bitCorp™

ZADIG: L'INASPETTATO INVESTIGATORE DI CYBERSECURITY

- Milano, 28 giugno 2021

INDICE

INTRODUZIONE

Rilevare un incidente di sicurezza[1] e tramutarlo in barriera inespugnabile è di fondamentale importanza per aziende, privati e istituzioni. La rete[2] si configura come un ambiente di proliferazione di pericoli che possono mettere a serio rischio ogni attività legata ad essa. Pensando a un sistema in grado di monitorare, rilevare e risolvere l'attacco[3], bitCorp srl ha creato il prodotto Zadig.

Ispirato alle disavventure del celebre personaggio di Voltaire, Zadig è molto più di un eroe che vive in un Oriente di fantasia: è un progetto reale, costruito da persone reali. Strettamente legato al Cyber Security Operation Center, questo sistema è in grado di scagliarsi contro l'intero flusso di traffico con intelligenze artificiali costruite ad-hoc, al fine di rilevare minacce complesse ed istruite tramite supervised Machine Learning.

LA CYBERSECURITY DI ZADIG E IL SISTEMA IDS: LE DIFFERENZE

Nell'ambito della sicurezza informatica, un sistema IDS[4] traduce l'espressione Intrusion Detection System. Si tratta di una combinazione di elementi hardware e software configurati al fine di identificare accessi non autorizzati ad una rete o ad un computer locale. Generalmente, questo sistema si avvale della professionalità di cracker esperti che sanno rilevare le vulnerabilità ed intervenire per tempo. La struttura di un IDS si compone di quattro diversi elementi:

- **una sonda**, o anche più, deputato alla ricezione di informazioni dalla rete,
- **un software di analisi** che individua eventuali falle di sistema,
- **una console di monitoraggio** che gestisce avvisi e interventi,
- **un database di archiviazione** nel quale viene tracciata una sintesi di ciò che è stato rilevato.

Si tratta, in definitiva, di un sistema costruito sulle concrete esigenze del singolo caso che può avere risvolti più o meno evoluti a seconda di quanta Intelligenza Artificiale (AI) venga utilizzata al suo interno.

Zadig rappresenta la versione più moderna e avanzata di un classico IDS, grazie ad un apparato di tecnologie di machine learning[5] in grado di apprendere progressivamente le caratteristiche peculiari della rete in cui opera. L'eccellenza di questo prodotto di cybersecurity risiede in un doppio canale di cyber – situational – awareness, nel quale si innestano le formule più avanzate di AI unitamente ad un personale tecnico dalle competenze estremamente raffinate ed evolute.

[1] https://www.matika.it/incidente-di-sicurezza-data-breach-differenza/#:~:text=Un%20incidente%20di%20sicurezza%20delle%20informazioni%20pu%C3%B2%20essere%20causato%20da,delle%20informazioni%20sensibili%20dell'azienda.

[2] https://itmanager.space/cosa-sono-e-quali-sono-le-reti-informatiche/

[3] https://it.wikipedia.org/wiki/Attacco_informatico#:~:text=Un%20attacco%20informatico%2C%20nell'ambito,alterazione%20o%20distruzione%20di%20specific

[4] https://en.wikipedia.org/wiki/Intrusion_detection_system

[5] https://venturebeat.com/2021/06/21/machine-learnings-rise-applications-and-challenges/

LA STRUTTURA DELLA CYBERSECURITY DI ZADIG

La soluzione di cybersecurity che si ottiene con Zadig è nata per essere versatile e adattarsi a qualunque tipo di infrastruttura a disposizione del cliente. Il sistema si compone di un software di tipo SaaS, Software As A Service, in formula back-end. I vantaggi di questo modello sono così riassumibili:

- consente un facile accesso ad applicazioni molto sofisticate,
- permette un'ottima scalabilità in base al livello d'uso,
- spesso non richiede alcuna configurazione,
- garantisce una totale mobilità di dati tra tutti i dispositivi autorizzati,
- lavora spesso in cloud sicuri ai quali si può accedere da qualunque luogo.

Con Zadig, dal prodotto in logica SaaS si può chiedere di integrare qualsiasi interfaccia applicativa già esistente. Questa versatilità lo trasforma in un PaaS per soluzioni altamente custom di cybersecurity.

PERCHÉ PREFERIRE LA CYBERSECURITY DI ZADIG

Ogni elemento della struttura di Zadig è pensato per funzionare ovunque lo si desideri. Già in uso presso le istituzioni nazionali di polizia e intelligence, e in numerose aziende private, esso permette di ottenere risultati notevoli:

- la necessaria struttura hardware è inclusa nel servizio,
- richiede ingombri minimi e nessuna installazione complessa,
- riduce i costi di implementazione di sistemi realizzati in locale,
- è customizzabile per qualunque realtà d'uso, si integra perfettamente con altri sistemi IDS eventualmente presenti.

L'elenco dei vantaggi di Zadig sintetizza i punti di forza di un prodotto nato per non avere competitor in fatto di cybersecurity. La squadra di esperti che lo ha realizzato proviene da due altissimi livelli di specializzazione: l'attacco informatico e la sua difesa. La conoscenza profonda di entrambi i settori ha permesso di conoscere le due facce della stessa medaglia, realizzando così un prodotto completo al servizio di chi vuole difendersi davvero dalle insidie della rete.

ZADIG È UN SISTEMA DI CYBERSECURITY CHE CONTROLLA A 360°

La maggior parte dei servizi di cybersecurity sul mercato si preoccupa di identificare le falle di sistema ed intervenire di conseguenza. Zadig fa molto più di questo: oltre ad analizzare, monitorare e gestire eventi di attacco informatico, è potenzialmente in grado di rilevare ulteriori anomalie, a fronte delle dovute integrazioni. All'interno di contesti aziendali molto complessi, ad esempio, il sistema è impostabile per registrare ulteriori stranezze:

- negligenze,
- infedeltà aziendali,
- guasti di impianti,
- perdite di dati
- e qualunque altra azione, o evento, che possa minare la sicurezza della struttura in cui opera.

Questo aspetto riduce notevolmente i costi di un doppio canale di controllo da implementare altrimenti all'interno del contesto lavorativo. In altre parole, Zadig è una piattaforma di sicurezza enterprise che risponde a qualunque esigenza di monitoraggio gestita da canali elettrici o elettronici.

ZADIG: IL TEAM E I RICONOSCIMENTI

La paternità di Zadig si attribuisce ad un team di esperti che ha profuso il suo impegno nella costruzione di un doppio versante di specializzazione: l'attacco e la difesa. I colori che rappresentano simbolicamente bitCorp srl sono il rosso e il blue.

Il Red Team è il nome della squadra d'attacco esperta in sistemi di irruzione nelle architetture di difesa altrui. Il Blue Team, invece, e il nome dei professionisti della difesa, responsabili della manutenzione interna della rete e della sua difesa da minacce esterne.
Nel 2020 Zadig si traduce in un riconoscimento per bitCorp: la vittoria ufficiale del bando di Startup Milano.

Se vuoi sapere di più su questo prodotto o avere una consulenza gratuita di cybersecurity contattaci per un consulto ad hoc. Noi di bitCorp saremo lieti di darti una mano!