bitCorp™

bitLex

I servizi di bitCorp destinati al mercato LegalTech

bitLex

La rivoluzione tecnologica in atto in tutte le realtà produttive sta portando ad un'evoluzione radicale dell'approccio degli studi legali nel percorso di accompagnamento dei propri clienti verso la cosiddetta "digitalizzazione".

Competenze legali e tecniche sono due facce della stessa medaglia, laddove lo scopo non sia solo quello di un adeguamento formale alla normativa, ma sostanziale rispetto ai rischi di attacchi informatici e furto di dati.

BitCorp, nata dalla fusione di ex appartenenti al comparto dell'Intelligence istituzionale ed ethical hackers, si pone come partner strategico di studi legali offrendo un pacchetto di soluzioni specificatamente studiato per le esigenze del mercato legal:, dalla consulenza, ai servizi, ai prodotti.

In una parola: **b**

Cyber Audit

L'obiettivo è **fungere da supporto tecnico/operativo alla realizzazione non solo di tutte quelle attività di verifica, necessarie alla compliance con la normativa vigente (GDPR), ma anche di quelle che consentono di avere un quadro realistico del livello di sicurezza delle infrastrutture e dei processi del cliente** allo scopo di fornire soluzioni efficaci ed economicamente vantaggiose alle vulnerabilità riscontrate.

In tale quadro si predispongono una serie di interventi tra cui:

- **realizzazione di questionari mirati;**
- **interviste;**
- **acquisizione di documentazione tecnica (asset informatici presenti, prodotti, architettura di rete, configurazioni, policy di sicurezza e accessi, disaster recovery, ecc.).**

Pentesting
Vulnerability & Assessment

L'evoluzione del punto precedente presuppone, a seconda delle circostanze, **la possibilità di testare sul campo le reali condizioni di sicurezza dell'infrastruttura del cliente, attraverso una serie di attività concordate di natura standard** (verifica vulnerabilità note; individuazione grosse falle o misconfigurazioni macroscopiche) **o approfondita** (bug; vulnerabilità e security hole; punti deboli nella progettazione della rete, nei firewall/router o negli script dei webserver; errori nella configurazione dei principali servizi in esecuzione; problemi relativi l'accesso fisico alle machine; ecc.).

Pentesting base

- Verifica vulnerabilità note
- Grosse falle
- Errate configurazioni

Pentesting medio

- Bug, vulnerabilità e security hole nel software presente
- Punti deboli nella progettazione della rete
- Punti deboli di firewall e router
- Punti deboli negli script dei web-server
- Errori nella configurazione dei principali servizi in esecuzione
- Problemi relativi l'accesso fisico alle macchine

Pentesting avanzato

- Verifica dei "sorgente" dei programmi
- Verifica di nuove vulnerabilità sui programmi

Secure
by design assessment

Attività di verifica del livello di sicurezza con cui sono stati realizzati i prodotti dei vostri clienti o dei loro fornitori.

L'utilizzo sempre più massivo di fornitori di big data per scopi commerciali può infatti rappresentare un serio pericolo per i vostri clienti, in caso di data breach, non solo per l'eventuale furto di dati, ma anche per la loro reputazione ed avere ricadute negative in termini di fiducia.

BitCorp esegue attività di verifica sul reale stato della sicurezza nella gestione di questi dati da parte dei fornitori dei vostri clienti mediante metodologie compliance con gli attuali standard internazionali, quali:

- **Open Web Application Cycle (OWASP)**
- **Secure Software Development Life Cycle (SSDLC)**
- **Information Risk AssessmentMethodology2 (IRAM2)**
- **Common Criteria for IT Security Evaluation**

Forensics Investigations

Attività di investigazione finalizzata alla ricostruzione della catena degli eventi, alla cristallizzazione delle fonti di prova e, ove possibile, all'individuazione delle responsabilità di un attacco di tipo criminale.

Attività che viene effettuata da tecnici bitCorp iscritti come CTU in Albi presso le principali Procure della Repubblica e Tribunali nazionali e supervisionata dai soci fondatori di bitCorp, ex ufficiali di Polizia Giudiziaria **con esperienza ultraventennale in attività investigative di alto profilo.**

Training

Un'attenzione particolare è dedicata all'anello debole di qualunque struttura di cybersecurity: l'elemento umano.

Anche i prodotti più sofisticati, infatti, possono vedere compromessa la loro efficacia a causa di comportamenti negligenti o superficiali di coloro i quali operano su tali sistemi.

BitCorp è ente formatore per la Pubblica Amministrazione (Amministrazione della Difesa) e dispone delle principali certificazioni tra cui:

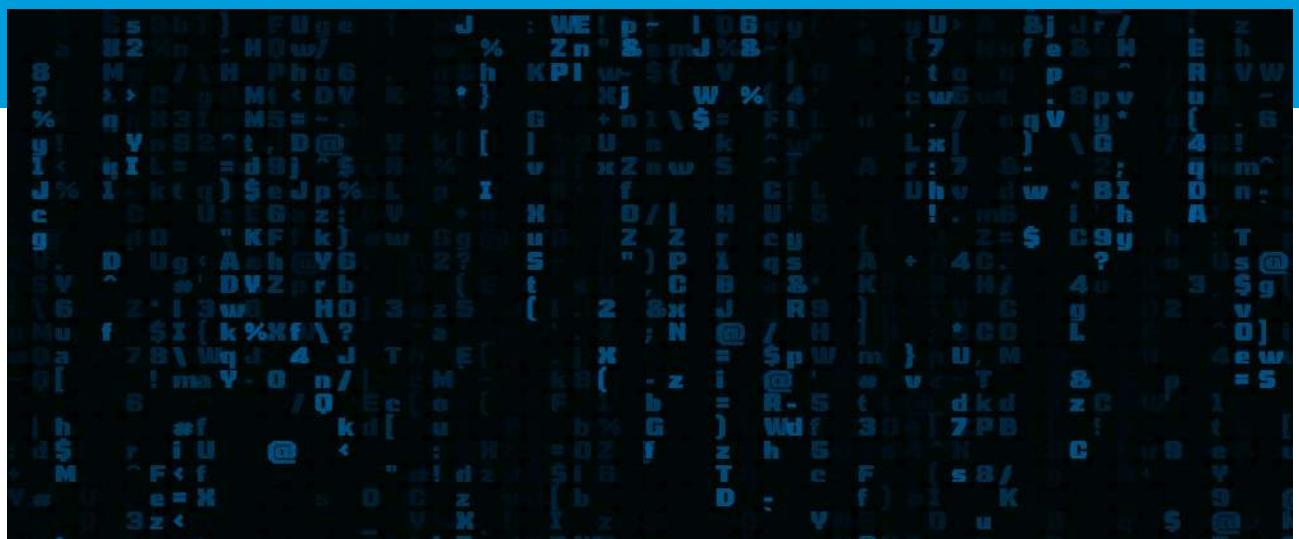
- **Offensive Security Certified Professional (OSCP);**
- **Certified Ethical Hacker (CEH).**

Sistemi di Cifratura

Sistemi di Crittografia Simmetrica (AES) ed Asimmetrica (RSA) impiegati su nostre piattaforme ad hoc per:

- **Creazione di dischi virtuali di qualsiasi dimensione criptati in hardware (AES 256 CBC);**
- **Dischi virtuali condivisibili tramite P.a.a.S. Cloud o Edge;**
- **I dati residenti localmente sul proprio dispositivo come cartella con file completamente criptati;**
- **Il volume virtuale viene montato come unità disco solo quando il dispositivo lo mostra e lo decripta;**
- **Configurazione per la generazione punti di ripristino automatici (Backup e Cronologia);**
- **Mount dei dischi nella loro versione storica (Punti di Ripristino).**

Questo tipo di soluzioni sono particolarmente utili per garantire la tutela del segreto industriale senza dovere ricorrere a costosi brevetti.



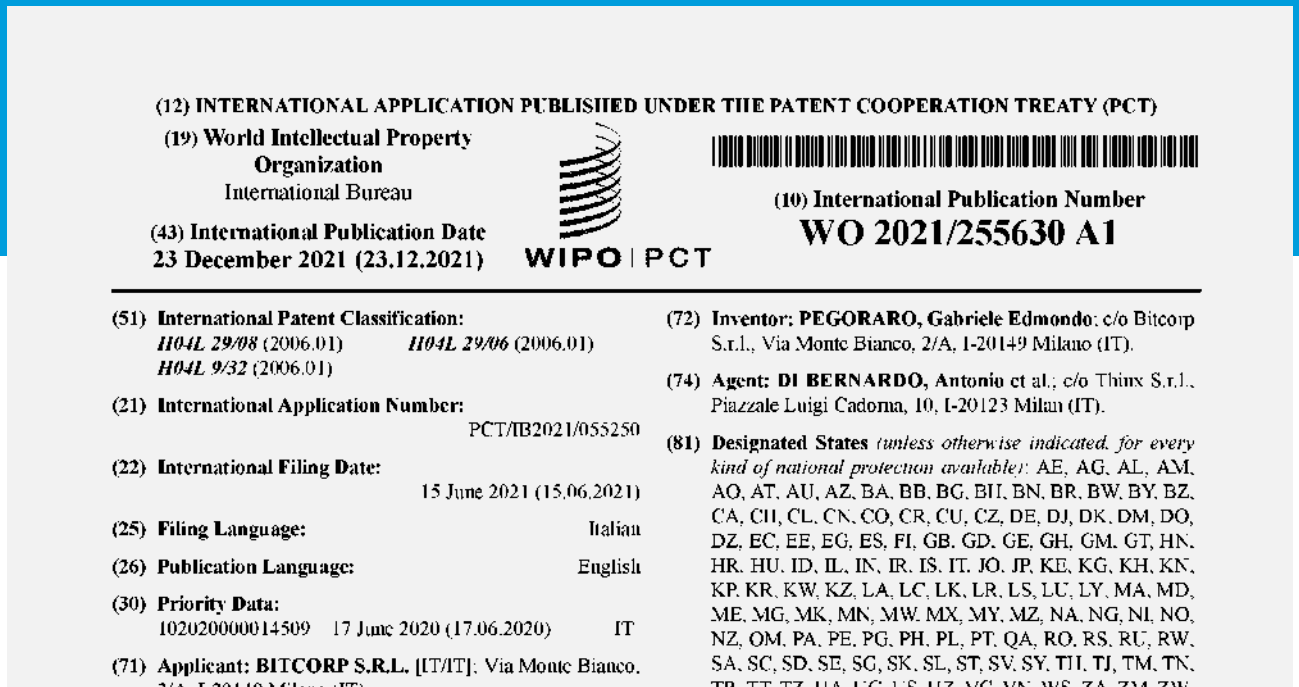
Blockchain

Smart contract & token

BitCorp ha depositato diversi brevetti per l'applicazione della blockchain alle telecomunicazioni.

BitCorp dispone inoltre di un framework blockchain proprietario per garantire più sicurezza e minor impatto ambientale.

Web Application per la realizzazione di propri Token Standard ERC20 Compliant (ERC-1363: ERC-20 Compatible Payable Token) con wizard per la configurazione del proprio Smart Contract e connesso alle API del sistema di validazione (Gas Fee, Burniable and Mintable) del framework Ethereumper la distribuzione (Etherscan Explorer e Wallet Metamask).



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 December 2021 (23.12.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/255630 A1

(51) International Patent Classification:
H04L 29/08 (2006.01) *H04L 29/06* (2006.01)
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/IB2021/055250

(22) International Filing Date:
15 June 2021 (15.06.2021)

(25) Filing Language: Italian

(26) Publication Language: English

(30) Priority Data:
102020000014509 17 June 2020 (17.06.2020) IT

(71) Applicant: **BITCORP S.R.L.** [IT/IT]; Via Monte Bianco,

(72) Inventor: **PEGORARO, Gabriele Edmondo**; c/o Bitcorp S.r.l., Via Monte Bianco, 2/A, I-20149 Milano (IT).

(74) Agent: **DI BERNARDO, Antonio** et al.; c/o Thinx S.r.l., Piazzale Luigi Cadorna, 10, I-20123 Milan (IT).

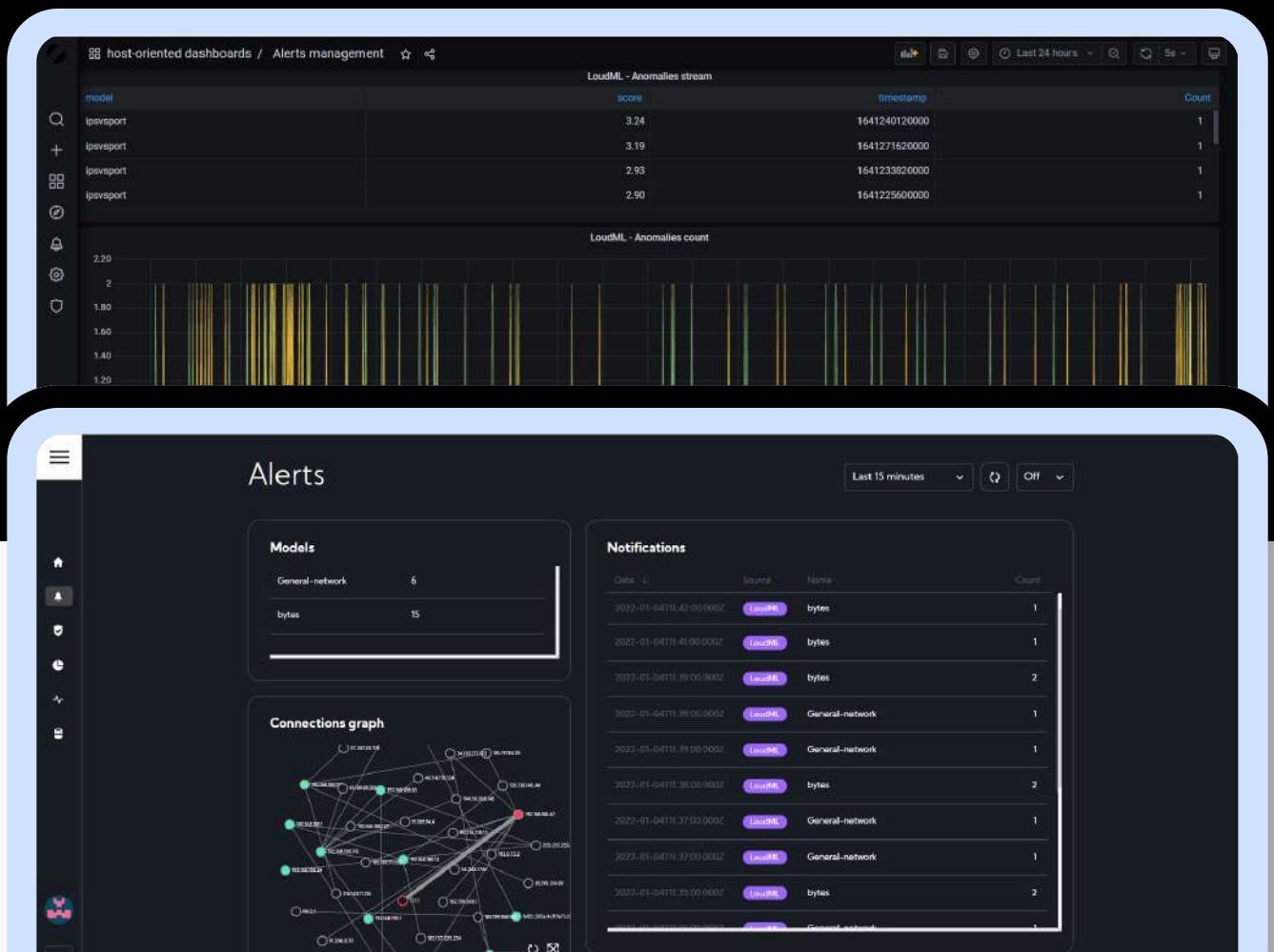
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN,

PRODOTTI

Sistemi di Monitoraggio

Indipendentemente dal settore in cui opera il cliente, è opportuno suggerire l'adozione di una serie di misure finalizzate a ridurre il rischio di attacchi informatici con la conseguente perdita di dati sensibili, interruzione dell'attività produttiva, ransomware, ecc.

BitCorp ha realizzato una serie di prodotti (destinati sia alle grandi imprese che ai piccoli professionisti ed agli studi legali) in grado di monitorare il traffico di rete, individuare per tempo possibili minacce o attacchi latenti e porvi rimedio, anche grazie all'esperienza accumulata nella realizzazione di soluzioni per il mercato Lawful Interception istituzionale.



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.

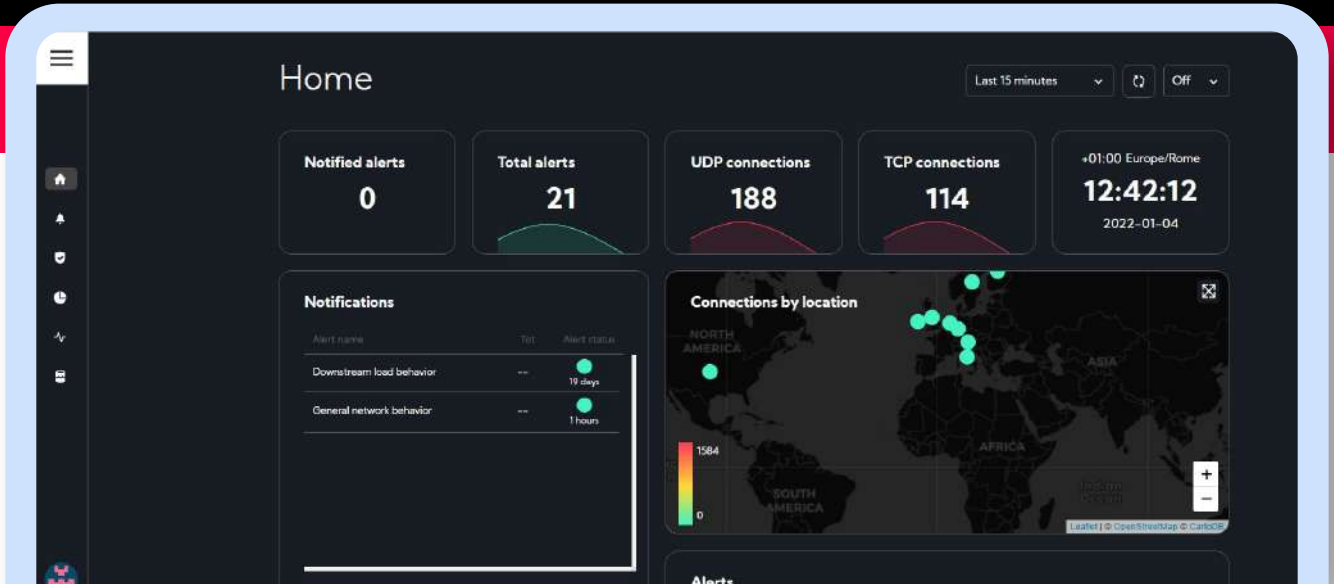
IDS-IPS

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.

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.



End Point management and protection

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

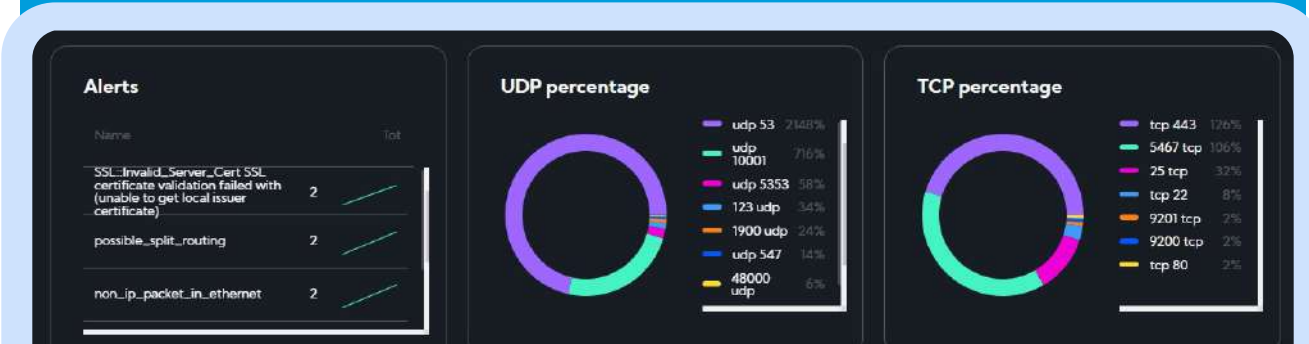
Ciò significa che è in grado di estendere il proprio scudo protettivo a ciascun endpoint presente nella rete monitorata (PC, server, NAS, ecc.) grazie ad una scansione continua e ad un monitoraggio di filesystem, processi e molto altro con API centralizzata che aggrega i dati raccolti e fornisce funzionalità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



PRODOTTI

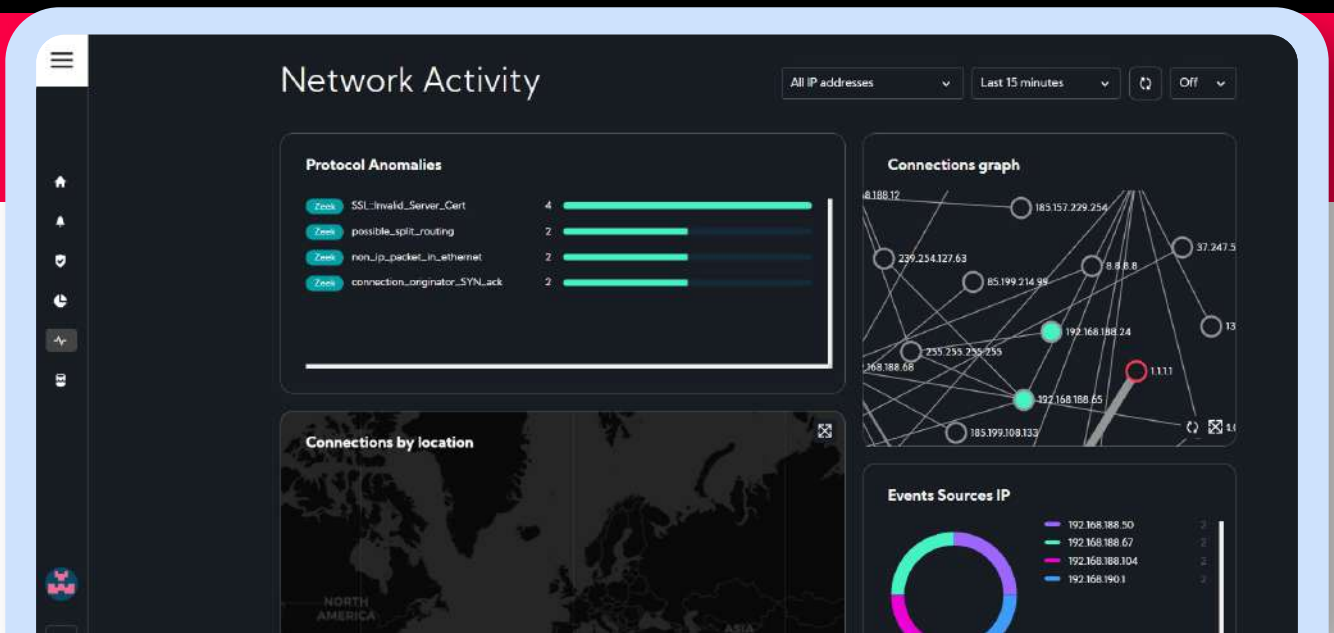
Log Aggregation and Analytics

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.



PRODOTTI

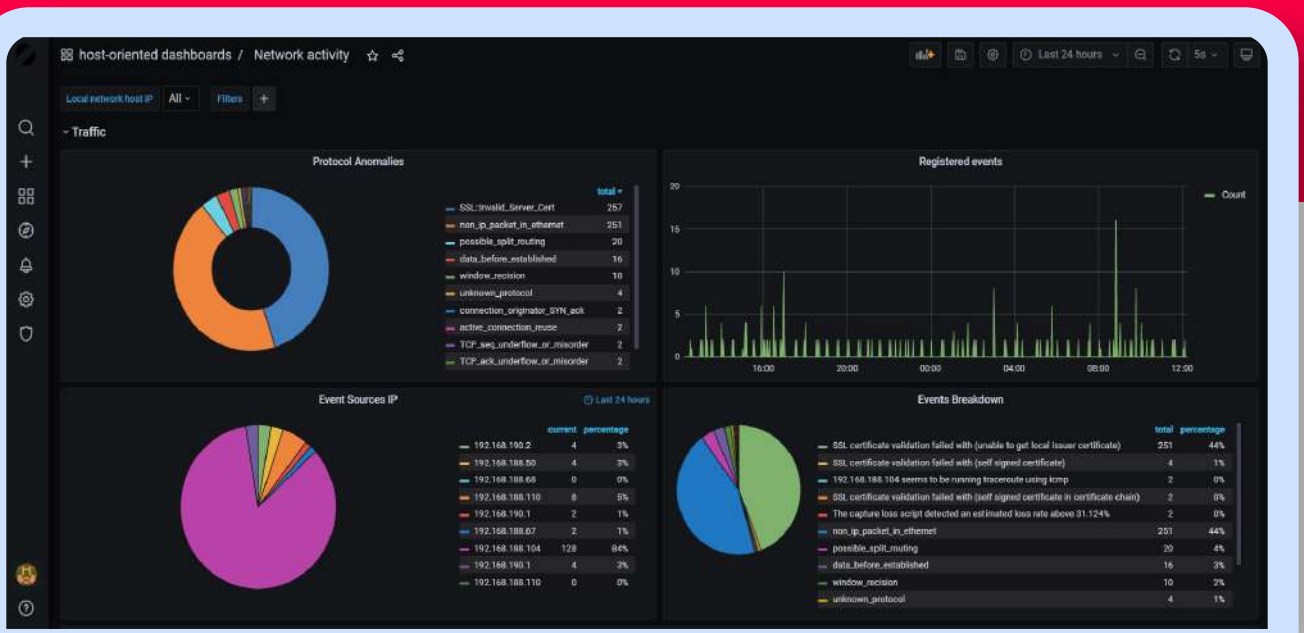
Remediation

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.

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



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 disponibilità 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

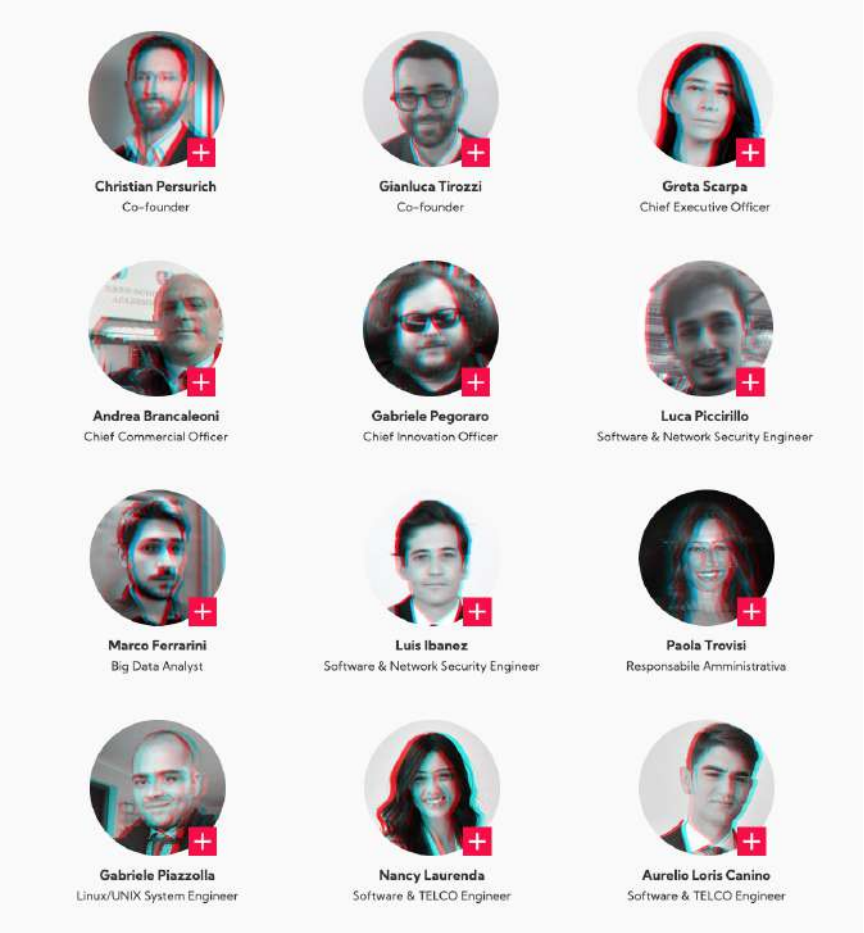
IBM PartnerWorld

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