La collaborazione con il team per la sicurezza di Leroy Merlin per analizzare i rischi e definire le priorità

Retail | Milano, Italia

Sfida

- L'implementazione di siti web, app mobili e metodi di pagamento digitale a supporto degli ecommerce ha generato un ampliamento delle superfici di attacco
- I clienti che effettuano acquisti online si espongono alla compromissione di conti finanziari, dati personali e informazioni di pagamento
- Gli attacchi implicano una perdita di ricavi e credibilità per i rivenditori che li subiscono

Soluzione

- Tramite i suoi strumenti di gestione della superficie di attacco, Hadrian ha utilizzato raccoglitori di dati open source e origini di dati passivi per identificare asset precedentemente ignoti a Leroy Merlin
- I test cross-asset hanno analizzato gli asset di vari fornitori di servizi cloud e domini e hanno evidenziato come sono collegati tra di loro
- Il fingerprinting ha contestualizzato gli asset prendendo in considerazione il linguaggio dell'applicazione, la versione e le vulnerabilità in comune
- I dati raccolti sono stati utilizzati per sviluppare dei percorsi di attacco univoci, personalizzati in base alla superficie di attacco di Leroy Merlin
- Hadrian ha collaborato con il team per la sicurezza di Leroy Merlin per analizzare i rischi e definire le priorità in base alle sue esigenze

Informazioni su Leroy Merlin Italia

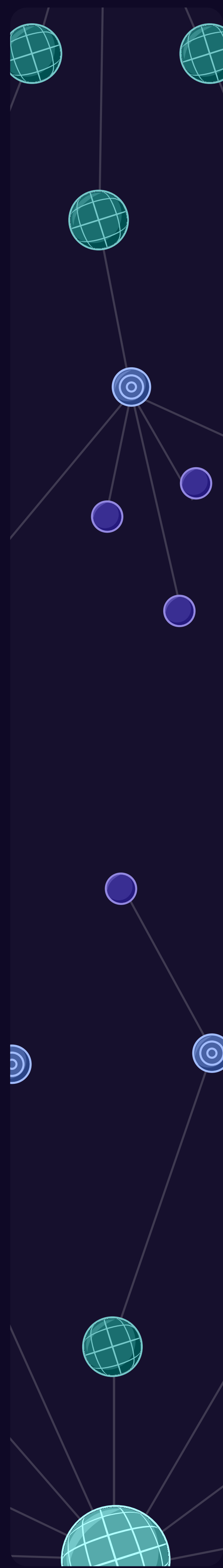
Leroy Merlin Italia è una società del gruppo Adeo con sede nelle vicinanze di Milano, in Italia. È un rivenditore specializzato in articoli per la ristrutturazione domestica e il giardinaggio che serve numerosi paesi in Europa, America del Sud e Africa.

Leroy Merlin annovera 9000+ dipendenti e registra un fatturato annuo di 7,5 miliardi di euro. Nel 2020, Leroy Merlin ha accelerato la sua trasformazione digitale e cloud, sviluppando dei tool per gli acquisti online e un'app.

9000+
Dipendenti

€ 7.5B
Di fatturato annuo

Risultato



Scoprire gli asset dimenticati

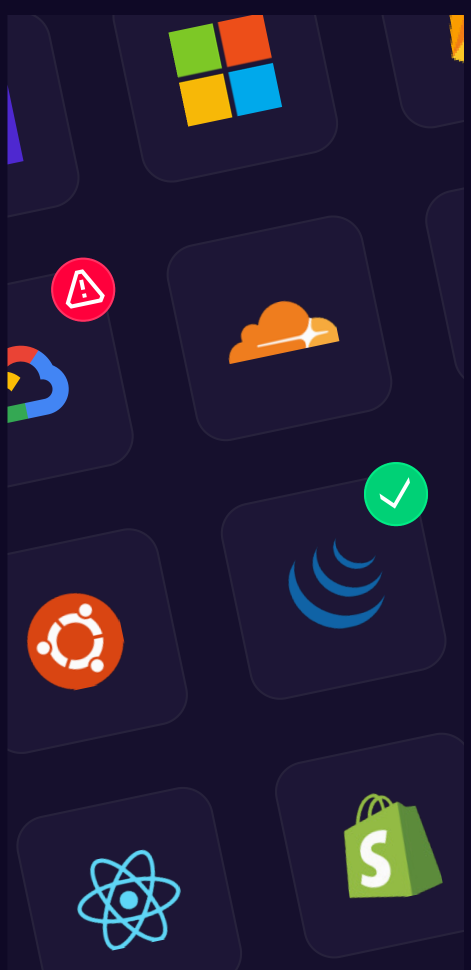
Hadrian ha implementato alcuni strumenti di rilevamento degli asset con un obiettivo ben preciso: identificare gli asset sconosciuti. Nel caso di Leroy Merlin, Hadrian ha utilizzato la sua conoscenza pregressa nell'ambito della sicurezza ecommerce per adottare degli strumenti in grado di monitorare quelle aree in cui la probabilità di contenere asset dimenticati era maggiore. Ad esempio, accade spesso che gli sviluppatori delle app nel settore ecommerce lascino inavvertitamente disponibili le pagine amministratore, consentendo così agli aggressori di accedere a funzioni di amministrazione sensibili. Sulla base di queste conoscenze, Hadrian ha implementato un modulo di hacking volto a identificare le directory/pagine di amministrazione dimenticate.

Hadrian è stato in grado di identificare un endpoint vulnerabile con una pagina di amministrazione non monitorata.

100+
Falsi positivi rimossi

3
Rischi critici identificati

> La piattaforma di Hadrian riesce a identificare le vulnerabilità in modo più profondo rispetto ad altri tool completamente automatizzati. I dati forniti da Hadrian ci hanno aiutato a migliorare l'hardening dei nostri sistemi. Fornisce degli insights davvero eccellenti.
>
> CISO - Leroy Merlin



Sviluppo di test mirati per identificare potenziali violazioni di dati

Quando ha identificato un asset dimenticato o non monitorato, Hadrian ha attinto a informazioni open source e alla propria logica per individuare percorsi di attacco pertinenti. I test mirati hanno permesso a Hadrian di convalidare la sicurezza di Leroy Merlin senza sovraccaricare l'infrastruttura informatica.

Nel caso della pagina di amministrazione non monitorata, Hadrian è riuscito a individuare il test più efficace in base al contesto dell'applicazione, nello specifico il suo linguaggio e il suo framework. Hadrian ha eseguito un test che in più occasioni aveva già messo in luce dei rischi su altri asset con framework simili.

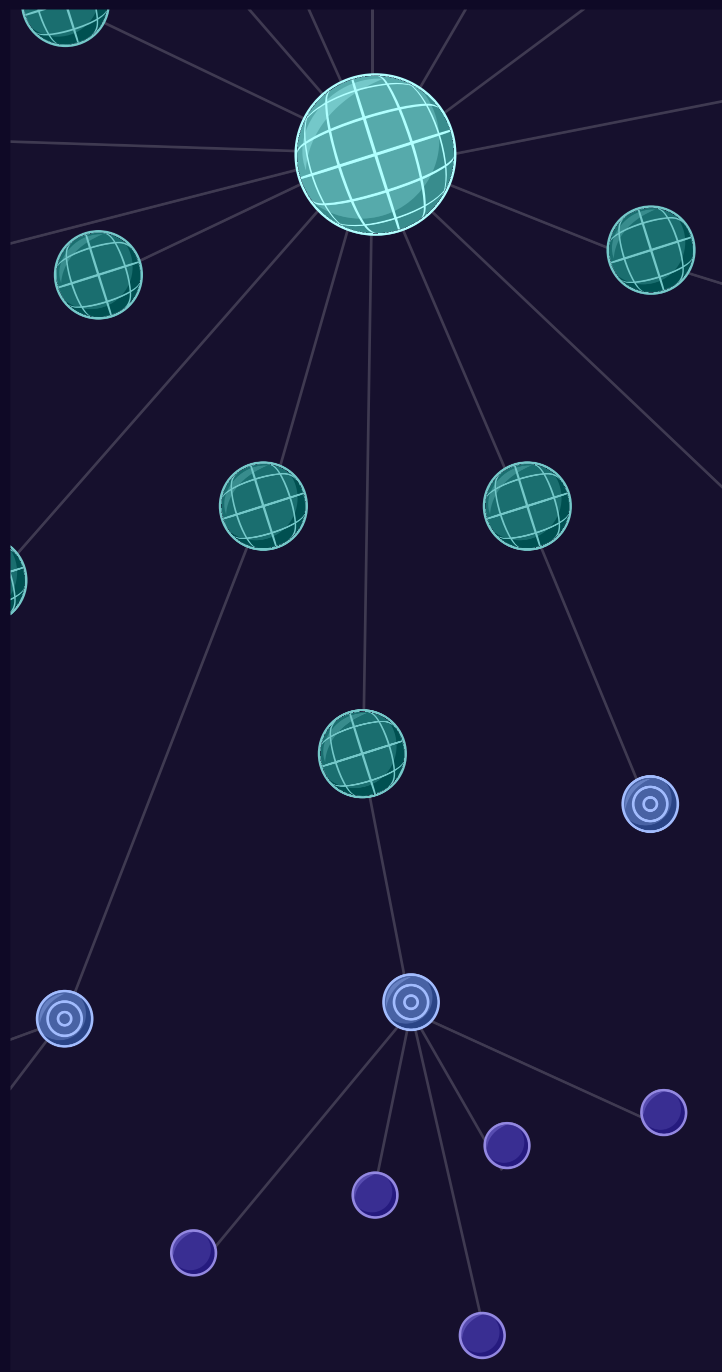
Il test è riuscito a scoprire le credenziali delle password di accesso ai database e di Google Cloud, nonché cookie contenenti informazioni utente sensibili.

La tecnologia basata sugli eventi genera percorsi di attacco complessi

Hadrian è stato creato utilizzando la tecnologia basata sugli eventi. I test basati su eventi consistono nello sferzare attacchi lunghi e complicati che vengono suddivisi in componenti più piccoli e possono essere combinati in varie sequenze per una maggiore flessibilità. Inoltre, si generano nuovi moduli a partire dagli insights raccolti tramite test precedenti; si tratta pertanto di una metodologia di test estremamente adattabile.

I componenti più piccoli consentono ad Hadrian di adattarsi di pari passo con l'emergere di nuovi dati. Ad esempio, quando Hadrian ha scoperto i cookie nella pagina di amministrazione, ha attivato uno strumento di hacking. Lo strumento di hacking ha utilizzato i cookie per ottenere l'accesso agli account contenenti le informazioni sensibili sull'azienda e sui clienti.

Hadrian continuerà a raccogliere dati e a implementare test in risposta a qualunque cambiamento nella superficie di attacco di Leroy Merlin.



Scopri di prima mano la piattaforma con una demo rapida di 15 minuti

Basta che ci comunichi il tuo dominio e il nostro sistema inizierà a scansionare autonomamente la tua superficie di attacco.

Prenota una demo

Scopri di più