeguate**. Questo comporta un'estrema vulnerabilità a Dictionary Attack un minimo organizzati per comprendere il nome dell'azienda o la posizione geografica dello stabilimento preso di mira. In particolare, diventa spesso cruciale l'utilizzo di pattern condivisi, che se ricostruiti fanno cadere l'intero castello.

Update 2023: come spiegato nei paragrafi precedenti, questo tipo di dinamica non è passata di moda e resta radicata a livello di cattiva gestione IT interno, lato fornitori esterni e dal punto di vista dell'utente finale.

09 - Scarso controllo della superficie di attacco pubblica - REVIEW

Questa voce, new entry del 2023, vuol rappresentare una verticalizzazione della precedente "Vulnerabilità in sistemi critici esposti".

Spesso in caso di End-to-End Red Teaming, risultano determinanti vulnerabilità classiche su perimetri poco controllati, ma contestualmente utilizzati e noti al parco dipendenti. Ecco che un banale Cross-Site Scripting sul portale dipendenti, diventa la leva utilizzata per convincere le vittime a inserire le proprie credenziali o a scaricare un file contenente del contenuto malevolo. **Più è critico il sistema, che sia per la confidenzialità dei dati gestiti o per la comunicazione diretta con la rete interna, più rigido dev'essere il processo di aggiornamento, continuo e tempestivo**.

Update 2023: il focus che si vuole porre rispetto a quanto emerso nel corso dell'anno è un passo oltre il concetto tecnico di vulnerabilità. Sempre più di frequente infatti, emerge come l'esposizione di servizi vulnerabili non nasca da una mancanza di consapevolezza sull'importanza di tenere al minimo le possibilità di accesso da rete pubblica, quanto più dallo scarso controllo nel continuo di ciò che è esposto. Infatti, sono numerosi i casi in cui determinate aree aziendali e, ancor più spesso, fornitori per così dire frettolosi, pubblicano spontaneamente servizi non approvati, anche per effettuare test temporanei, senza che l'azienda ne abbia contezza. Nei casi peggiori questi entry-point risultano particolarmente ghiotti per i Threat Actor, abili a individuare rapidamente queste situazioni, al contrario delle aziende stesse che spesso mancano di processi di monitoraggio della propria superficie esposta, nel continuo.

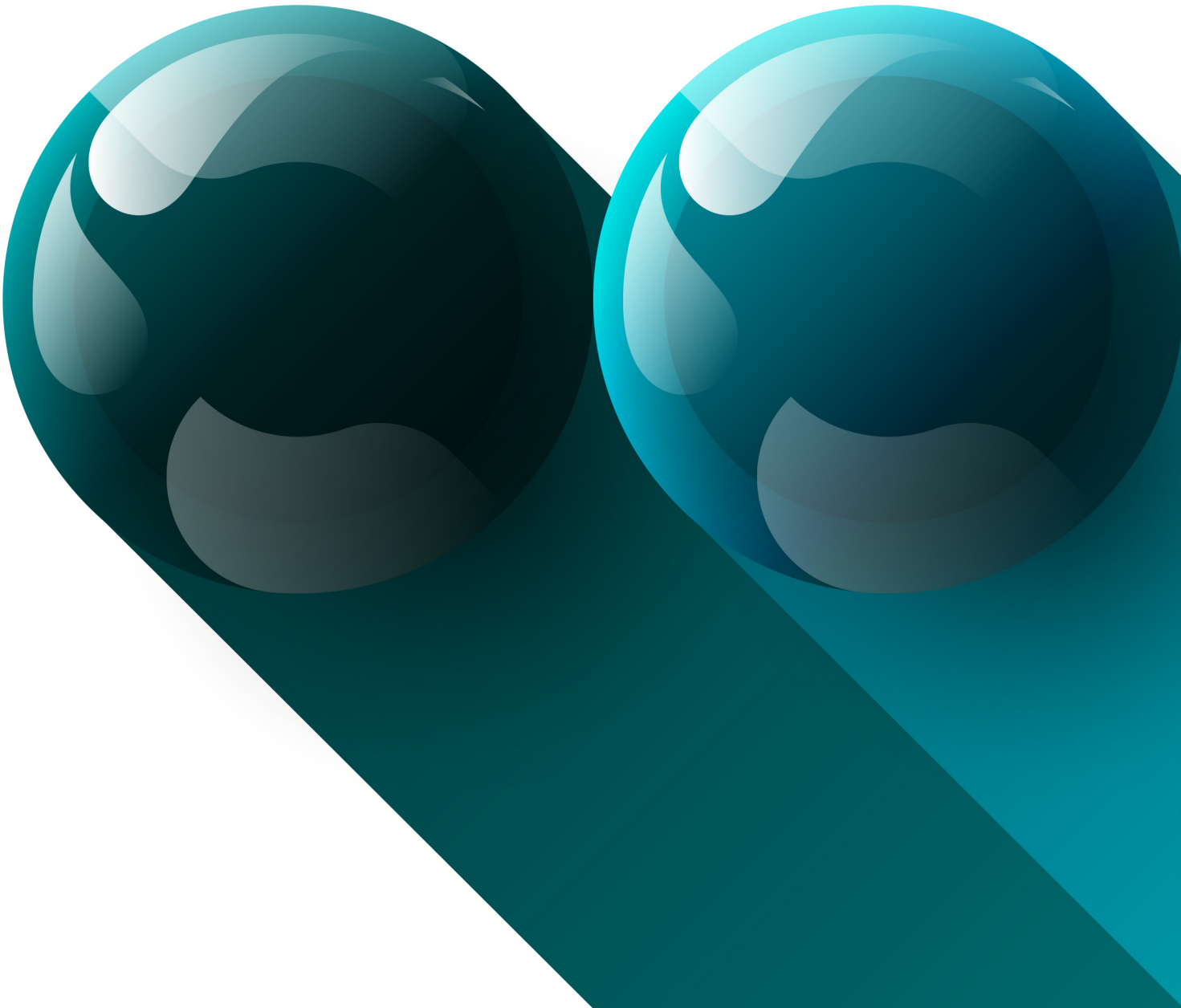
10 - Applicazione approssimativa della Two-Factor Authentication

La legge deve essere uguale per tutti. Molte aziende nel corso degli ultimi anni hanno investito molto nell'applicazione della two-factor authentication su interfacce critiche, come ad esempio mail, VPN, portali critici. Per motivi pratici o, per così dire, organizzativi, **ancora troppo spesso questo meccanismo viene applicato in maniera approssimativa**. Ad esempio, un Amministratore Delegato che condivide la propria casella mail con l'assistente, o per il fornitore che offre manutenzione da remoto all'impianto elettrico tramite un proprio device, fino a quei dipendenti di magazzino che non dispongono di un proprio device aziendale, potrebbero essere esenti da questa misura di sicurezza, rappresentando un target ghiotto per il Threat Actor.

Update 2023: anche per questa voce, il 2023 rappresenta un anno di conferma della presenza piuttosto diffusa di questa cattiva pratica.

Appendice

AUTOMOTIVE CYBER SECURITY



Automotive Cyber Security

Norma ONU R155 e la sua importanza per l'industria automotive

Il Regolamento ONU n. 155 (UN R155) introdotto dalla Commissione economica per l'Europa delle Nazioni Unite (UNECE WP.29) **segna una svolta nell'industria automotive e nell'intera catena del valore associata allo sviluppo dei veicoli. Obiettivo: omologazione dei veicoli sotto il profilo della cyber security**.

La norma è entrata in vigore a luglio 2022 per l'omologazione dei nuovi tipi di veicoli e ne richiede la piena attuazione per tutti i veicoli di nuova immatricolazione entro luglio 2024, introducendo per la prima volta una normativa giuridicamente vincolante di vasta portata in materia di cyber security dei veicoli.

L'applicabilità del Regolamento Onu n. 155 **riguarda i 59 Stati membri attualmente aderenti alla Convenzione UNECE sull'armonizzazione dei veicoli a motore** (basata sull'accordo del 1958 tra gli Stati membri dell'UNECE), tra cui tutti gli Stati membri dell'Unione Europea, che resta uno dei principali mercati di vendita del settore.

I regolamenti dell'UNECE devono essere recepiti nelle legislazioni nazionali degli Stati membri, ovvero i singoli Paesi devono integrare la norma UN R155 nel proprio quadro giuridico.

I produttori globali che intendono commercializzare i propri prodotti nei mercati di riferimento sono pertanto giuridicamente obbligati a istituire e mantenere un Sistema di gestione della sicurezza informatica (CSMS) al fine di ottenere l'autorizzazione all'immissione in commercio per i veicoli di loro produzione e non incorrere, in caso contrario, in potenziali divieti di vendita.

Benché non siano tra i firmatari del suddetto accordo UNECE, anche altri Paesi con mercati importanti per le case automobilistiche internazionali, come India, Cina e Stati Uniti, si stanno uniformando con l'adozione di analoghe normative giuridicamente vincolanti in materia di cyber security o con l'adeguamento degli standard di settore, anch'essi importanti per le case automobilistiche, nell'ottica dello sviluppo e della vendita di veicoli che rispettino i requisiti di cyber security in questi Paesi.

La norma ONU R155 si applica a tutti i nuovi tipi di veicoli ed è principalmente finalizzata a tutelare i veicoli dagli attacchi informatici e nel contempo a creare un contesto gestionale per l'implementazione, la gestione e il miglioramento continui della cyber security. L'obiettivo è garantire la protezione e la sicurezza degli utenti dei veicoli, nonché assicurare la disponibilità delle funzioni dei veicoli e l'integrità dei dati del veicolo. Ciò che è importante comprendere fin dall'inizio è che il raggiungimento di questo obiettivo comporta l'implementazione della cyber security relativa al prodotto anche in altre fasi oltre quelle dello sviluppo e della produzione.

Automotive Cyber Security

Le nuove tecnologie accrescono l'importanza della cyber security nei veicoli

L'esigenza di una regolamentazione in tal senso è sottolineata dai **rapidi progressi tecnologici dell'industria automotive**, tra cui la crescente connettività dei veicoli, l'aumento dell'offerta di servizi sia interni che esterni per i veicoli, l'introduzione di funzioni di guida autonoma e l'utilizzo dei big data. Questi sviluppi hanno creato le premesse per nuovi vettori di attacco.

Attacchi hacker massici da remoto mirati contro singoli veicoli o intere flotte di veicoli rappresentano una possibilità concreta se la cyber security del veicolo non è adeguatamente garantita.

Pertanto, è in aumento il rischio di attacchi informatici, fughe di dati e manomissioni. La norma ONU R155 si propone di contrastare questi rischi con l'introduzione di rigidi requisiti di sicurezza e revisioni periodiche delle misure di cyber security.

Non solo automobili: implicazioni di vasta portata in tutti i settori e per tutte le categorie di veicoli.
Le nuove disposizioni previste dalla norma ONU R155 in materia di cyber security non riguardano solo il mercato tradizionale delle autovetture. Rientrano nel suo ambito di applicazione anche categorie affini di veicoli, come i veicoli commerciali, i veicoli speciali, i veicoli di emergenza, gli autobus e, allo stato attuale, i motocicli e altre possibili forme di mobilità automotive.

Questo approccio globale all'applicabilità dei **requisiti di cyber security** per diversi tipi di veicoli **è finalizzato a proteggere il maggior numero possibile di utenti finali da minacce informatiche**.

La regola generale è: i costruttori e i loro fornitori dell'industria automotive che sviluppano e installano sistemi elettrici/elettronici devono sempre verificare in quale misura le loro attività e i loro rapporti commerciali devono sottostare a tali norme e in quale misura i loro prodotti hanno pertinenza alla sfera della cyber security.

Effetti su OEM e fornitori

L'implementazione della **norma ONU R155 ha conseguenze di vasta portata per i produttori di veicoli e ricambi originali (OEM) e i loro fornitori in tutto il mondo**. Ai sensi dell'implementazione di un CSMS come previsto dal regolamento, gli OEM non solo devono assumersi la responsabilità di garantire la cyber security, ma sono anche tenuti a controllare le rispettive catene di fornitura. Concretamente, il rischio dell'operato dei fornitori in materia di cyber security ricade sulle spalle degli OEM.

È difficile stimare una cifra esatta, ma è presumibile che **migliaia di aziende nella sola Europa siano interessate direttamente o indirettamente da questa normativa**. L'implementazione di un CSMS garantisce che sia gli OEM sia i loro fornitori conducano regolarmente valutazioni dei rischi, colmando le lacune in materia di sicurezza e adeguandosi alla rapida evoluzione delle minacce informatiche.

Automotive Cyber Security

Attualmente, il più importante punto di riferimento dell'intero settore è considerato lo standard **ISO/SAE 21434 Road vehicles – Cyber security engineering per la cyber security nell'ingegneria dei veicoli stradali**. La discussione, l'interpretazione e l'implementazione specifica dello standard a livello delle singole organizzazioni hanno subito una notevole accelerazione in tutto il mondo. Rimane tuttavia l'esigenza di una disamina approfondita dei dettagli di questa norma e di una valutazione di quale sia il modo più efficiente per applicarli, in quanto lo standard definisce ciò che deve essere fatto ma non chiarisce come farlo. Si tratta dunque di una sfida che deve ancora essere affrontata nella pratica quotidiana dell'implementazione della cyber security.

Requisiti di cyber security

Nel dibattito attuale sui requisiti di cyber security, ai vari attori della catena di fornitura si chiede di condurre nuove valutazioni granulari del rischio. Appare immediatamente chiaro che è necessario trovare risposte molto diverse agli stessi requisiti di cyber security per i grandi OEM, per i tanti fornitori grandi e piccoli, nonché per le start-up e i provider di tecnologie che vogliono entrare nel mercato con nuovi approcci e nuove soluzioni.

Questa esigenza è resa più pressante da **diversi obiettivi di protezione della sicurezza**: oltre al sistema/prodotto vero e proprio e ai dati (anche di identificazione personale) e ai flussi informativi, la cyber security come dimensione qualitativa riguarda sempre anche i rischi operativi reali: dalla responsabilità del prodotto alle penali contrattuali e ai rischi finanziari fino alle perdite reputazionali e commerciali. C'è poi un'altra dimensione che deve essere oggetto di un'attenzione particolare quando i veicoli sono intesi come mezzi di trasporto: la sicurezza fisica.

Sicurezza come protezione e come incolumità: l'esigenza di una cyber security olistica

In linea con i requisiti di cyber security, l'ambito della sicurezza funzionale per l'incolumità degli utenti nell'industria automotive è già stato professionalizzato diversi anni fa e, in modo altrettanto sistematico, sta spostando l'attenzione sul funzionamento corretto e privo di errori dei sistemi. Questa dimensione dell'integrità fisica del conducente e dell'ambiente del veicolo deve ora essere armonizzata in maniera sostenibile con i requisiti di cyber security. Entrambi **gli ambiti mirano a garantire l'affidabilità, la sicurezza e la protezione dei sistemi critici dei veicoli**. Ciò richiede un approccio coordinato con l'ausilio di concetti di sicurezza coordinati fin dalla fase di sviluppo e per l'intera durata del ciclo vitale del veicolo.

Oltre a ciò, anche l'**ambito degli aggiornamenti software sta emergendo come ulteriore area di responsabilità: la gestione e l'implementazione degli aggiornamenti software** (previsti dalle disposizioni contenute nel Regolamento ONU n. 156 in materia di sistemi di gestione degli aggiornamenti software nell'industria automotive) **svolgono un ruolo altrettanto fondamentale nell'interazione delle norme di sicurezza**.

Ci sono poi molte altre esigenze, legate alla necessità di garantire attività continue di cyber security, il monitoraggio della flotta di veicoli (ad es. da parte di un centro operativo dedicato), un'efficace gestione della risposta agli incidenti e perfino obblighi di vasta portata fino allo smantellamento del veicolo: tutta una serie di compiti che devono essere affrontati in maniera coordinata.

Automotive Cyber Security

Differenziazione rispetto alla sicurezza delle informazioni e all'IT

Date queste premesse, è evidente che **i requisiti per l'implementazione della cyber security nello sviluppo dei veicoli trascendono i tradizionali aspetti della sicurezza delle informazioni all'interno di un'azienda**. Nello stesso tempo, tuttavia, ci sono anche nuove importanti connessioni e interconnessioni favorite in particolare dall'avvento di nuove tecnologie, nuovi sistemi e nuove competenze specialistiche, per esempio quando si tratta della realizzazione di soluzioni olistiche a livello aziendale, nelle attività a monte, nei processi produttivi e operativi e a livello di sistemi di qualità e di gestione.

Miglioramento dell'agilità per la cyber security

Alla luce della rapidità della digitalizzazione e connettività dell'industria automotive, **è essenziale che i responsabili della cyber security rivedano e adattino costantemente le loro strategie di sicurezza**. L'integrazione di tecnologie avanzate nei veicoli apre il fianco a nuovi attacchi e richiede nuovi requisiti per un approccio flessibile alle sfide in materia di cyber security. È necessario verificare periodicamente la validità dell'assetto di un'azienda, della sua organizzazione, dei suoi processi e dei suoi prodotti.

Promozione di una collaborazione interdisciplinare

La complessità associata all'aumento dei requisiti di sicurezza dei veicoli (nello sviluppo, nella produzione, nel post-vendita e a livello aziendale) richiede una **stretta collaborazione tra sviluppatori, ingegneri, collaudatori, responsabili della qualità e degli acquisti e altre funzioni, nonché provider di servizi di terze parte**. Costruire un approccio olistico che trascenda i confini tra le discipline è essenziale per affrontare le molteplici sfide della cyber security e gestire efficacemente il rischio.

Comprensione chiara degli impegni del top management

Per il buon esito dell'implementazione e del mantenimento delle misure di cyber security è essenziale **un forte impegno a livello dei decisori e dei manager "C-level", sia per mettere a disposizione le risorse necessarie**, sia per promuovere una cultura della sicurezza all'interno dell'organizzazione. Chi si occupa di cyber security deve fare in modo che il senior management comprenda i requisiti normativi e li integri nelle proprie strategie aziendali.

Sviluppo autentico della consapevolezza sulla sicurezza

Diventa ogni giorno più importante **creare consapevolezza e competenza in materia di cyber security** al di là dei tradizionali reparti responsabili dell'IT e dello sviluppo in tutti gli ambiti specialistici relativi ai prodotti dell'industria automotive. Ingegneri, sviluppatori, product manager, possessori di materie prime, acquirenti e altri professionisti non IT dovrebbero avere una conoscenza di base dei principi della cyber security nell'industria automotive. **Una cultura della sicurezza a tutti i livelli aziendali contribuisce a garantire che tutto il personale dipendente riconosca i rischi potenziali e agisca di conseguenza**.

Automotive Cyber Security

Nuove opportunità di sviluppo delle conoscenze e delle competenze

Qual è lo stato del centro di competenza per la cyber security della vostra azienda? In un contesto in rapido mutamento, è **fondamentale investire continuamente nelle conoscenze e nelle competenze in materia di cyber security** e nel giusto approccio all'esperienza e alle best practice. Questo comporta migliorare le competenze dei dipendenti già in organico e reclutare nuovi talenti con conoscenze specialistiche. La promozione dell'apprendimento continuo è fondamentale per restare al passo con le sfide sempre nuove della cyber security.

Promozione della cyber security come motore trainante di qualità

Ritenere che la cyber security sia solo un costoso "add-on" non è più accettabile. Data la crescita delle tecnologie e il modo in cui vengono utilizzate nello sviluppo e all'interno dell'organizzazione, è **necessario un approccio proattivo per identificare e difendersi da potenziali rischi informatici**. Se l'approccio è corretto, i giusti adeguamenti sulla base delle raccomandazioni e delle disposizioni attuative in materia di cyber security possono dare un forte impulso al miglioramento della qualità e della competitività, nonché della conformità normativa.

CONSIDERAZIONI FINALI

Considerazioni finali

La cyber security non è più un'opzione

In un mondo sempre più connesso e tecnologicamente avanzato, la sicurezza cyber non è più un'opzione, ma una necessità imperativa. **L'incremento degli attacchi informatici di varia natura e complessità testimonia una realtà in cui nessun settore è immune**. Si è registrato un notevole aumento nel numero totale di eventi e incidenti di sicurezza, quasi raddoppiando la quantità rispetto al 2022. Questo aumento è particolarmente marcato per gli eventi di gravità critica, che hanno visto un incremento del 300%. In accordo con questa tendenza, nel 2023 il team YCTI ha identificato oltre 193 milioni di credenziali compromesse, un aumento del 180% rispetto al 2022. Questa **crescita è stata attribuita alla distribuzione di nuovi malware Infostealer e all'aggiunta di nuove fonti di intelligence**, che rappresentano i principali punti di ingresso utilizzati dagli attaccanti insieme allo sfruttamento di servizi esposti e malware veicolato via e-mail. Le statistiche del 2023 mostrano, infatti, che **il 41.4% dei dipendenti apre e-mail di phishing, il 21.9% interagisce con link o pulsanti in esse contenuti, e il 13.4% inserisce credenziali valide in form trappola**, indicando un livello di awareness ancora migliorabile.

Dalla manipolazione di dati sensibili fino al sabotaggio di intere flotte di veicoli, gli attacchi cyber stanno diventando sempre più sofisticati e pericolosi. In risposta a questa crescente minaccia, sono state introdotte nuove normative che richiedono un adeguamento rapido e strategico da parte delle aziende. **Regolamenti come la Direttiva sulla resilienza operativa digitale (DORA), il framework TIBER per la simulazione di attacchi, e la Regolamentazione UN R155 impongono standard rigorosi per la gestione della sicurezza informatica**. La UN R155, in particolare, segna una svolta nell'industria automobilistica, richiedendo l'integrazione di sistemi di gestione della sicurezza (CSMS) per garantire la protezione contro attacchi informatici a veicoli sempre più connessi e autonomi.

In questo contesto dinamico, la **collaborazione tra diversi team di sicurezza è diventata fondamentale**. **L'interazione tra il Security Operation Center (SOC) e il Red Team attraverso attività di Purple Teaming ha permesso una migliore preparazione e risposta agli attacchi, combinando difesa e attacco simulato per testare e rafforzare le misure di sicurezza**. Allo stesso modo, l'**integrazione tra Cyber Threat Intelligence (CTI) e Red Team ha promosso un approccio basato sull'intelligence per le simulazioni di attacco**, mentre la collaborazione tra SOC e Incident Response (IR) ha rafforzato i piani di risposta agli incidenti e le valutazioni della prevenzione delle intrusioni.

Considerazioni finali

Innovazione imprescindibile

La crescente complessità degli scenari di minaccia ha reso imprescindibile l'innovazione in questo settore. L'**introduzione di automazione e progetti di intelligenza artificiale supporta significativamente le attività degli analisti**. Queste tecnologie non solo accelerano la raccolta e l'analisi dei dati, ma migliorano anche la precisione nel rilevare minacce e nel generare risposte tempestive. **Il progetto Egyda ha segnato un punto di svolta, introducendo hyper-automation, machine learning (ML) e intelligenza artificiale (AI)** per migliorare la rilevazione e gestione delle minacce. Queste tecnologie hanno permesso una maggiore efficienza nell'analisi e nella risposta agli incidenti. È altrettanto importante sottolineare la **necessità di continuare a sviluppare e implementare soluzioni che sfruttino tecnologie avanzate**, come i Large Language Models (LLM), per gestire l'enorme volume di dati e migliorare ulteriormente le capacità di rilevamento e gestione delle minacce o di simulazione degli attacchi.

In conclusione, nel panorama digitale odierno, **la sicurezza richiede un approccio integrato e innovativo**. Le nuove normative non solo stabiliscono standard più elevati, ma spingono anche le aziende a essere sempre un passo avanti rispetto ai cyber criminali. **La collaborazione tra diversi team di sicurezza e l'adozione di tecnologie avanzate sono essenziali per costruire un ambiente digitale sicuro e resiliente**. In questo modo, non solo possiamo proteggere le informazioni e le infrastrutture critiche, ma garantire al tempo stesso la sicurezza e la fiducia.