learn.sharelock.ai | www.sharelock.ai | info@sharelock.ai

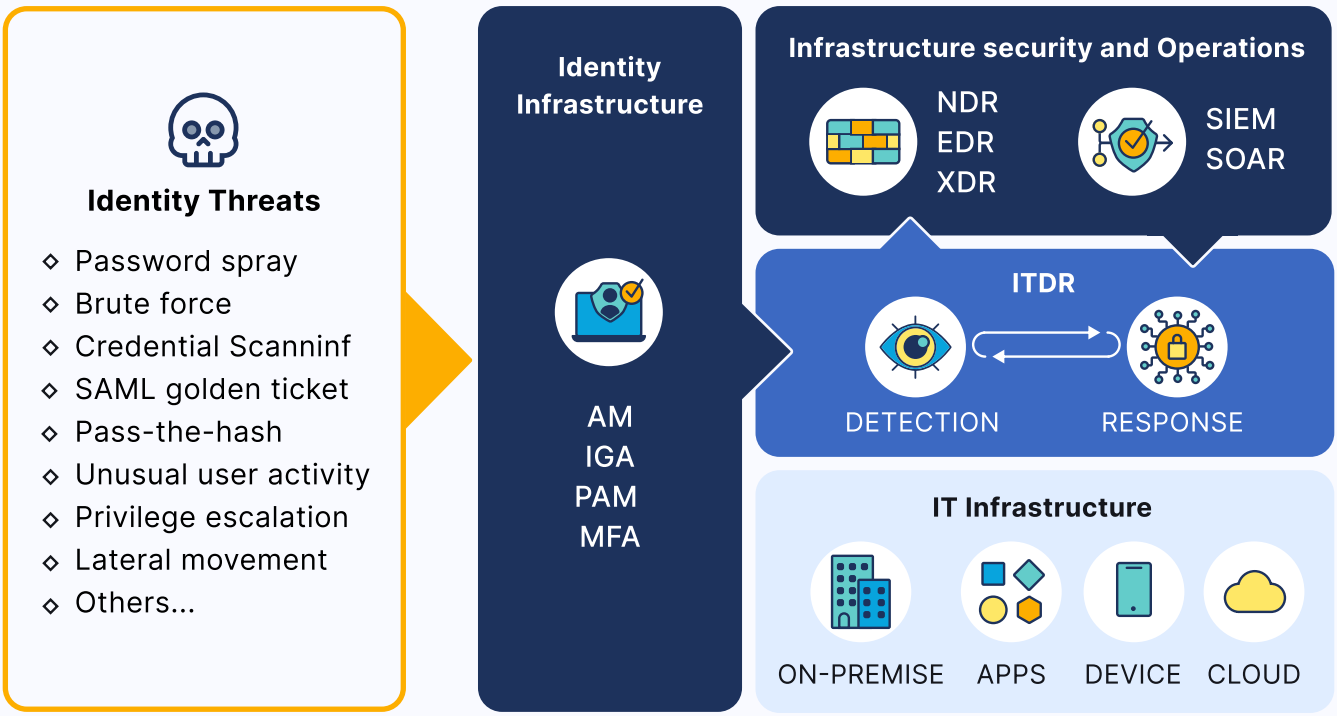
Sharelock

Identity Security Platform

Sharelock

L’ identità come nuovo perimetro di sicurezza aziendale

Nell’Ottobre 2022, Gartner ha pubblicato un documento di ricerca che discute l’importanza dell‘ Identity Threat Detection & Response (ITDR) intitolato: "Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response", pubblicato il 20 ottobre 2022, redatto da Henrique Teixeira, Peter Firstbrook, Ant Allan e Rebecca Archambault. ITDR è un termine introdotto proprio da Gartner per caratterizzare la disciplina della sicurezza dedicata a proteggere l'infrastruttura dell'identità. Similmente a come il Network Detection & Response (NDR) e l’Endpoint Detection & Response (EDR) proteggono l'infrastruttura organizzativa critica, ITDR svolge un ruolo cruciale nel garantire la sicurezza dei sistemi che governano l'identità e l'accesso in tutta l'organizzazione. Con l'identità che ora funge da nuovo perimetro, gli attori maligni, sia interni che esterni, sfruttano frequentemente le lacune nel rilevamento tra le soluzioni tradizionali di Identity & Access Management (IAM) e i controlli di sicurezza dell'infrastruttura.



Sharelock Identity Security Platform

Sharelock Identity Security Platform comprende due moduli interconnessi: Sharelock ITDR e Sharelock ISPM.

Sharelock ITDR • Identity Threat Detection & Response

Questo modulo rileva e risponde alle minacce legate alla sicurezza dell'identità. Si concentra sull'analisi comportamentale degli utenti e delle macchine, impiegando algoritmi di machine learning per stabilire baselines e identificare deviazioni dai pattern normali. Questa capacità permette a Sharelock ITDR di scoprire e adattarsi a minacce all'identità sconosciute o in evoluzione, eliminando la necessità di regole predefinite e consentendo l'identificazione dinamica e la risposta immediata alle violazioni della sicurezza.

Sharelock ISPM • Identity Security Posture Management

Questo modulo gestisce e migliora la postura di sicurezza complessiva delle identità all'interno di un'organizzazione. Si assicura che siano in atto e funzionino correttamente adeguate misure di sicurezza per prevenire minacce potenziali alle identità digitali (es. policy MFA), fa la discovery di account inattivi, account ghost, triggera campagne di ricertificazione su base rischio e su base permesso, riduce la superficie di attacco dell'identità e aiuta l'organizzazione ad avere una corretta igiene dell'identità.

Entrambi i moduli sono parte integrante del prodotto Sharelock Identity Security Platform, integrandosi reciprocamente per fornire una robusta combinazione di rilevamento delle minacce, risposta e gestione della postura di sicurezza. La piattaforma è progettata tenendo presente la facilità d'uso, in particolare per gli analisti della sicurezza e gli amministratori, presentando un cruscotto intuitivo, configurazione senza codice, analisi visuale e capacità di risposta dinamica.

Architettura e Integrazioni

L'architettura di Sharelock Identity Security Platform è organizzata in microservizi. Questi microservizi sono implementati utilizzando container la cui orchestrazione avviene all'interno di un cluster Kubernetes. Grazie a questa peculiarità non c'è effettiva differenza nel distribuire Sharelock sia on-premises che nel cloud. Sharelock funziona senza problemi in tutte e due le modalità con la stessa code-base e il servizio nativo multi-tenant. Stesso set di funzionalità, stesse prestazioni.

Sharelock Identity Security Platform può integrarsi perfettamente con la security posture aziendale presente, inclusi i sistemi SIEM o le piattaforme di protezione degli endpoint. Le capacità di integrazione di Sharelock sono progettate con flessibilità per cooperare strettamente con altre soluzioni di sicurezza utilizzate all'interno di un'organizzazione.

Ecco alcuni punti chiave riguardanti le capacità di integrazione:

Integrazione con i Sistemi SIEM: Sharelock ITDR può fare l'ingestion di dati in real-time da varie fonti, inclusi le applicazioni SaaS tramite API o formati tradizionali di ingestione di log on-prem come Syslog, Filebeat e CEF. Sharelock può sfruttare i SIEM esistenti per "portare intelligenza comportamentale" migliorandone la funzionalità e la capacità di detection o può utilizzarli come sorgente dati per le proprie analisi e usarli solo nella fase di response e incident management.

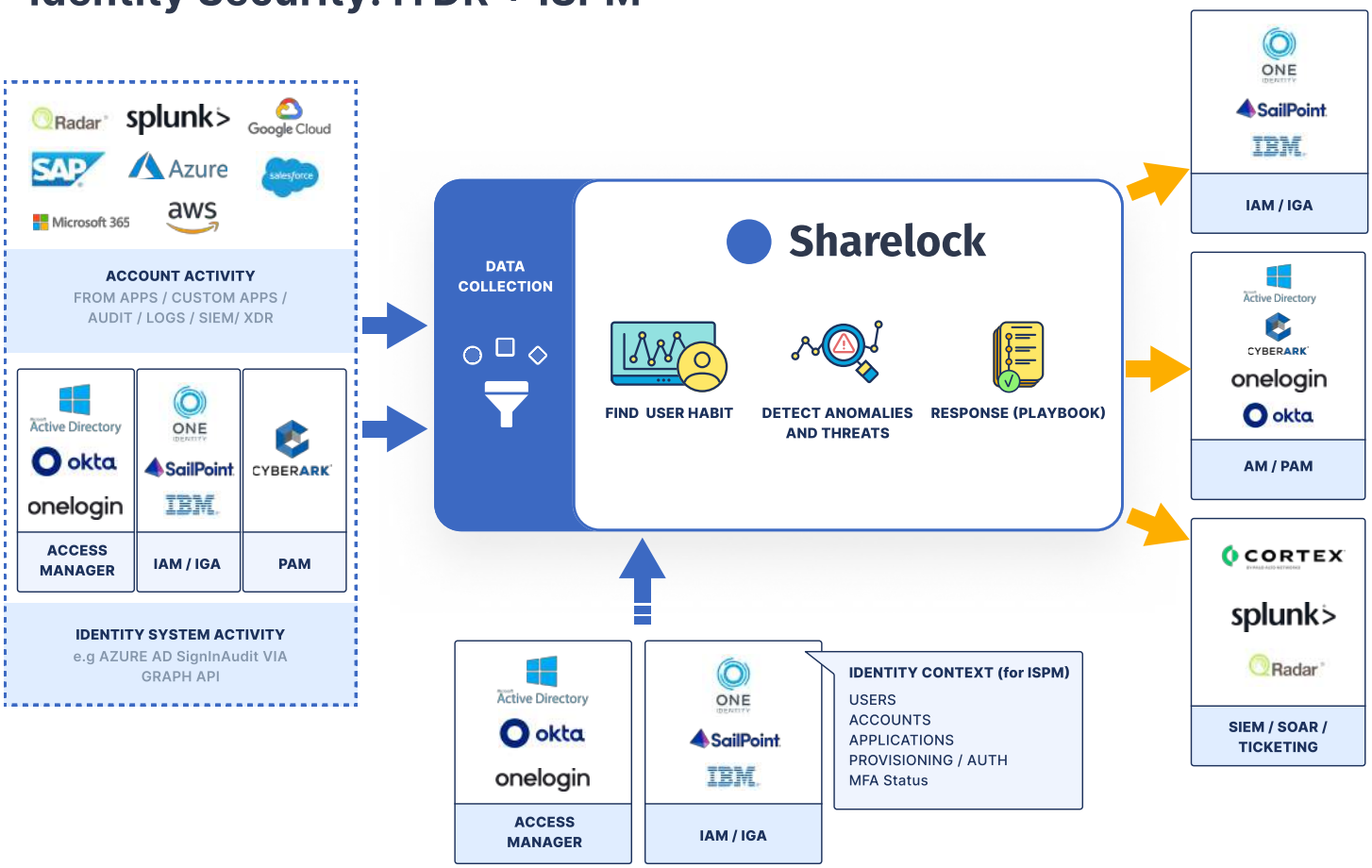
Integrazione con le Piattaforme IAM: Sharelock fornisce un'interazione bidirezionale con le piattaforme IAM ingerendo i registri di audit IAM per identificare anomalie ed applicare risposte operative, come la disabilitazione degli account, il blocco degli utenti e la convalida dell'accesso. Aiuta inoltre alla riduzione della superficie di attacco andando a bonificare i sistemi di identity degli account inattivi, account ghost, account orfani e ad implementare le politiche diminimo privilegio con campagne di certificazione ad hoc.

Protezione degli Endpoint: Sharelock può ridurre significativamente i falsi positivi analizzando i dati provenienti dai sistemi di sicurezza degli endpoint o dai sistemi XDR, applicando il machine learning per distinguere comportamenti benigni da malevoli, ottimizzando il processo di segnalazione e migliorando la risposta alle minacce.

Gestione degli Accessi Privilegiati (PAM): Sharelock si integra con i sistemi PAM per implementare un approccio a zero trust, incorporando flussi di lavoro di approvazione automatizzati basati sul rischio per le approvazioni delle sessioni, rafforzando così i controlli intorno agli account privilegiati.

Personalizzazione e Configurazione: Gli strumenti di configurazione offerti da Sharelock consentono di estendere il rilevamento ML a nuove applicazioni, definire indicatori di comportamento personalizzati e personalizzare le risposte automatiche che sono importanti per l'integrazione con la security posture di un'organizzazione.

Identity Security: ITDR + ISPM



L'AI in aiuto della cybersecurity

Sharelock Identity Security Platform rileva e risponde alle minacce correlate all'identità attraverso il suo modulo ITDR sfruttando diversi approcci chiave:

Comprensione completa: ITDR costruisce diversi Indicator of Behavior da varie combinazioni di soggetti e metriche, ottenendo una comprensione dettagliata dei modelli comportamentali normali. Questa copertura garantisce la considerazione di una vasta gamma di minacce potenziali e attività anomale, anche minacce e attacchi sconosciuti (0-days).

Adattabilità ai diversi pattern di accesso: ITDR si adatta ai diversi pattern di accesso di utenti o entità adattandosi ai cambiamenti comportamentali nel tempo.

Apprendimento dinamico ed evoluzione: gli algoritmi di analisi comportamentale all'interno di ITDR sono continuamente in fase di apprendimento ed evoluzione, mantenendo il sistema aggiornato con i cambiamenti comportamentali e identificando efficacemente nuove minacce e minacce non viste in precedenza.

IoBs come sensori comportamentali: gli IoBs monitorano le attività per identificare anomalie mappando le tecniche nel framework MITRE ATT&CK, ma potenziandolo con l'apprendimento automatico per rilevare le deviazioni comportamentali.

Correlazione di IoBs per la threat detection: quando le anomalie rilevate da singoli IoB vengono combinate, possono suggerire la presenza di una potenziale minaccia. Ciò fornisce una maggiore precisione e affidabilità nel rilevamento delle minacce e una drastica riduzione dei falsi positivi.

Il modulo ITDR è ulteriormente potenziato con circa 100 IoBs OOTB che coprono la maggior parte delle esigenze di analisi comportamentale nelle grandi organizzazioni. Può generare avvisi o addirittura bloccare l'accesso quando viene rilevato un potenziale takeover dell'account o un'altra minaccia. Inoltre, Sharelock ITDR può monitorare pattern di accesso insoliti, trasferimenti di dati o modifiche nel comportamento dell'utente che potrebbero indicare minacce interne e generare avvisi di conformità quando vengono rilevate potenziali violazioni della conformità normativa.

Le capacità di rilevamento di Sharelock non si limitano agli utenti e agli account; agisce come un sistema di sicurezza intelligente che monitora anche entità non umane e operazioni all'interno di un'organizzazione. Il sistema stabilisce una base per l'attività normale e segnala qualsiasi deviazione che potrebbe indicare problemi di sicurezza, fornendo così una protezione completa contro vari tipi di minacce correlate all'identità.

Esempio di utilizzo reale di Sharelock ISP

Cliente: grande Telco europea
Numero di identità analizzate: 58,000
Numero di indicatori di comportamento configurati: 124
Numero di baseline comportamentali: 1,253,000
Periodo di training: 3 Mesi
Periodo di analisi real-time: 2 Mesi
Numero totale di eventi analizzati: 1.35 Miliardi

La soluzione è stata fornita dal vendor come cluster Kubernetes/Elastic compost da diversi nodi così suddivisi:

- **8 nodi per il cluster database;**
  - 700gb di storage per nodo
  - 24gb di RAM per nodo
  - CPU 12 core per nodo
- **4 nodi (1 master e 3 worker) per il cluster Kubernetes**
  - master 200gb; worker 200gb x3
  - master 24gb di RAM; worker 24gb di RAM x3
  - master CPU 12 core; worker CPU 12 core x3

Sharelock è stato agganciato al tenant Azure di produzione del cliente con lo scopo di collezionare i seguenti log Office365:

- Audit.AzureActiveDirectory;
- Audit.Exchange;
- Audit.SharePoint;
- Audit.General (include i restanti workloads non inclusi nei precedent contenuti);
- DLP.All (eventi relativi a “Data Loss Prevention” per tutti i workloads)

Media giornaliera di Threat rilevati

I dati sono relativi al periodo 01/10/2023 - 31/12/2023

Complessivamente, i risultati del test sul campo indicano che Sharelock ISP ha raggiunto un lodevole equilibrio tra sensibilità e riduzione dei falsi positivi. La capacità del sistema di rilevare e dare priorità alle minacce con precisione, riducendo al minimo i falsi positivi, riflette la sua efficacia nel migliorare la postura della cybersecurity e mitigare efficacemente i rischi di sicurezza. Di conseguenza, questi risultati possono essere considerati come una testimonianza della affidabilità ed efficacia del sistema in scenari di implementazione nel mondo reale.

Sharelock

CONTACT US

learn.sharelock.ai | www.sharelock.ai | info@sharelock.ai