zadig™

bitCorp™

Zadig™

La soluzione integrata di cybersecurity per medie e grandi imprese.

ZADIG è una soluzione all-in-one formata da:

- **sistema IDS-IPS arricchito da modelli di Intelligenza Artificiale proprietari e customizzabili**
- **protezione centralizzata end point (HIDS) multipiattaforma**
- **integrazione dati tipicamente afferibili a sistemi SIEM**

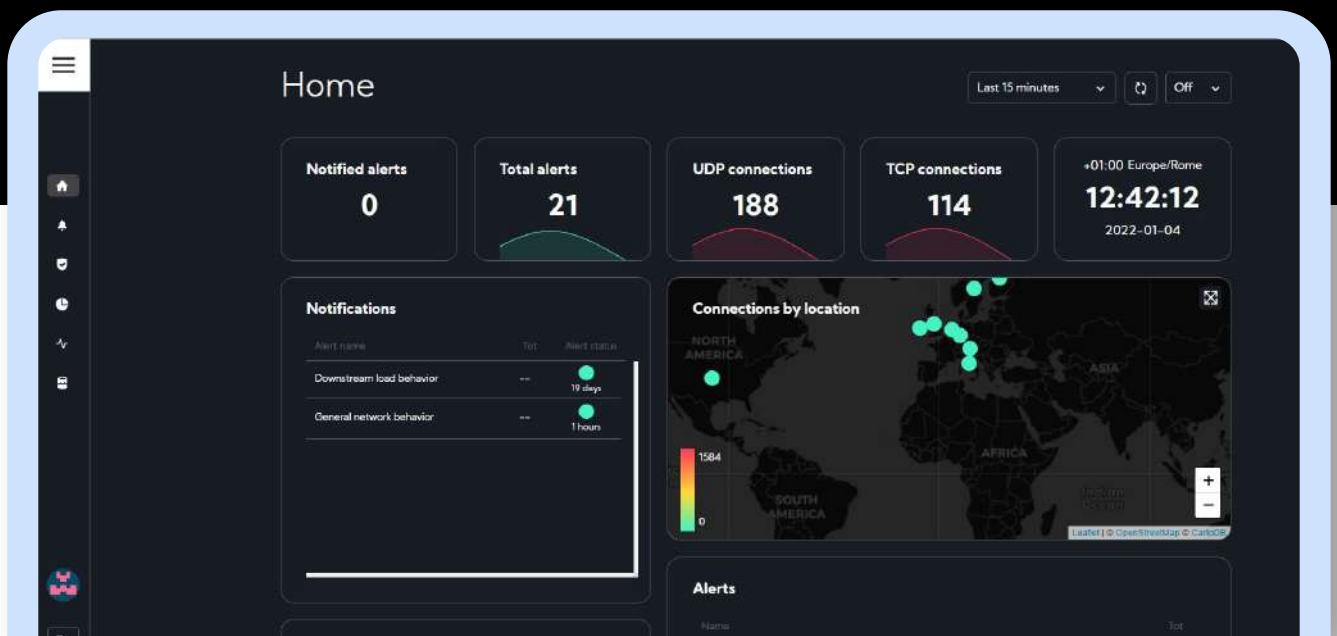
La versatilità di ZADIG consente di potere acquistare la soluzione in forma completa oppure per singole funzionalità, integrando ogni componente con eventuali sistemi di sicurezza già in uso.

IDS - IPS

L'IDS-IPS di ZADIG è un sistema integrato in grado di monitorare la rete inviando alert per attività sospette (IDS) e di intervenire per bloccare l'invio/ricezione di pacchetti in funzione del loro contenuto (IPS).

Il monitoraggio avviene sia su base signature che behavioral. Grazie a quest'ultima funzione – realizzata attraverso modelli di apprendimento artificiale – **ZADIG non solo identifica e neutralizza minacce note, ma è anche in grado di comprendere se vi sia un attacco in corso interpretando anomalie nel regolare comportamento dell'infrastruttura monitorata.** Funzionalità utile perché si adatta al mutamento delle condizioni in cui opera, quali l'aumento delle dimensioni o delle caratteristiche dell'infrastruttura del cliente.

Zadig, oltre ad avvalersi di un potente sistema di pattern matching su signature (ovvero un riconoscimento byte per byte di impronte riconoscibili e note), consente anche, grazie ad un linguaggio di scripting Turing-completo ad eventi specifico, di manipolare i pacchetti di rete per adeguarsi nel modo più efficace alle discrepanze di matching eventualmente esistenti sull'infrastruttura del cliente, realizzando quindi una soluzione di protezione ad-hoc ai massimi livelli di efficienza ed efficacia.

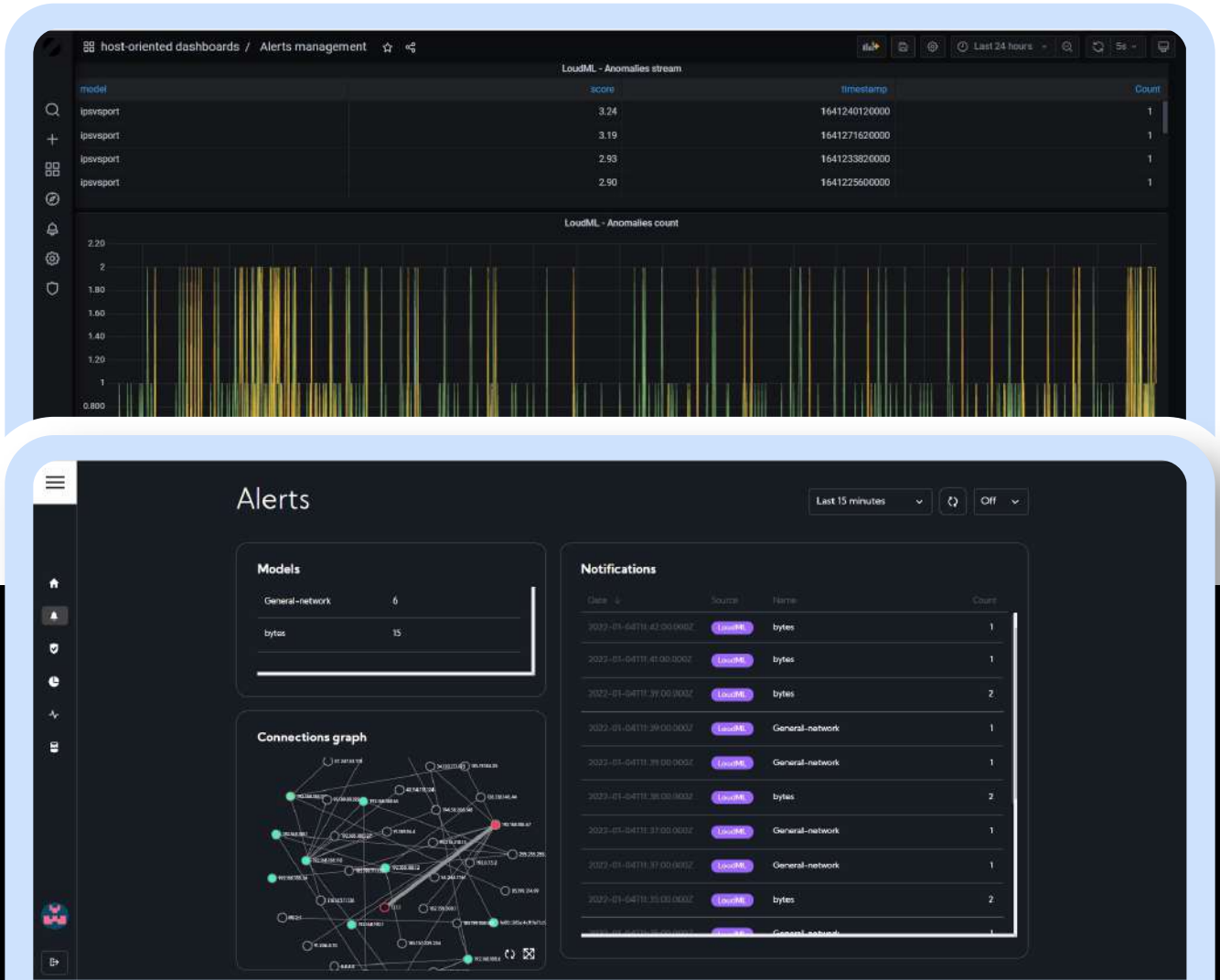


Questo aspetto riveste particolare importanza nel caso, ad esempio, di ambienti software obsoleti, quindi non più aggiornabili oppure adattati con specifici layer di integrazione che, proprio per le specifiche di deployment adottate dal cliente, possono presentare vulnerabilità anche ad alto rischio di attacco e non risolvibili dai fornitori.

Unitamente a modelli standardizzati inclusi in ZADIG, sono proposti, di concerto con il cliente, soluzioni ad-hoc adeguate alla tipologia di rete, al tipo di utilizzo che ne viene fatto o ai processi produttivi che caratterizzano il settore in cui opera il cliente.

Ciò è reso possibile grazie all'attività di osservazione e monitoraggio della rete e delle modalità con cui essa viene utilizzata. Verranno quindi implementati sia modelli automatizzati che regole, per così dire, "scritte a mano" in funzione della tipologia di utilizzo osservata.

l' IDS-IPS di ZADIG si alimenta anche grazie a un insieme di feed mantenuti e distribuiti da comunità open source ad ulteriore garanzia di aggiornamento costante contro le tecniche di attacco più recenti sfruttate dagli attaccanti.

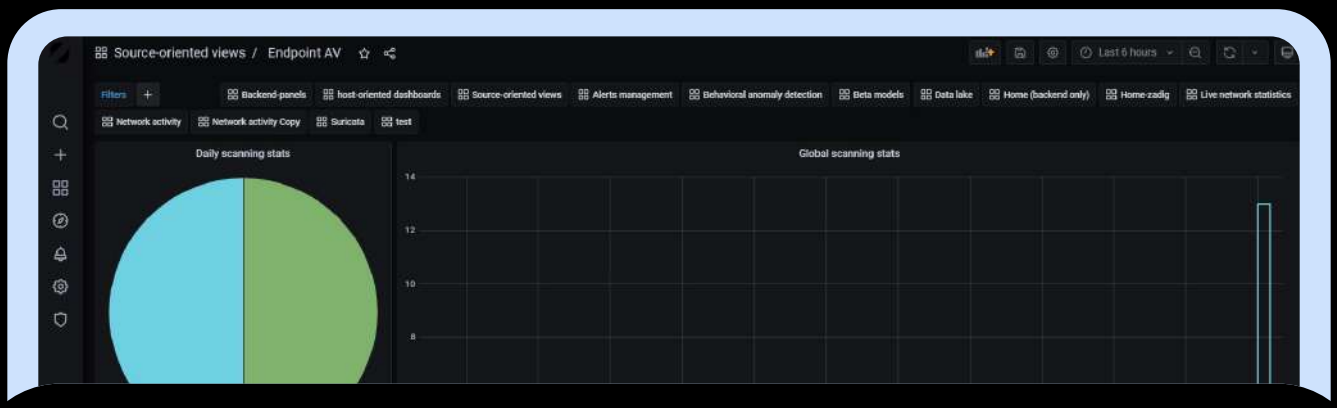


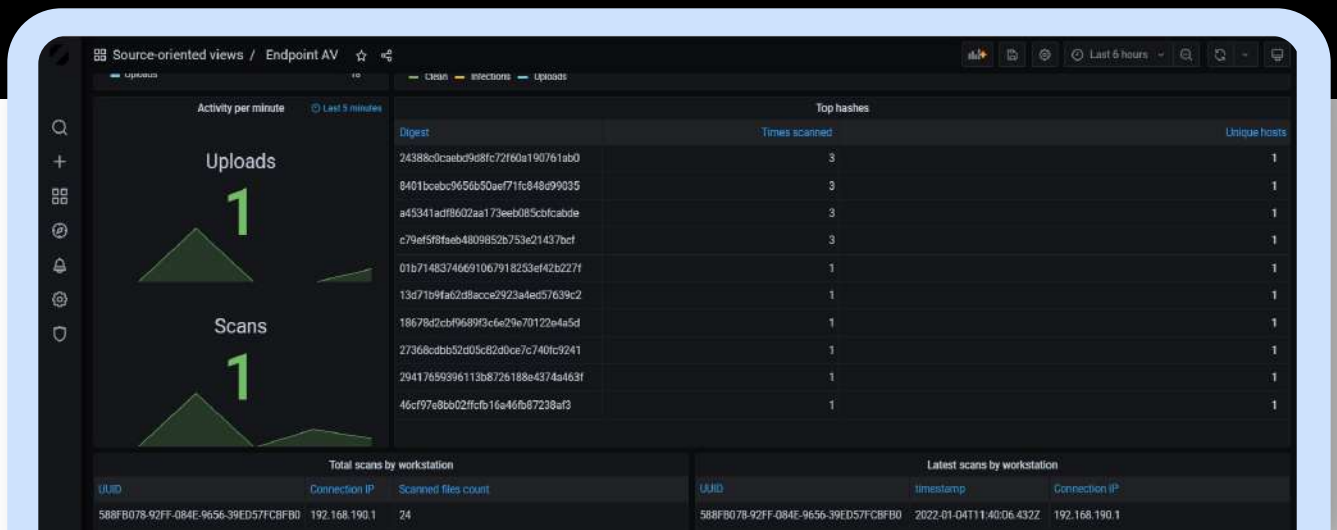
End Point management and protection

ZADIG offre anche funzioni HIPS (Host-based Intrusion Prevention System).

Ciò significa che è in grado di estendere il proprio scudo protettivo a ciascun endpoint presente nella rete monitorata (PC, server, NAS, ecc.) grazie ad una scansione continua e ad un monitoraggio di filesystem, processi e molto altro con API centralizzata che aggrega i dati raccolti e fornisce funzionalità di intelligenza artificiale per identificare ed intervenire su comportamenti anomali di natura sospetta.

ZADIG in questo modo sostituisce di fatto le tipiche funzionalità di un prodotto antivirus professionale: l'IDS identifica una minaccia sull'endpoint e l'IPS interviene neutralizzando ogni tentativo di diffusione nella rete, ad esempio isolando la macchina infettata.

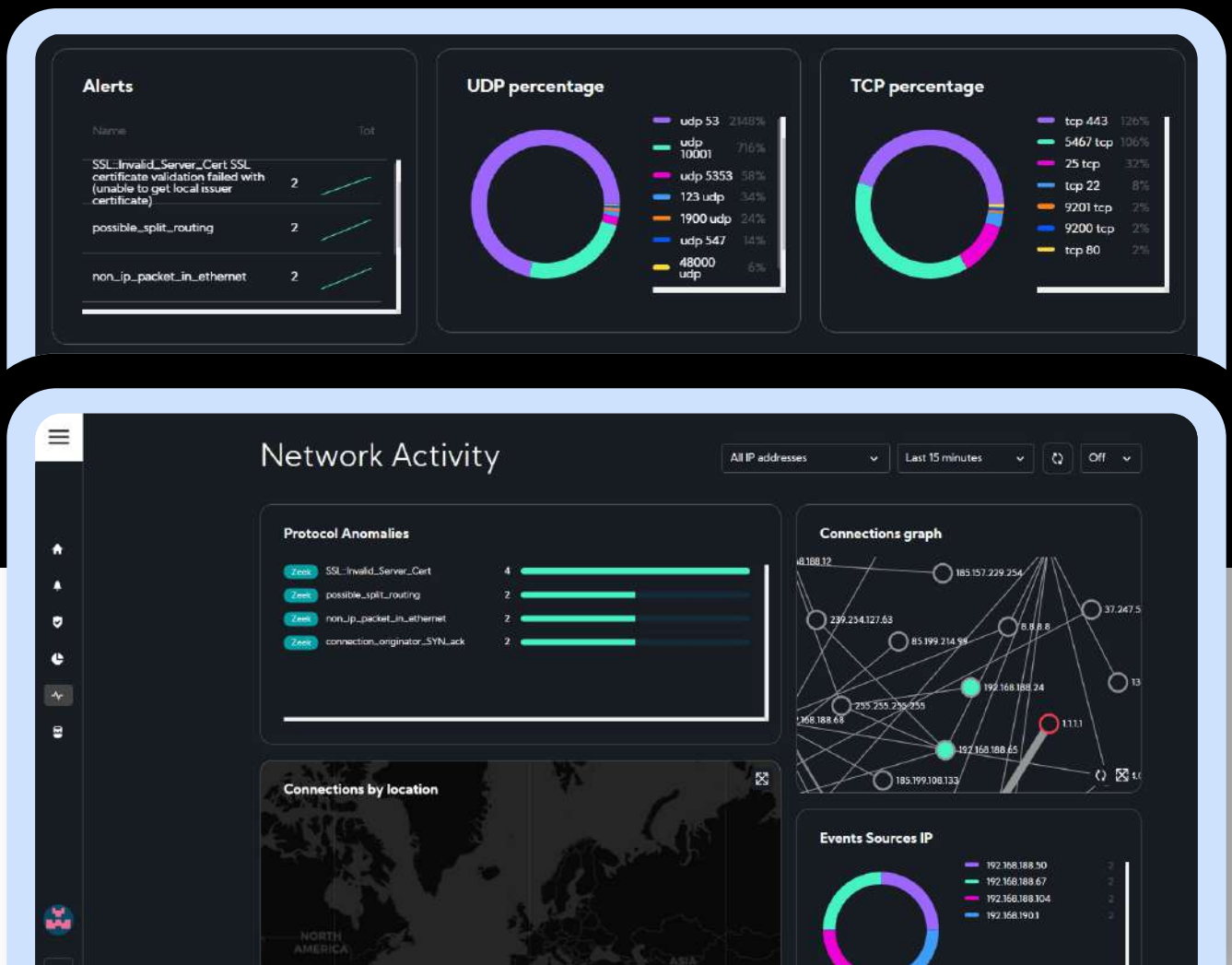




Integrazione con IoT

La versatilità di ZADIG consente di estendere le proprie capacità di monitoraggio e analisi a qualsiasi sistema dotato di sensori, quali la tecnologia IoT.

ZADIG è infatti in grado di analizzare qualsiasi tipo di dato in input: è quindi sufficiente immaginare al posto di un PC un qualsiasi sistema basato su telemetria o sensoristica per avere un monitoraggio efficace di qualunque impianto basato su IoT, quali smart building, smart wasting, ecc.



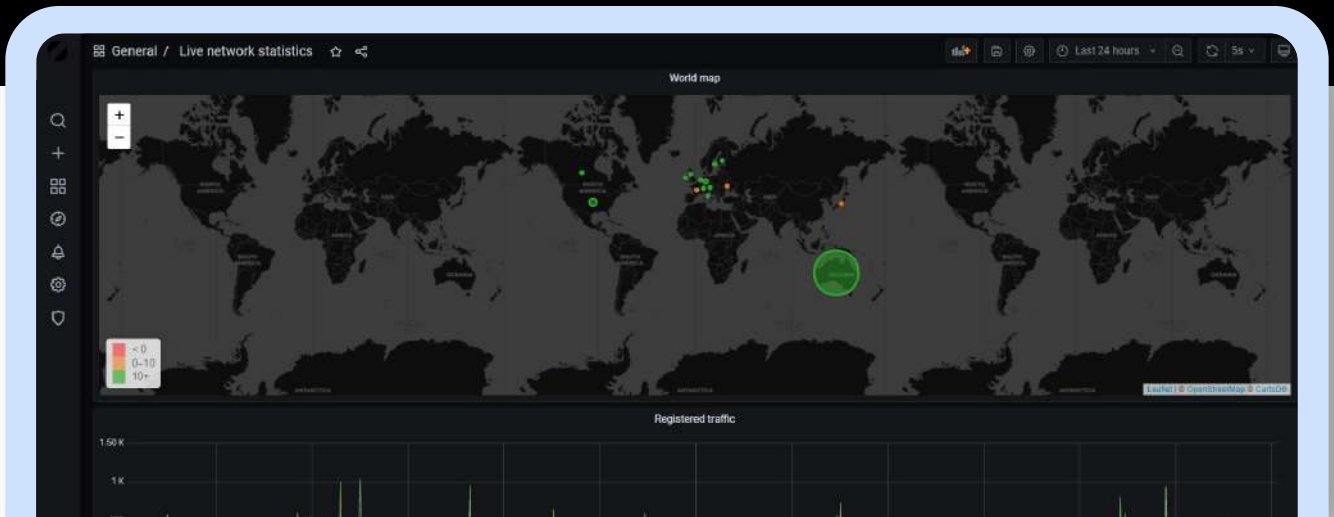
Log Aggregation and Analytics

I dati di log raccolti da ZADIG confluiscono in un sistema di gestione e analisi che, grazie ad un avanzatissimo hardware dotato di NIC fino a 10Gbit/sec di traffico (equivalente a circa l'informazione in transito per 625 streaming video 4K HDR compressi e trasmessi simultaneamente dalle più note piattaforme) proveniente da una mirror port di uno o più switch, effettua correlazioni tra le varie fonti dati alla ricerca di eventi rilevanti.

Inoltre, grazie alla sua grande scalabilità è possibile coordinare l'afflusso di dati provenienti da diverse sottoreti sulla medesima sede mantenendo un unico concentratore di informazioni.

Il sistema di Log Aggregation and Analytics di ZADIG consente di analizzare dati provenienti da diversi tipi di fonti ed è dotato di una dashboard di controllo che consente all'utente di interagire in modo veloce e intuitivo con tutte le informazioni che le funzionalità di ZADIG producono, tra cui eventi di incident management, threat intelligence feeds, telemetrie, error reporting, ecc.

Anche le policy di log retention sono naturalmente personalizzabile in funzione delle necessità e disponibilità di archiviazione del singolo cliente.



Remediation

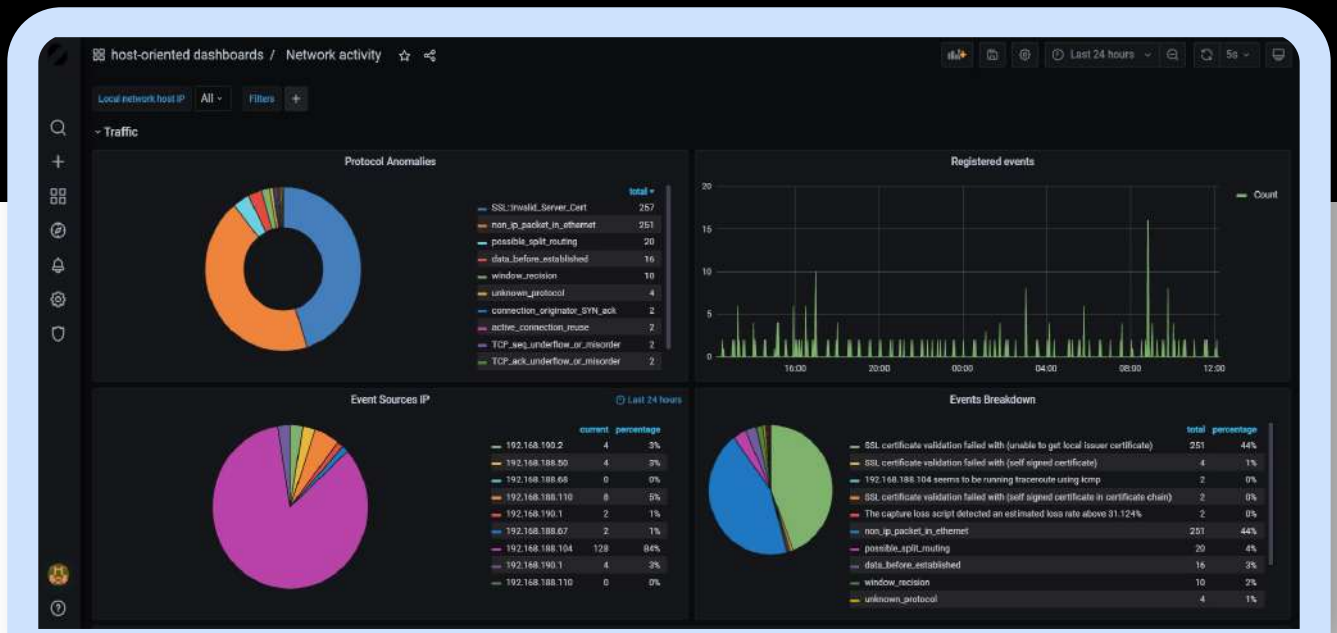
L'attività dell'IPS di ZADIG trova la sua ragion d'essere nella neutralizzazione di ogni minaccia.

La remediation può essere automatizzata (ad esempio isolando la macchina eventualmente infettata ed attivando il recupero dei dati alla versione precedente l'attacco) oppure personalizzata in funzione delle esigenze del singolo utente.

Gli alert vengono condivisi ai vari sistemi mediante un'ampia serie di canali di comunicazione scelti dal cliente in base alle possibili integrazioni, tra cui e-mail, piattaforme di instant messaging o altri di tipo M2M come webhook.

Dopo eventuali attività ostili, gli analisti di bitCorp possono essere ingaggiati per realizzare una serie di attività, quali:

- **generazione di regole di protezione ad hoc**
- **controllo integrità dati e log**
- **report e ripristino di sistemi in quarantena**



Reale innovazione

ZADIG è il frutto della ricerca reale e costante effettuata da bitCorp. Una ricerca che parte dalla conoscenza aggiornata delle metodologie di attacchi informatici, anche le più sofisticate e recenti.

Prevenzione ransomware integrata

ZADIG consente di prevenire e proteggerti contro la più frequente minaccia informatica, il "Ransomware", grazie ad un sistema proprietario in grado di individuare gli atti preparatori con cui viene realizzato questo genere di attacco.

L'integrabilità degli alert prodotti da ZADIG con sistemi di back-up e recovery consente di implementare processi di recupero automatizzato di ogni tipo di storage dati allo stato immediatamente precedente al tentativo di attacco.

Modellazione A.I. in-house

Ogni modello di intelligenza artificiale impiegato da ZADIG è realizzato direttamente da bitCorp. A seconda delle esigenze realizziamo modelli e script ad-hoc per rispondere in maniera efficace ad ogni peculiarità dell'asset da proteggere.

Remediation personalizzata

ZADIG non propone un modello standard di remediation, ma opera secondo i criteri e processi stabiliti dal cliente.

Basta falsi allarmi

Oltre ad impiegare metodologie standard per limitare i falsi positivi, come i playbook di Splunk, bitCorp possiede algoritmi proprietari di hierarchical-clustering e PAM-clustering che aiutano a ridurre l'emissione di allarmi falsi positivi in modo automatico.

In aggiunta, anche gli operatori possono modificare le soglie di allerta, qualora necessario, per personalizzare i profili sulla base delle specifiche, dei tratti caratteristici e della natura della rete.

Integrazione con sistemi IoT

La capacità di ZADIG di analizzare qualsiasi tipo di dato consente di sfruttarne le potenzialità di monitoraggio integrando fonti provenienti da qualunque infrastruttura dotata di sensoristica e telemetria.

Un impiego adatto per progetti smart building, smart wasting, smart lighting, ecc.

Dashboard personalizzabile

La dashboard di consultazione dei dati disponibili alla Log Aggregation and Analytics di ZADIG è modificabile in funzione delle esigenze del cliente e del tipo di query che si rendono necessarie.

Zadig™ small business

L'offerta ZADIG comprende l'abbinamento GRATUITO di ZADIG small business, il nostro sistema di cybersec multifunzione, che comprende un'ampia gamma di funzionalità tra cui

WI-FI Access Point Enterprise Protection

Monitoraggio del traffico generato attraverso la rete Wi-Fi aziendale mediante la fornitura (anche multi-pla) di access point professionali con configurazioni personalizzate.

VPN Safe Smart Working & VPN Site2Site

Installazione di VPN implementate da bitCorp per l'accesso in remoto alla rete aziendale e garantire l'accesso sicuro e protetto in caso di smart working, anche su più sedi.

Integrated Back-up Solution by Microsoft

Microsoft Partner

Microsoft

Sistema di recovery basato sul back-up dei file in combinazione con policies e strumenti di produttività in modalità cloud, per garantire sempre la disponibili-tà dei dati e il business continuity in caso di tentativo di attacco.

Zadig™ small business

DMZ for a safe e-commerce

Realizzazione di una o più DMZ su sotto reti isolate nel caso in cui il cliente abbia la necessità di esporre macchine, come nel caso di siti web interattivi.

AD-Blocker centralizzato

Grazie al sistema di AD BLOCKER integrato, ZADIG blocca direttamente alla frontiera qualunque tipo di interferenza con la normale user experience.

Gestione Domini

Grazie al controller di dominio di Active Directory, ZADIG è in grado di estendere automaticamente i servizi inclusi nell'offerta a tutti i nuovi utenti aggiungi al dominio.

About us

Microsoft Partner
Microsoft

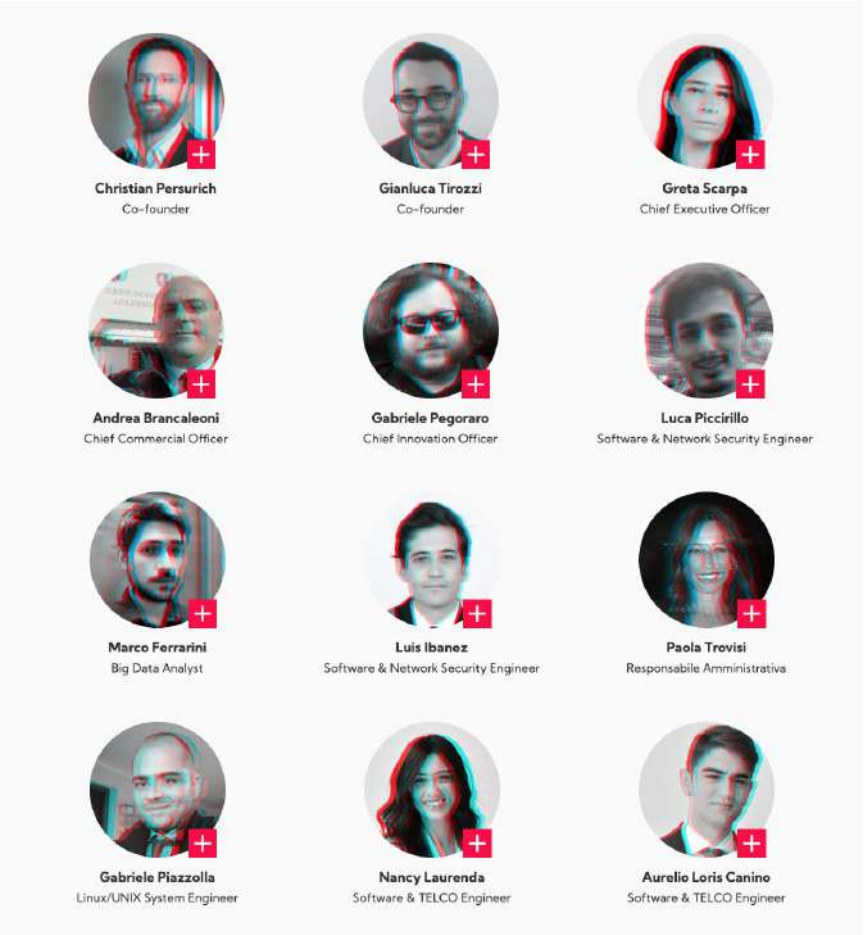
IBM PartnerWorld

vmware PARTNER
TECHNOLOGY ALLIANCE

BITCORP opera con tecnologia esclusivamente made in Italy nel mercato del cyber intelligence, cyber security e smart living, realizzando soluzioni su misura per le esigenze di clienti istituzionali e corporate.

Un Intelligence Creative Lab in grado di interpretare le singole esigenze e fornire le soluzioni più efficaci sia di natura offensiva che difensiva, principalmente nel settore IT e Telco, ma non solo.

Team



Nata dall'unione di professionalità del mondo dell'intelligence istituzionale e dell'ethical hacking, BITCORP è l'esempio di efficace sinergia tra la componente di Human Intelligence (HUMINT) e quella di Technical Intelligence (TECHINT).

Il core business si sviluppa offrendo soluzioni innovative ad alto contenuto tecnologico per il mercato della Lawful Interception e della Sicurezza Informatica.

bitCorp™

Sede legale
via Monte Bianco 2/A, 20149 – Milano

Sede di Milano
Galleria del Corso 4, 20121 – Milano

Sede di Roma
via Ludovisi 16, 00187 – Roma

Sede di Madrid
Moreno Nieto 7, Piso Bajo, letra B, 28005 – Madrid

www.bitcorp.it