zadig™ XDR

LA SOLUZIONE INTEGRATA DI CYBERSECURITY PER MEDIE E GRANDI IMPRESE.

Company

VISION

bitCorp è una realtà nata dall'esperienza di due ex operatori di intelligence istituzionale dedicata alla realizzazione di software per il mercato cybersecurity.

In bitCorp ridefiniamo il concetto di cybersecurity distinguendoci dalla concorrenza grazie a una profonda conoscenza delle metodologie di hacking e di vulnerabilità non ancora scoperte che nasce dall'esperienza acquisita nel mercato "lawful interception".

Questo background unico ci fornisce le chiavi per interpretare il modo in cui operano le organizzazioni di hacking criminale, consentendoci di anticipare le loro mosse perché pensiamo come loro.

Sappiamo difendere perché sappiamo come si attacca.

Da qui il nostro motto:

Secured by Professional Strikers

ZADIG XDR

XDR, un esclusivo sistema integrato (ITD) 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 XDR 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.

L'IDS-IPS di ZADIG XDR 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.

Ma ciò che distingue ZADIG XDR da altri sistemi da scaffale è l'altissima capacità di personalizzazione delle proprie funzionalità adattandole alle esigenze del ciente ed al proprio modello di business.

Il nostro impegno va oltre le misure di sicurezza convenzionali; ci sforziamo di fornire un'esperienza in cui la protezione è perfettamente integrata, l'intelligence è in primo piano e la personalizzazione non è solo una caratteristica, ma una filosofia.

Benvenuti in una nuova era della cybersecurity.
Benvenuti in bitCorp.

Company

CHRISTIAN PERSURICH, PHD
CEO

Ex operatore di intelligence, Criminologo e ricercatore presso l'Università Cattolica del Sacro Cuore, ha una esperenzia ventennale, in Italia e all'estero, nel contrasto ai fenomeni terroristici e nell'esecuzione di investigazioni complesse su crimini violenti (omicidi, sequestri di persona, ecc.).

Segue la massima di Confucio "scegli il lavoro che ami e non lavorerai neanche un giorno in vita tua".

GIANLUCA TIROZZI, PHD
PRESIDENTE

Ex operatore di intelligence e ricercatore in Scienze Sociali presso lo IESE, Business School dell'Università di Navarra, ha accumulato esperienze in teatri operativi esteri nell'ambito della gestione di fonti informative e risorse umane, specializzandosi nel contrasto al terrorismo islamista.

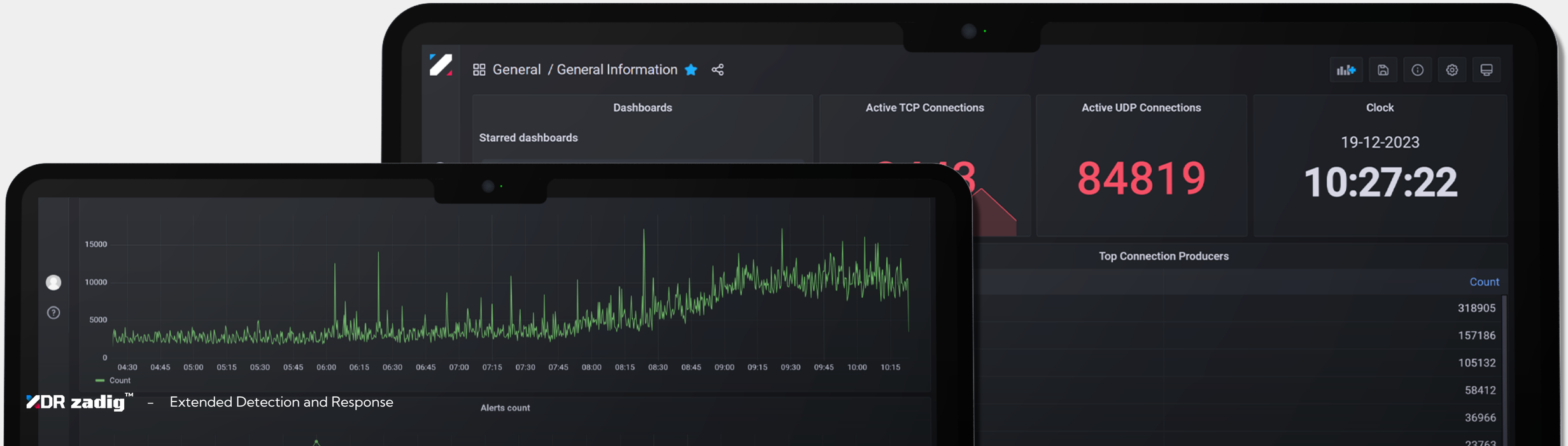
Profondo conoscitore della lingua araba e delle culture pan-Islamiche, il suo motto è "la fortuna di un uomo la fa sempre un altro uomo".

Introduzione

La nostra soluzione Extended Detection and Response (XDR), denominata ZADIG XDR integra una serie di funzionalità avanzate di cybersecurity per il riconoscimento efficace e real-time di minacce.

ZADIG XDR è una piattaforma modulare sulla quale è possibile progettare processi di monitoraggio, rilevamento e reazione sulla base dei threat model che caratterizzano il business di un'organizzazione. Quanto detto è possibile grazie ai vari moduli che consentono di osservare i fenomeni che avvengono sulla rete, sui device e sui servizi.
Per gestire scenari che non consentono la definizione statica di un potenziale problema, il sistema di ZADIG XDR è inoltre dotato di un motore di Intelligenza Artificiale in grado di valutare fenomeni anomali e predire il ripetersi degli stessi.

Il sistema di Log Aggregation and Analytics di ZADIG XDR 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 collezionate dalla soluzione, tra cui eventi di incident management, threat intelligence feeds, log derivanti da apparati di rete ed error reporting.



Pipeline di ingestione dei dati

PIPELINE DI INGESTIONE

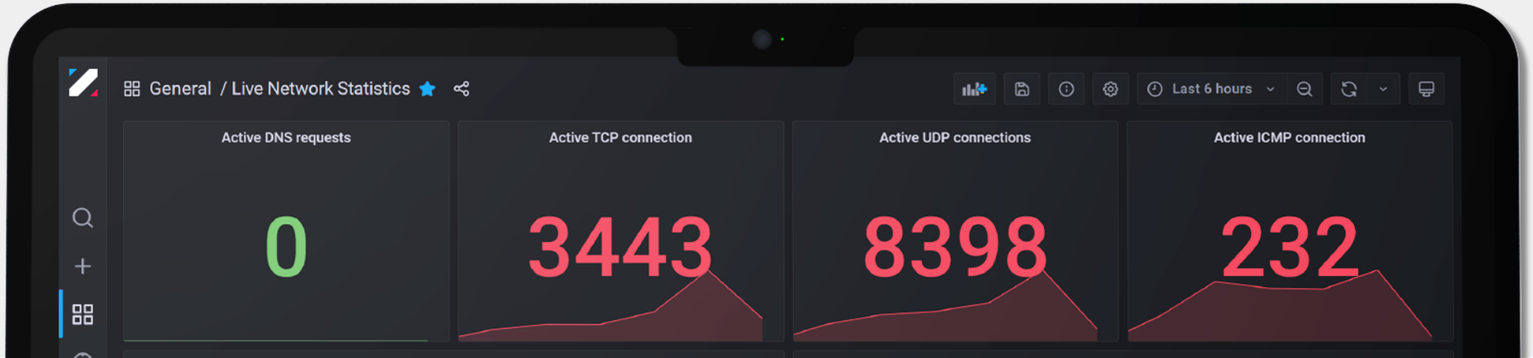
ZADIG XDR offre un'efficiente pipeline di ingestione dei dati che automatizza il processo di collezionamento degli stessi, assicurando che i dati provenienti dalle varie sorgenti siano integrati, elaborati e poi archiaviati in modo coerente ai requisiti definiti.

La nostra soluzione XDR è totalmente flessibile e abilita l'integrazione di dati provenienti da innumerevoli tipologie di sorgenti (ad esempio log provenienti da altri ambienti/produttori). Infatti, il componente che si occupa della gestione della pipeline di ingestione è in grado di collezionare dati provenienti da sorgenti diversificate attraverso plugin di input quali syslog o TCP. Si specifica che **il collezionamento di dati da nuova sorgente può essere configurato in qualunque momento**, anche a seguito dell'effettiva messa in opera della piattaforma XDR, al fine di accomodare eventuali modifiche dell'infrastruttura dell'organizzazione monitorata.

Le principali metodologie di ingestione di log supportate sono:

- **SYSLOG Collector**
- **CSV Collector**
- **DB Collector**
- **FTP Collector**
- **NetFlow Collector**
- **Windows Event Collector**
- **Kafka Collector**
- **HTTP**
- **Raccolta di log utilizzando filebeat**

La soluzione integra nativamente **kafka come tecnologia di log collection**, ad esempio per l'ingestione dei dati monitorati dal suo modulo IDPS integrato (quando previsto), la **metodologia di collection basata su protocollo SYSLOG** per l'integrazione dei log derivanti da altri dispositivi o apparati presenti nell'infrastruttura, e la **metodologia di collection basata sulla lettura di file** per l'integrazione dei log derivanti da altri componenti che producono un feed di alert testuale su file.
È chiaro che tutte le altre metodologie di collection possono essere facilmente attivate in base alle specifiche esigenze.



Pipeline di ingestione dei dati

Di seguito un esempio di file di configurazione di Logstash che abilita l'integrazione dei log provenienti da un firewall di rete con installato sistema operativo pfSense:

```
input {
  tcp {
   id => "pfSense-suricata"
   port => 5544
   type => "suricata"
   codec => line
   mode => "server"
   ssl_enable => true
   ssl_certificate_authorities => ["/usr/share/logstash/config/bundle-ca-pfSense.crt"]
   ssl_cert => "/usr/share/logstash/config/logger.smart.zadig.cloud_cert.pem.cer"
   ssl_key => "/usr/share/logstash/config/key-server.key"
}
  syslog {
    port => 5514
    type => "firewall-1"
    id => "pfSense-AzSentinel-1"
 }
}
```

In aggiunta, la nostra soluzione **XDR offre un supporto nativo per l'integrazione con Azure AD**. Affinché sia possibile raccogliere in modo efficiente i log da Azure Active Directory (AD), è necessario configurare Azure Monitor per esportare i log su Event Hub. Il sistema presenta una pipeline già ottimizzata per la raccolta dei dati provenienti da Event Hub. Al fine di integrare i log provenienti da Microsoft AD, è richiesta l'attivazione di un servizio di Windows sul server domain controller on-premises. A questo software è demandata la raccolta e l'invio dei log al componente di ingestione.

In termini più generali, nel caso in cui una qualsiasi altra soluzione di Identity non supportasse un'integrazione diretta dei log con la nostra soluzione XDR e qualora tale soluzione integrasse i dati in un Security Information and Event Management (SIEM), sarebbe possibile collezionare questi ultimi configurando il SIEM come ennesima sorgente dati diretta della piattaforma XDR.

Pipeline di ingestione dei dati

REPOSITORY DEI DATI

La soluzione XDR è predisposta per interagire con repository di dati situati on-premises o in cloud. In particolare, i repository di dati in cloud nativamente integrati nella soluzione sono **Opensearch di AWS e Log Analytics di Microsoft Azure ed on-premises Elasticsearch**. I repository supportano un motore di ricerca distribuito, con un'interfaccia web HTTP e documenti in formato JSON. Il componente di gestione della pipeline dei dati dovrà interagire con il già menzionato repository per il salvataggio di quanto inviato da ciascuna sorgente sfruttando un apposito plugin di output. Le uniche informazioni necessarie al plugin per salvare correttamente i dati all'interno del repository sono l'indirizzo o nome DNS del repository e l'indice/tabella contenitore dei dati stessi.

Di seguito un estratto di file di configurazione per salvare i dati su un cluster di Opensearch su AWS:

```
opensearch {
   hosts => ["https://vpc-aws8672558-oss-ec1-zadig-01-k2qdi2aw6wtmijc5phkvpblzoe.eu-central-1.es.amazonaws.com:443"]
   auth_type => {
               type => 'aws_iam'
               region => 'eu-central-1'
            }
   index => "logstash-%{+YYYY.MM}"
   action => "create"
   ssl => true
   ecs_compatibility => disabled
   #ilm_enabled => false
  }
```

Di seguito un estratto di file di configurazione per salvare i dati su Log Analytics:

```
microsoft-sentinel-logstash-output-plugin {

                        client_app_Id => "cd4d90a2-287c-497d-81d9-fb334ee836d4"

                        client_app_secret => "t6r8Q~EDcw6NidiKB.vaWpxcNQZtmMN4H2dMcdlm"

                        tenant_id => "8b344519-45d1-44ff-a276-5a67ae3890ce"

                        data_collection_endpoint => "https://logs-ingestion-1ogm.westeurope-1.ingest.monitor.azure.com"

                        dcr_immutable_id => "dcr-0a9941bcd9244ba3a4a15a6bf491b01a"

                        dcr_stream_name => "Custom-gatewaylogs_CL"

                        #create_sample_file => true

                        #sample_file_path => "/tmp"

    }
```

Quando il repository è in cloud, tramite un adapter di log collection, distribuito anch'esso direttamente in cloud risulta possibile integrare sorgenti dati, supportando diversi protocolli, quali Syslog (CEF, LEEF, CISCO, CORELIGHT o RAW – UDP, TCP o Secure TCP, consentendo di impostare una versione minima di TLS 1.2), CSV, Database (MySQL, PostgreSQL, MSSQL o Oracle), Cloud (AWS, Azure, Google), File e cartelle, FTP, NetFlow e Windows Events.

On-premises sono predisposti eventuali aggregatori di log che si limitano a raccogliere i dati dalle fonti presenti sulla sede, applicare logiche di parsing totalmente personalizzabili sui dati stessi ed inviare il risultato in cloud. Tutto questo avviene real-time senza che nessuna informazione venga anche momentaneamente mantenuta localmente.

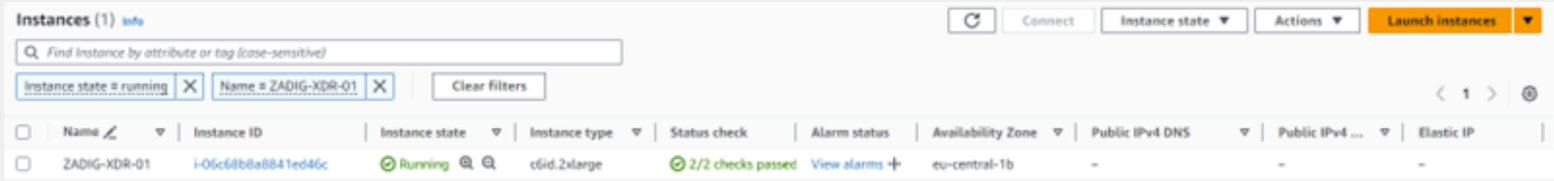
Pipeline di ingestione dei dati

Gli aggregatori di log presenti on premise supportano il deploy affidabilità e sono compatibili con i seguenti hypervisor sia cloud che private:

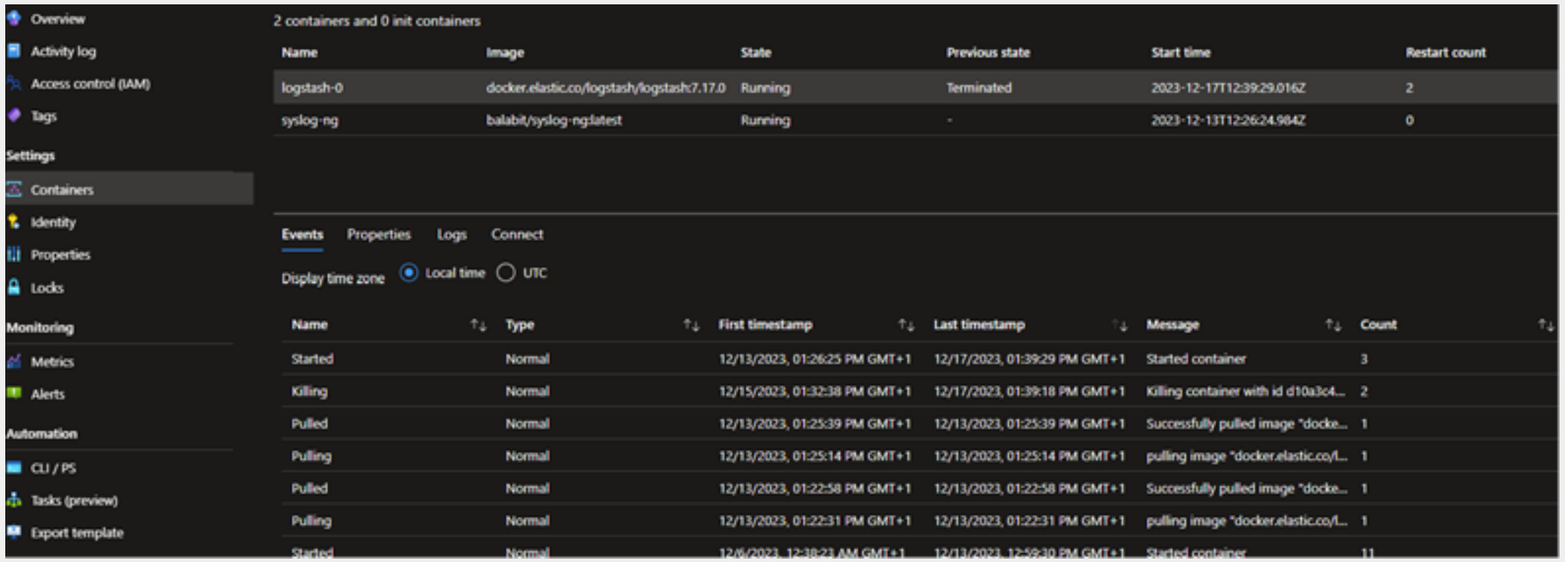
- **Amazon Web Services (AWS)**
- **Microsoft Azure**
- **Microsoft Hyper-V**
- **VMware ESXi**

Risulta possibile effettuare il deploy degli aggregatori di log su macchina virtuale (VM) o su container.

Di seguito un esempio di deploy dell'aggregatore di log su macchina virtuale attiva su Amazon Web Services (AWS):



Di seguito un esempio di deploy degli aggregatori di log su container su Microsoft Azure:



Pipeline di ingestione dei dati

POLICY DI RETENTION DEI DATI

ZADIG XDR conserva nativamente i dati su Elasticsearch o altro storage cloud equivalente. Il sistema consente la creazione di una lifecycle policy sui dati tale da attivare una certa policy di retention sugli stessi, completamente personalizzabile in base alle esigenze della specifica organizzazione destinataria della soluzione.

I dati sono conservati all'interno del repository divisi per indici, su ogni indice è possibile impostare una policy di retention specifica.
Ad esempio, i dati generici (non afferenti ad incidenti informatici) sono conservati in indici del database creati ad-hoc, suddivisi eventualmente per categorie, su cui risulta possibile applicare una policy di retention a scelta (ad esempio almeno 30 giorni). Dati di altra natura, ad esempio quelli relativi agli incidenti di cybersecurity, sono conservati invece in indici differenti, ai quali si può applicare una retention maggiore (ad esmepio almeno 180 giorni).

Al fine di conservare i dati (anche solo alcune specifiche tipologie di questi) per un tempo illimitato, occorre impostare la policy di retention di conseguenza.

La nostra soluzione XDR consente la suddivisione della retention dei dati in hot e cold e considerando alcune tipologie di repository abilita l'aggiunta dello stato di retention warm.

La categorizzazione viene gestita come segue:

- **Hot:** l'indice è in continuo aggiornamento e viene spesso interrogato;
- **Warm:** l'indice non viene più aggiornato ma viene ancora interrogato;
- **Cold:** l'indice non viene né aggiornato né interrogato.

CONFIDENZIALITÀ DEI DATI E DELLE COMUNICAZIONI

I **dati mantenuti nel repository in cloud sono gestiti nel pieno rispetto della privacy.** Essi sono conservati nello spazio cloud dell'organizzazione oggetto del monitoraggio e **sono cifrati sia in transito che "at rest" con algoritmi di encryption sofisticati**, quali almeno AES-256. L'accesso agli stessi è gestito in maniera granulare e garantito solo all'entità che necessitano dell'accesso per ragioni di funzionalità dell'intera soluzione.

Le comunicazioni tra i vari componenti della soluzione sono completamente cifrate con protocollo TLS. La versione minima di protocollo TLS utilizzabile per la cifratura dei dati in transito è TLS v1.2. Ciascun plugin di input è predisposto per accettare comunicazioni cifrate, nel caso il plugin non dovesse supportare TLS, è predisposto apposito proxy TLS per la ricezione sicura dei dati all'esterno. Allo stesso modo, la nostra soluzione XDR trasmette i dati al repository utilizzando protocollo TLS.

Si specifica che ciascun componente integrato nella nostra soluzione XDR offre API per l'automazione.

Interfaccia di gestione

ZADIG XDR è gestito tramite un'interfaccia grafica basata sul Web. La dashboard di gestione della nostra soluzione XDR offre agli analisti la visualizzazione di diverse tipologie di informazioni.

L'interfaccia integra nativamente la visualizzazione di eventi prioritari impostando una sezione dedicata agli alert sulla home page della piattaforma.
Attraverso gli alert, gli analisti possono accedere alla cronologia e alle informazioni di contesto necessarie per la ricerca relativa alle catene di causa-effetto che hanno provocato l'innesco dell'alert. In questo contesto, possono essere attivate tutte le fonti dati a disposizione del cliente, come strumenti di threat intelligence, feed RSS di piattaforme di triage degli allarmi, piattaforme di ticketing e forum di discussione pubblica.

Di seguito due esempi di dashboard:

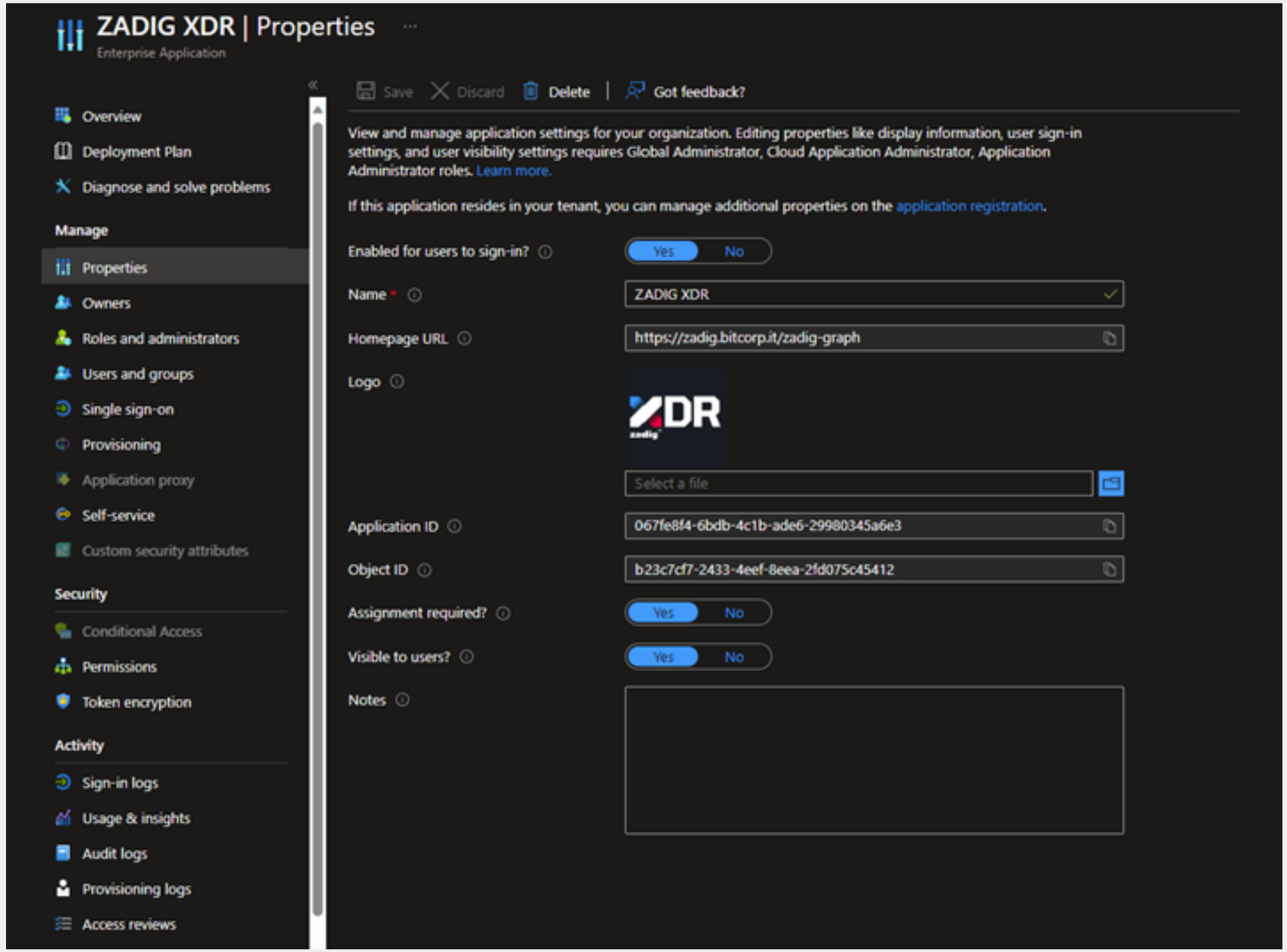
Interfaccia di gestione

ACCESSO SINGLE SIGN ON (SSO)

Per l'accesso alla piattaforma di gestione sono supportati protocolli SAML e OAuth2 per la gestione degli accessi tramite SSO con support MFA.

A scopo esemplificativo di seguito i passaggi principali per poter utilizzare il tenant di Azure AD come identity provider. A tal scopo per riuscire a configurare l'accesso al portale di management tramite SSO è necessario creare un'applicazione su Azure AD. Per abilitare un utente della directory all'accesso è necessario includere l'utente stesso come abilitato all'accesso attraverso la voce del menu "Users and groups".

Di seguito uno screenshot di esempio di Enterprise Application per la gestione dell'accesso SSO:



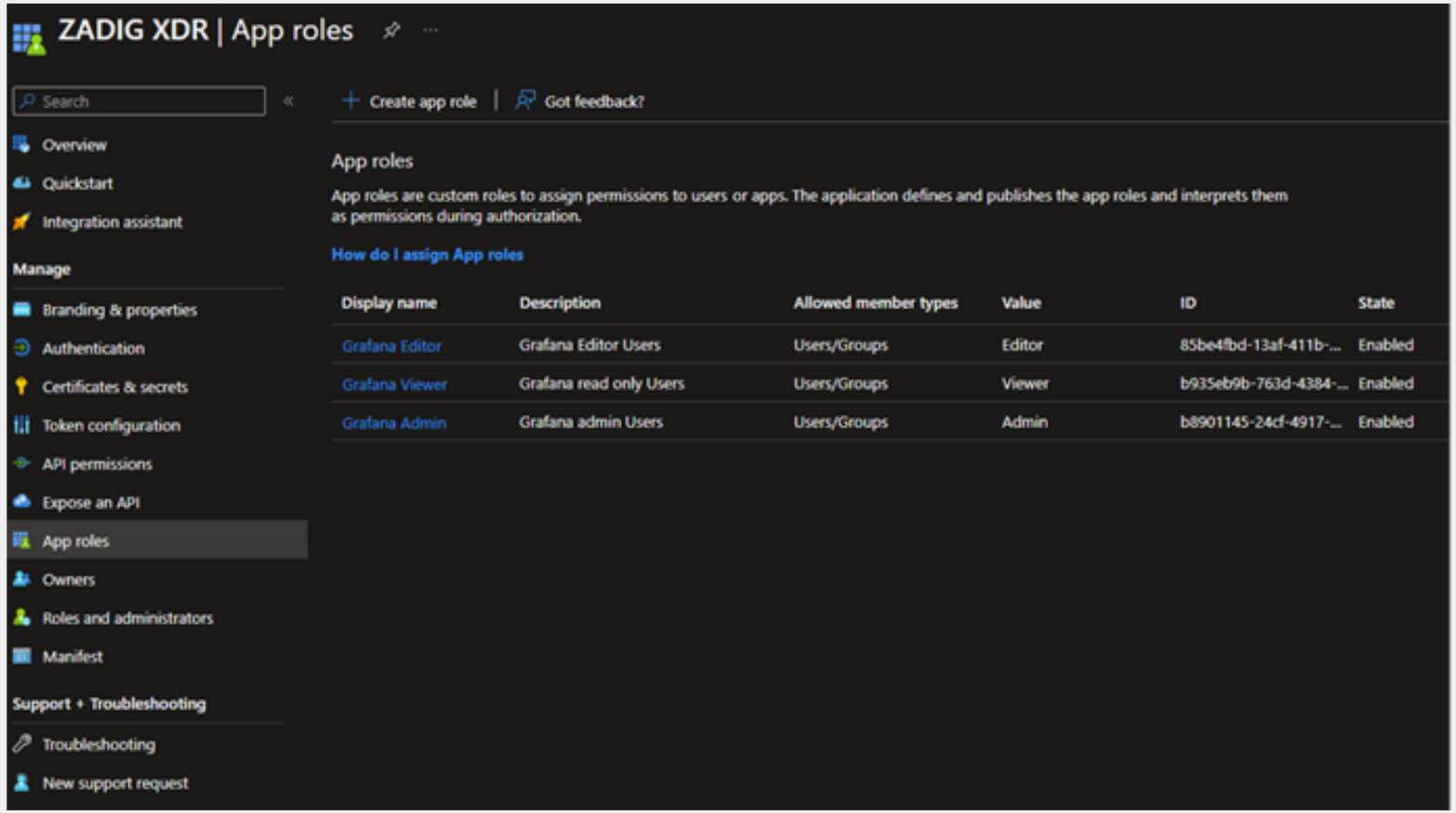
Interfaccia di gestione

L'enterprise application consente la definizione di ruoli assegnabili agli utenti della directory per l'accesso alla piattaforma di gestione.

Affianco un esempio di possibili ruoli definibili.

Dopo aver configurato l'applicazione sul tenant, è dunque necessario abilitare Azure AD OAuth2.0 sul file di configurazione del componente di visualizzazione della soluzione XDR.

Una volta configurato l'ambiente per l'abilitazione del Single Sign On (SSO) con Azure AD, dal portale Entra ID è possibile visualizzare tutti i record di sign-in effettuati dai vari utenti.



Interfaccia di gestione

ROLE BASED ACCESS CONTROL (RBAC)

Come già specificato, **per l'accesso alla dashboard di gestione della nostra soluzione XDR è previsto che ad ogni utente sia associato un ruolo con determinati permessi.** La lista dei possibili ruoli base predefiniti ed associabili ad ogni utente è di seguito definita. **Si specifica che l'elenco può essere personalizzato con l'aggiunta di ruoli specifici** per le esigenze dell'organizzazione destinataria della soluzione:

- **Admin:** ha accesso a tutte le risorse dell'organizzazione, comprese le dashboard, gli utenti ed i team;
- **Editor:** può vedere e modificare le dashboard, le cartelle e le playlist;
- **Viewer:** può visualizzare le dashboard e le playlist.

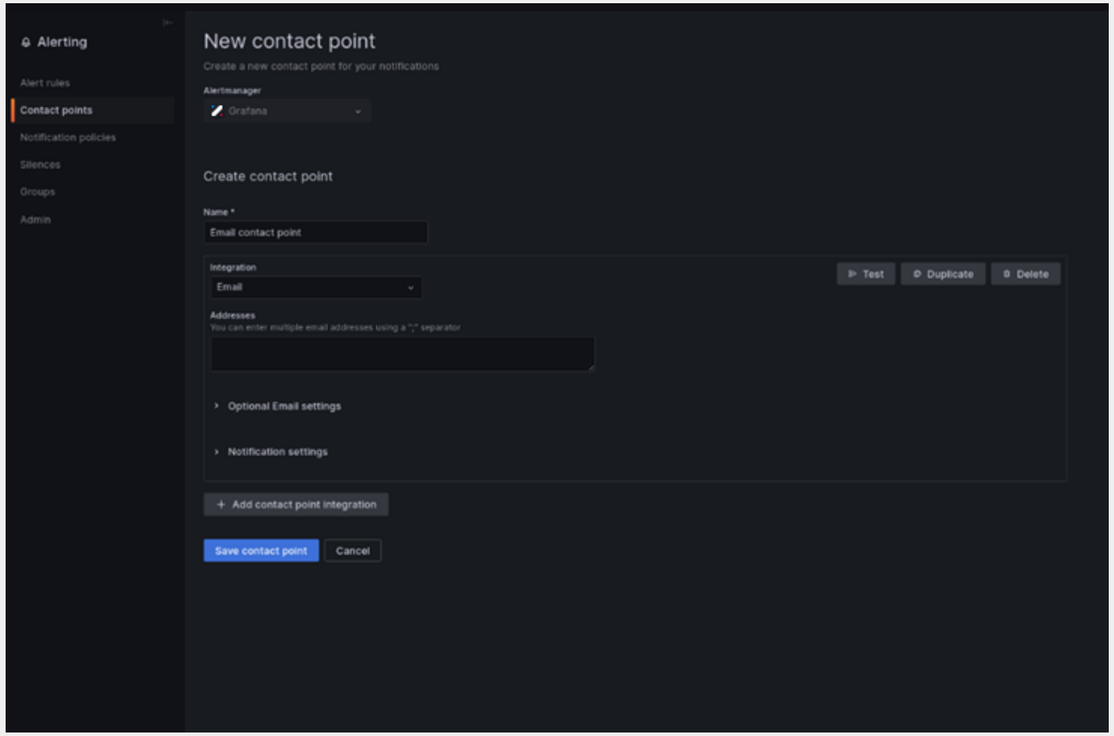
I permessi mappati su ciascuno dei tre ruoli sono disponibili alla seguente tabella:

Permission	Organization administrator	Editor	Viewer
View dashboards	x	x	x
Add, edit, delete dashboards	x	x	
Add, edit, delete folders	x	x	
View playlists	x	x	x
Add, edit, delete playlists	x	x	
Create library panels	x	x	
View annotations	x	x	x
Add, edit, delete annotations	x	x	
Access Explore	x	x	
Add, edit, delete data sources	x		
Add and edit users	x		
Add and edit teams	x		
Change organizations settings	x		
Change team settings	x		
Configure application plugins	x		

Notifica degli allarmi e reportistica

La dashboard di gestione della nostra soluzione XDR offre la funzionalità di definizione dei cosiddetti punti di contatto ai quali inviare la notifica di alerts. Ciascun punto di contatto consente di configurare la metodologia di invio della notifica stessa.

Di seguito uno screenshot che mostra la configurazione di un punto di contatto con metodo di notifica e-mail:



Sono supportati molti altri canali di notifica come Telegram, Slack, Discord e Webhook per qualsiasi altra piattaforma di Instant Messaging (IM).

Sempre dalla piattaforma di management è possibile configurare gli alert per il monitoraggio di determinati eventi rilevanti per lo scenario in esame, ciascun alert può essere associato ad una policy di notifica attiva su un punto di contatto. Così facendo l'attivazione dell'alert sarà automaticamente notificata al punto di contatto selezionato. Il punto di contatto potrebbe essere un altro sistema o apparato di rete in grado di reagire all'alert stesso. Infatti, attraverso l'attivazione di Webhook è possibile notificare l'incidente arricchendo il messaggio con metadati e informazioni utili,ad esempio agli apparati di rete (firewall) per applicare contromisure parametrizzate sui metadati stessi (blocco di un determinato indirizzo IP).

Per ciascun alert **è possibile configurare una metodologia di invio della notifica,** scegliendo uno o più punti di contatto. In aggiunta **la generazione di un alert sull'XDR viene opportunamente notificata agli altri sistemi di cybersecurity attivi sull'infrastruttura** (SIEM, SOAR). Contestualmente alla notifica viene fornita ai già menzionati sistemi una serie di informazioni (metadati) utili ai fini della generazione di un report di sicurezza che include tutte le informazioni di contesto necessarie incluso un ritaglio di schermata della visualizzazione grafica dell'alert che ha generato l'allarme. La generazione effettiva del report è delegata al modulo SOAR che se lo reputa opportuno innesca la relativa produzione documentale.

Rilevamento delle minacce

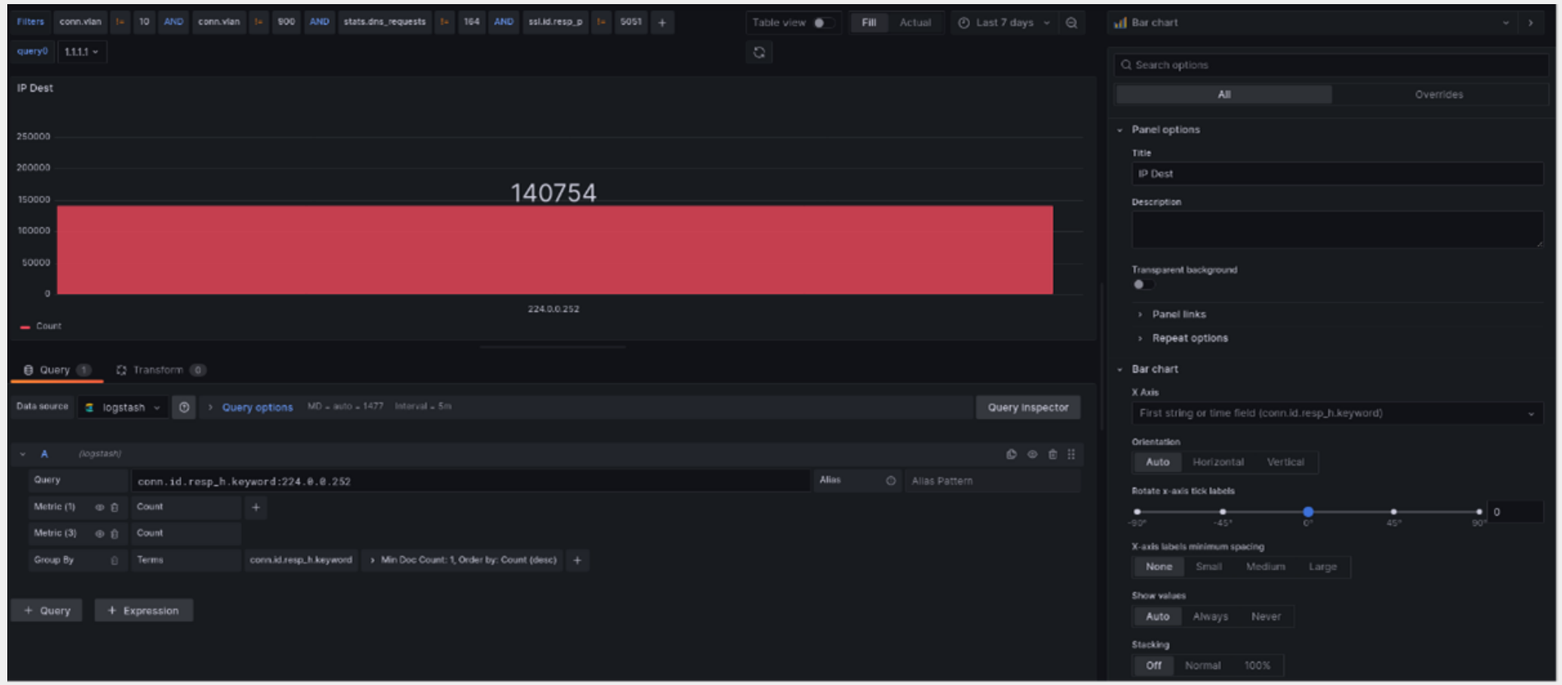
L'identificazione delle minacce avviene attraverso due approcci distinti:

1. **Signature-Based:** Riconoscimento statico basato su pattern malevoli noti, con file di signature regolarmente aggiornato.

2. **Behavioral-Based:** Riconoscimento dinamico mediante modelli di Machine Learning.

Entrambi gli approcci lavorano anche sui dati storici mantenuti all'interno del repository che è possibile interrogare per tutto il periodo di retention impostato. La piattaforma di gestione abilita la ricerca manuale di IOC nei dati raccolti. Si consideri di sapere che un certo IP destinazione rappresenta un IOC, ovvero è evidenza di un qualche tipo di attacco o minaccia. La piattaforma di gestione della nostra soluzione XDR consente la generazione di query specifiche per la ricerca di tale dato all'interno di tutti gli IP destinazione associati alle connessioni.

Di seguito un esempio di query per effettuare la ricerca appena esposta, supponendo di voler ricercare l'IP destinazione 224.0.0.252:



Rilevamento delle minacce

La query è impostata per restituire anche il conteggio del numero di connessioni che hanno coinvolto quell'IP. In aggiunta, come specificato anche in precedenza, la piattaforma consente la configurazione di un alert che **invia una notifica ogni volta che l'IP appare all'interno di una connessione.**

La soluzione integra modelli di Machine Learning progettati per il rilevamento di comportamenti anomali all'interno dell'infrastruttura monitorata. Tali modelli, al fine di garantire delle metriche di performance adeguate, sono addestrati utilizzando i dati dell'infrastruttura stessa, qualunque sia la loro provenienza (log derivati da apparati di rete, traffico di rete intercettato dalla sonda, log derivanti da soluzioni di identity, eventi derivanti dalla componente ISD statica ecc..). La soluzione è fornita con una serie di modelli preconfigurati per la detection di incidenti, resta vero che è possibile sviluppare ulteriori modelli di ML per il riconoscimento specifici comportamenti anomali caratterizzanti il business dell'organizzazione monitorata.

I modelli possono essere configurati per lavorare su un certo bucket di input, che corrisponde ad una serie di indici del repository dei dati. Ogni modello, così configurato **riesce ad apprendere il comportamento standard della rete attraverso i dati derivanti da più sorgenti al fine di rilevare comportamenti sospetti** su dispositivi non direttamente monitorati (dispositivo su cui non è stato installato alcun agente). Questo risulta fondamentale **al fine di monitorare il comportamento di dispositivi di proprietà di utenti ospiti o occasionali** che per ovvie ragioni non sono direttamente monitorati dalle soluzioni di cybersecurity messe in atto dall'organizzazione.

Di seguito è mostrato il json relativo ad uno dei modelli integrati nella soluzione XDR:


```
{
    "state" : {
      "loss" : 0.00905147445824953,
      "trained" : true
    },
    "settings" : {
      "min_threshold" : 0,
      "default_bucket" : "input",
      "run" : {
        "detect_anomalies" : true,
        "flag_abnormal_data" : true,
        "save_prediction" : true,
        "output_bucket" : "output",
        "save_output_data" : true
      },
      "interval" : 60,
      "forecast" : 5,
      "span" : 20,
      "type" : "timeseries",
      "features" : [
        {
          "io" : "io",
          "field" : "conn.id.resp_h.keyword",
          "default" : 0,
          "anomaly_type" : "high",
          "measurement" : "traffic",
          "metric" : "cardinality",
          "name" : "Number_of_ips"
        },
        {
          "metric" : "cardinality",
          "name" : "open_ports",
          "measurement" : "opened_ports",
          "field" : "conn.id.resp_p",
          "io" : "i",
          "default" : 0
        }
      ],
      "grace_period" : 0,
      "default_datasource" : "input",
      "name" : "ipsvsport",
      "seasonality" : {
        "daytime" : true,
        "weekday" : true
      },
      "max_threshold" : 0,
      "bucket_interval" : "1m",
      "max_evals" : 10,
      "timestamp_field" : "@timestamp",
      "offset" : 30
    }
}
```

Rilevamento delle minacce

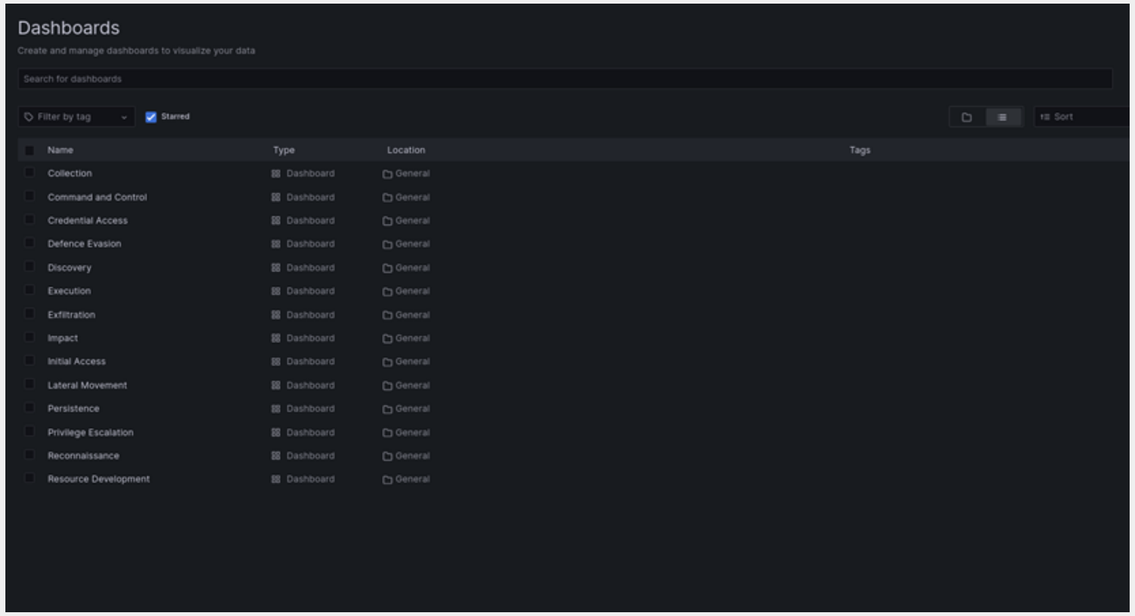
Di seguito un esempio di configurazione dei bucket di input ed output, il primo indica l'insieme dei dati sui quali il modello sarà addestrato, il secondo, invece rappresenta il contenitore dentro il quale il modello archivierà le predizioni effettuate:

```
buckets:
  - name: input
    type: elasticsearch
    addr: localhost:9200
    index: logstash-*
    doc_type: _doc

  - name: output
    type: elasticsearch
    addr: localhost:9200
    index: output-models
    doc_type: _doc

storage:
  path: /var/lib/loudml

server:
  listen: 0.0.0.0:8077

#
```

Inoltre, i modelli di Machine Learning utilizzati dalla soluzione XDR associano un punteggio per ciascun evento predetto. Il punteggio assegnato i**ndica la priorità e quindi la pericolosità dell'evento appena avvenuto**, superata una certa soglia di score, l'evento viene considerano anomalo e quindi prioritario.

Sfruttando i modelli di ML la soluzione effettua riconoscimento di IOC su base comportamentale. Ogni IOC può essere modificato ed è possibile aggiungere nuovi indicatori personalizzati sulla base di quanto detto nel requisito precedente, assegnando di volta in volta la categoria di ATT&CK corrispondente.

Ciascuna macrocategoria definita dal framework è associata ad una specifica dashboard sulla piattaforma. Ogni dashboard contiene una serie di visualizzazioni, ognuna impostata per rilevare IOC di attacchi e minacce afferenti alla categoria associata alla dashboard stessa.



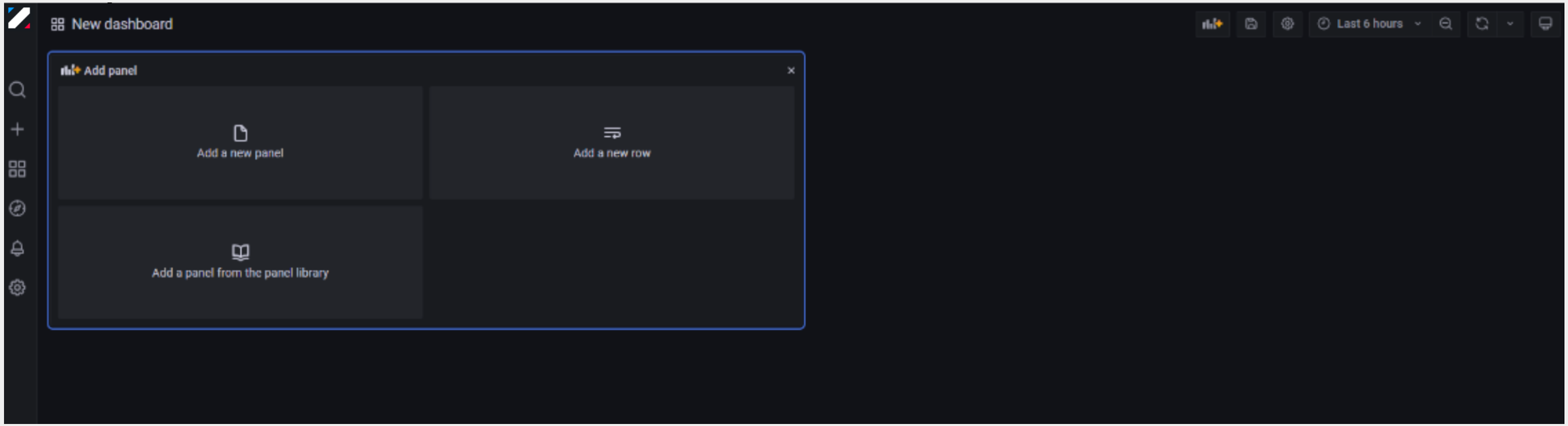
Parsificazione ed interrogazione dei dati

La nostra soluzione XDR include procedure standard e un linguaggio specifico per l'esecuzione di query volte all'analisi delle informazioni disponibili.

Le varie informazioni possono essere organizzate in dashboard, ognuna delle quali contiene diversi pannelli di visualizzazione.

La schermata per la creazione di un pannello consente di impostare una query di ricerca da eseguire su una specifica data source, ovvero su uno specifico indice o tabella presente nel repository dei dati.

Ad ogni pannello deve essere associata una visualizzazione attraverso cui mostrare i dati.

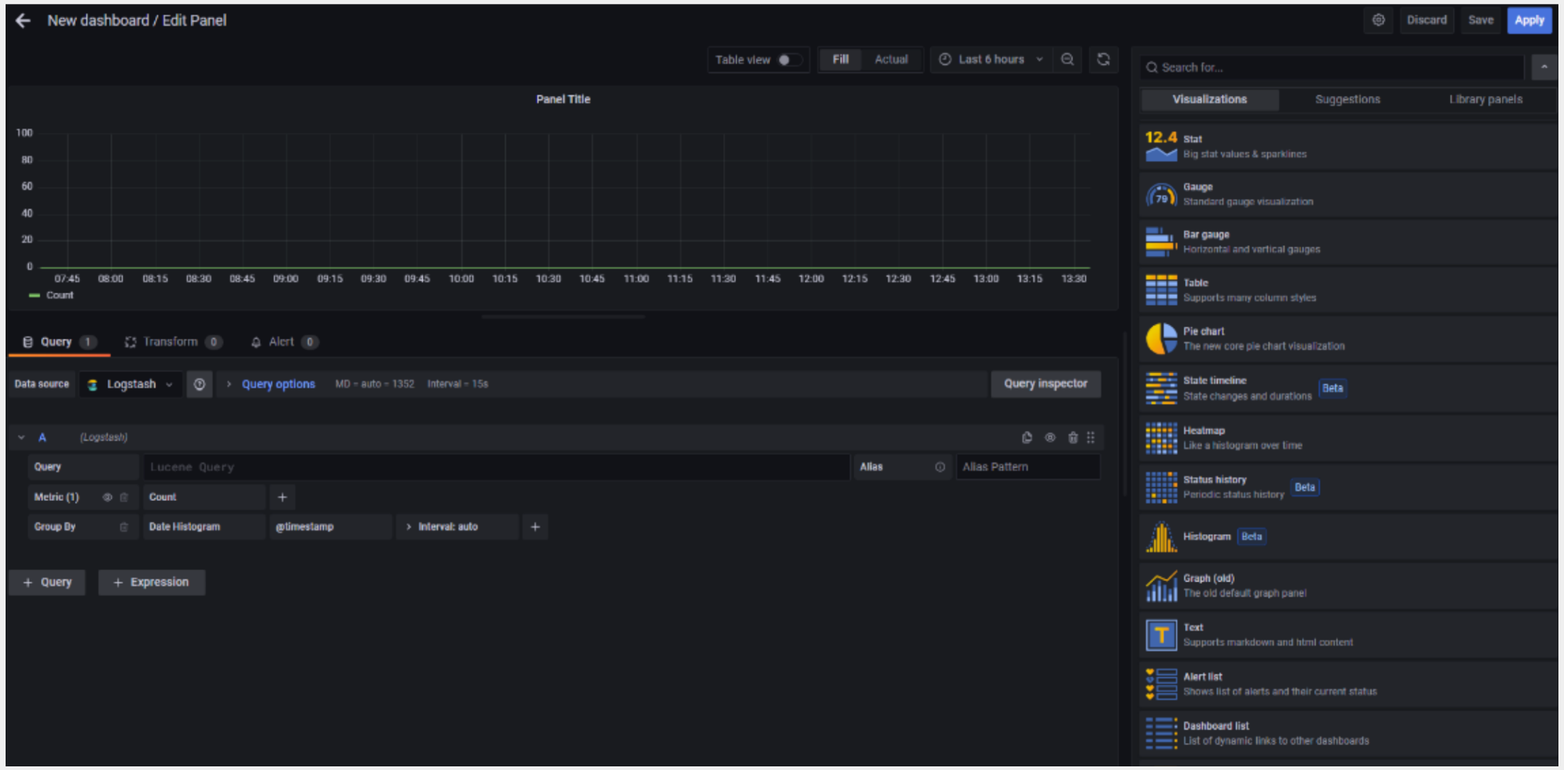


Parsificazione ed interrogazione dei dati

Di seguito è riportata la schermata per la creazione di un pannello:

Il linguaggio di query offerto dalla nostra soluzione **supporta**, tra le altre cose, le seguenti funzionalità: **filtraggio per individuare condizioni specifiche, la scelta di un sottoinsieme di campi da mostrare, la trasformazione di determinati campi restituiti dalla query, il calcolo di media, conteggio ecc, la possibilità di ordinare i risultati e la gestione dei deduplicati.** Esiste un set di query predefinito. Ogni query può essere associata ad una dashboard per attivarne il continuo monitoraggio o per eseguirla on-demand su dati afferenti ad uno specifico intervallo di tempo.

Ciascuna query può essere trasformata in un BIOC, associando alla stessa un alert. Questo consentirà di monitorare ed individuare nuovi eventi sospetti oppure ricercare quel BIOC su dati esistenti che lo attivano.



Parsificazione ed interrogazione dei dati

PARSING DEI DATI

È disponibile una piattaforma specifica per la gestione dei file contenenti la configurazione delle regole di parsing, di fatto dei filtri che vengono applicati ai dati grezzi ingeriti in ingresso dal componente di ingestione dei dati. Tali filtri **consentono l'eliminazione di un dato potenzialmente inutile, con l'obiettivo di ridurre i costi di archiviazione.** Inoltre, **consentono l'arricchimento dei dati con tag utilizzabili dal resto del flusso di raccolta,** ad esempio di seguito un estratto della configurazione che aggiunge dei tag se determinate condizioni sono soddisfatte:

```
if [process][name] =~ /^dhcpd$/ {

    mutate {

      add_tag => [ "dhcp", "dhcpdv4", "firewall" ]

      add_field => { "[event][dataset]" => "pfAzSentinel.dhcp" }

    }

    grok {

      patterns_dir => [ "/usr/share/logstash/patterns" ]

      match => [ "filter_message", "%{DHCPD}"]

    }

  }
```

Parsificazione ed interrogazione dei dati

I filtri di parsing consentono inoltre l'aggiunta di informazioni efficaci per il rilevamento di minacce, come quella relativa alla geolocalizzazione di un indirizzo IP, di seguito il frammento di configurazione creato per adempiere il già menzionato scopo:

```
if [destination][ip] {
      ### Check if destination.ip address is private
      cidr {
        address => [ "%{[destination][ip]}" ]
        network => [ "0.0.0.0/32", "10.0.0.0/8", "172.16.0.0/12", "192.168.0.0/16", "fc00::/7", "127.0.0.0/8", "::1/128", "169.254.0.0/16", "fe80::/10", "224.0.0.0/4", "ff00::/8", "255.255.255.255/32", "::" ]
        add_tag => "IP_Private_Destination"
      }
      if "IP_Private_Destination" not in [tags] {
        geoip {
          source => "[destination][ip]"
#MMR#           database => "/var/lib/GeoIP/GeoLite2-City.mmdb"
          target => "[destination][geo]"
        }
        geoip {
          default_database_type => 'ASN'
#MMR#           database => "/var/lib/GeoIP/GeoLite2-ASN.mmdb"
          source => "[destination][ip]"
          target => "[destination][as]"
        }
        mutate {
          rename => { "[destination][as][asn]" => "[destination][as][number]"}
          rename => { "[destination][as][as_org]" => "[destination][as][organization][name]"}
          rename => { "[destination][geo][country_code2]" => "[destination][geo][country_iso_code]"}
          rename => { "[destination][geo][region_code]" => "[destination][geo][region_iso_code]"}
          add_tag => "GeoIP_Destination"
        }
      }
    }
```

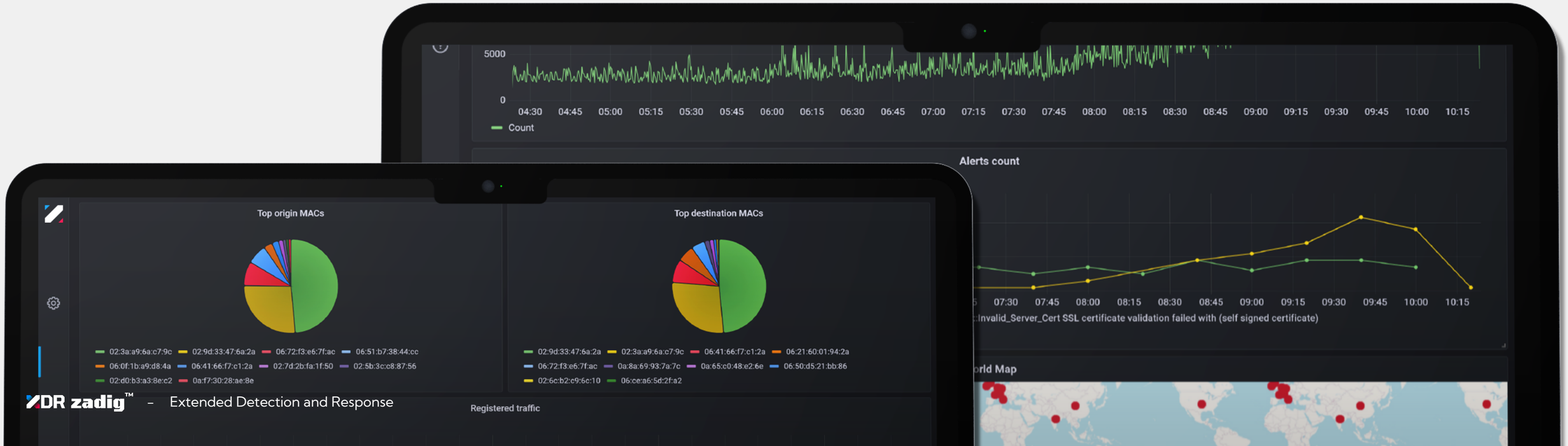
zadig™

XDR

MODULO EDR

Modulo EDR

ZADIG XDR offre un software EDR. Esso è composto da un insieme di progetti che implementano un unico core di servizio multipiattaforma, che combina più moduli (eventualmente nativi) e viene distribuito in modo coerente su diverse piattaforme di destinazione. L'agente vero e proprio è progettato per funzionare in background e reagire a diversi tipi di eventi. La soluzione XDR **prevede un agent persistente** i cui dati vengono visualizzati e gestiti tramite piattaforma unificata con funzionalità di gestione e protezione endpoint e che consente di effettuare correlazione con gli altri dati provenienti da tutte le altre sorgenti integrate. **È stato inizialmente progettato per supportare gli eventi del filesystem di accesso, ma può facilmente ospitare altre fonti di eventi.**
La soluzione supporta installazioni non persistenti nella misura in cui il cliente sia già dotato di una soluzione di gestione automatica della distribuzione di applicazioni. **Gli alert prodotti dalla piattaforma possono essere elaborati dal SOAR al fine di attivare i profili di distribuzione dell'agente sui dispositivi coinvolti dall'alert.**



XDR zadig™ – Extended Detection and Response

Modulo EDR

INSERIMENTO DI MODULI

La risoluzione delle dipendenze avviene tramite autofac utilizzando un file di configurazione. Tutti i moduli possono essere considerati produttori di eventi (generatori) o consumatori (gestori). Tutti espongono o si connettono ad alcune interfacce comuni. A seconda della piattaforma di destinazione e delle caratteristiche desiderate, è possibile configurare un diverso set di moduli per la risoluzione di dipendenze in base alla distribuzione.

ESTENSIONI NATIVE

I moduli possono dipendere da funzionalità o API specifiche della piattaforma. In questo caso, il modulo fornisce tutte le estensioni native richieste, ad es. binding, librerie, driver o applicazioni aggiuntive.
In nessun caso altri moduli di interfacciamento dovrebbero preoccuparsi di come tale specificità della piattaforma viene implementata, tutto rimane nascosto all'interno del modulo.

APP HOSTS

La compositon root fa parte di una libreria che può essere referenziata da diversi tipi di application host. Questo rende più facile sviluppare, testare e distribuire l'agente all'interno di più wrapper minimi che meglio si adattano al dispositivo endpoint. Ad esempio, è possibile eseguire la stessa base di codice del servizio agente come applicazione console o servizio in background.

APPLICAZIONI UTENTE

Un certo numero di features richiede interazioni utente. La loro implementazione fa parte di applicazioni specifiche per la piattaforma che meglio corrispondono ai vari casi d'uso in diverse classi di dispositivi endpoint.

CONFIGURAZIONE

Il servizio core dell'agente può includere un modulo che necessita di parametri out-of-package da impostare in modo che il modulo sia funzionale. Le applicazioni utente devono avere accesso in scrittura – a determinate condizioni – a posizioni di configurazione condivise che il core dell'agente potrebbe leggere all'avvio.

Dato che il core del servizio agente sarà probabilmente eseguito con alti privilegi a livello di sistema, l'applicazione utente deve eventualmente chiedere diritti elevati per scrivere nella posizione di configurazione condivisa.

Modulo EDR

INTERAZIONE CON IL SERVIZIO CORE

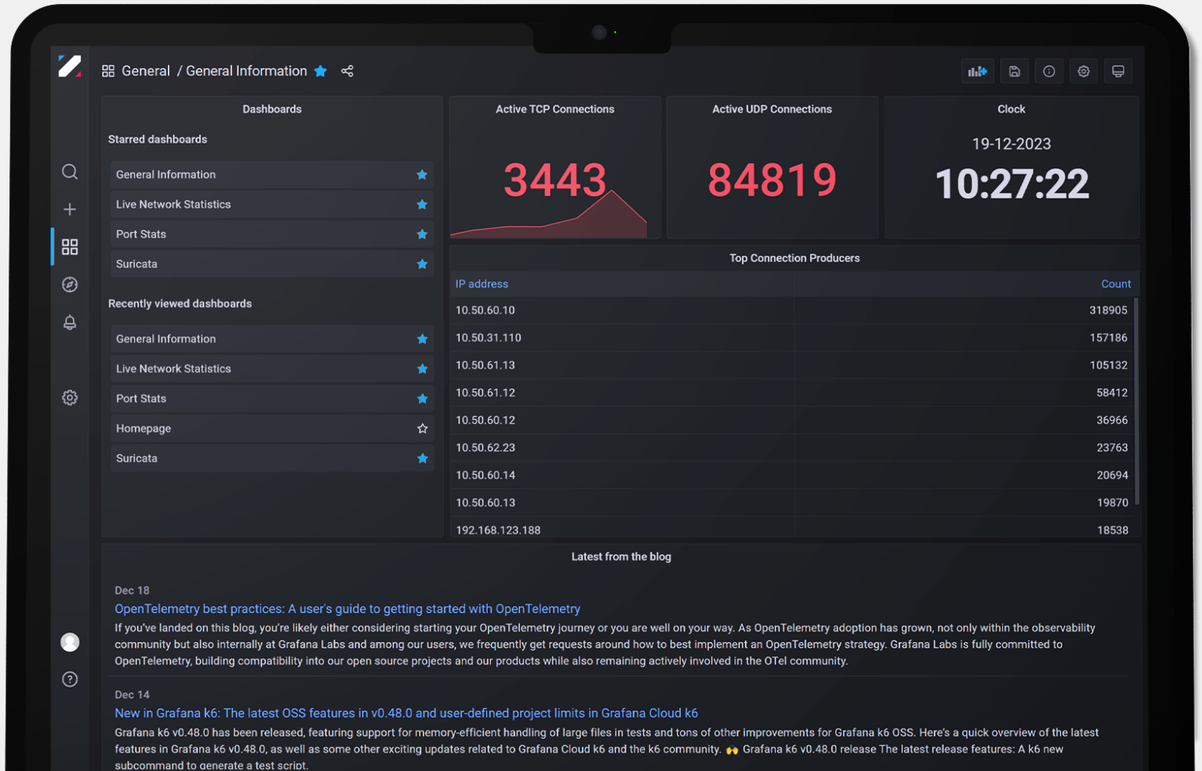
Il servizio core dell'agente potrebbe includere moduli di gestione degli eventi che richiedono interazioni asincrone dell'utente per la segnalazione dello stato del servizio, l'avviso o l'adozione di decisioni.
Le applicazioni dell'utente si associano a questo tipo di moduli e forniscono l'interfaccia utente necessaria e le integrazioni con le API shell della piattaforma.

MODELLO DI DISTRIBUZIONE

Ogni piattaforma consente una serie di diversi modelli di distribuzione. E' stato necessario scegliere alcuni che forniscano in modo efficiente sia l'agent service worker di base (con tutti i suoi moduli) e l'applicazione utente.
L'implementazione pacchettizzata sembra essere abbastanza conveniente per i requisiti esterni, poiché ogni sistema operativo attualmente fornisce un modo per raggruppare i nostri due componenti in un unico elemento distribuibile.

FUNZIONALITÀ DISPONIBILI CON DISTRIBUZIONE A PACCHETTO

Le applicazioni pacchettizzate possono beneficiare di funzionalità della piattaforma come gli aggiornamenti automatici, la facile disinstallazione, la consegna e licenza dei pacchetti ottimizzati (che potrebbero essere utili in futuro nel caso in cui diversi moduli vengano installati come plug-in aggiuntivi).



zadig™

XDR

MODULO SOAR

Modulo SOAR

La funzionalità SOAR di ZADIG XDR è uno strumento di cybersecurity per automatizzare la prevenzione da attacchi informatici e la risposta agli incidenti.

La nostra soluzione SOAR è una piattaforma innovativa di automazione della sicurezza che combina l'intelligenza umana ed Intelligenza Artificiale per garantire il massimo livello di protezione. La nostra soluzione integra diversi playbook che eseguono il triage degli eventi da un qualsiasi SIEM, EDR o un'altra fonte gestita. È possibile utilizzare un webhook per inviare gli alert alla piattaforma ed ogni alert viene elaborato per identificare ed estrarre gli indicatori rilevanti.

Applicazione di Gestione di Casistiche e Incidenti (CIM)

Il CIM funge da punto centrale di interazione per un team che opera nell'ambito della sicurezza. Puoi utilizzare questa applicazione in modo indipendente o in combinazione con una soluzione come la SOC.

COME FUNZIONA

L'applicazione di Gestione di Casistiche e Incidenti (CIM), come parte della Soluzione SOC, funge da punto centrale di interazione per il team che si occupa della sicurezza. L'applicazione fornisce le seguenti capacità pratiche:

- Triage unificato dei segnali da triage degli alert, triage delle frodi e creazione manuale di playbook con automazioni per la creazione di record;
- Interfaccia di arricchimento dell'Intelligence sulle minacce (TI);
- Vari punti di avvio per l'orchestrazione;
- Triage del segnale, gestione di casi, gestione degli incidenti, dettagli delle indagini, articoli della Knowledge Base, rimedio, correlazione e rapporti di attività post intervento;
- Spazi dedicati per personalizzazioni;
- Raccolta automatica di metriche;
- Modalità avanzata per il troubleshooting e il fine tuning;

PAGINA PRINCIPALE DELLA CIM

Dopo aver effettuato l'accesso, segui questi passaggi per accedere alla homepage della CIM.

1. Seleziona il tuo tenant.

   Se hai accesso a più tenant, assicurati di essere nel tenant corretto. Se hai accesso a un solo tenant, verrà selezionato automaticamente il tenant corretto.

2. Seleziona lo spazio di lavoro **Soluzioni SOC** o lo spazio di lavoro desiderato.

3. Nel riquadro di navigazione a sinistra, fai clic su **RECORD DELL'APPLICAZIONE.**

4. Seleziona **Gestione di Casistiche e Incidenti.**

5. Seleziona un record CIM dalla lista dei record CIM nel report predefinito.

Puoi visualizzare un record dell'applicazione CIM. È possibile vedere immediatamente i dettagli del record nel riquadro di sinistra, tra cui tipo di segnale, verdetto dell'intelligence, fonte del segnale, ecc. Inoltre, ci sono sezioni espandibili e comprimibili che forniscono ulteriori informazioni sul record.

Applicazione di Gestione di Casistiche e Incidenti (CIM)

AZIONI DI CREAZIONE DEL RECORD

Quando viene creato un nuovo record nell'applicazione CIM, vengono eseguite due azioni di automazione per arricchire il segnale con verdetti osservabili e un brief automatico.

BRIEF AUTOMATICO

Al record dell'evento sull'applicazione CIM è associato un riepilogo generato automaticamente.

PUNTI DI AVVIO DELL'ORCHESTRAZIONE

Questi rappresentano punti naturali nel ciclo di vita del record all'interno dell'applicazione di Gestione di Casistiche e Incidenti in cui può idealmente avere luogo l'automazione/orchestrazione configurabile.

TIPO: SEGNALE

I record arrivano nell'applicazione come Segnali. I Segnali rappresentano un evento in arrivo da un sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM) o da un sistema di rilevamento e risposta agli endpoint (EDR), un'email di phishing segnalata o una indicazione ad hoc di attività sospetta creata manualmente. Un segnale in arrivo deve avere uno dei seguenti valori come fonte:

- Alert
- Email Phishing
- Manuale

Per reclamare il record e intraprendere ulteriori azioni.

- Per reclamare il record, fai clic su Reclama.

Una volta reclamato il record, diventi il Proprietario Attuale e lo stato del record si aggiorna a "In corso". Dopo aver valutato l'attività, è possibile far escalation il record a un caso nell'evenienza in cui il caso sia un vero positivo o vengano raggiunte altre soglie (le soglie sono determinate dalle policy della tua organizzazione).

Applicazione di Gestione di Casistiche e Incidenti (CIM)

RICHIEDERE L'ASSEGNAZIONE DEL RECORD PER INTRAPRENDERE ULTERIORI AZIONI

TIPO: CASO

L'elevazione a un caso cambia semplicemente il valore del Tipo a "Caso". È importante sottolineare nuovamente che questo è un importante punto di avvio per l'Orchestrazione.

Nel lavorare su un caso, potrebbe essere un'ottima opportunità per identificare segnali o casi aggiuntivi che possono essere correlati. Al momento, la funzione di Correlazione nella Soluzione SOC è un semplice campo di riferimento. Le future versioni della Soluzione SOC cercheranno di ampliare la capacità di Correlazione.

TIPO: INCIDENTE

n determinate circostanze, quando si lavora su un caso, un operatore può scegliere di Dichiarare un Incidente. Generalmente, ciò avviene quando viene raggiunta una soglia di impatto specificata che richiede passi aggiuntivi, segnalazioni, comunicazioni agli interessati, ecc.

1. Per dichiarare un incidente, clicca su Dichiara Incidente.

Ciò cambia il valore del Tipo a Incidente. Inoltre, compare un banner rosso in alto al record per accentuare la criticità del record.

A mano a mano che l'incidente viene mitigato può essere fatta de-escalation dell'incidente. De-escalation di un incidente è un'indicazione che l'incidente è stato mitigato e le squadre di intervento possono sospendere le operazioni di emergenza.

1. Per fare de-escalation di un incidente, clicca su De-Escalation dell'Incidente.

PERSONALIZZAZIONE

Il nuovo CIM fornisce uno spazio dedicato in cui è possibile aggiungere campi personalizzati senza influenzare l'aspetto e la sensazione dello spazio principale dell'applicazione.

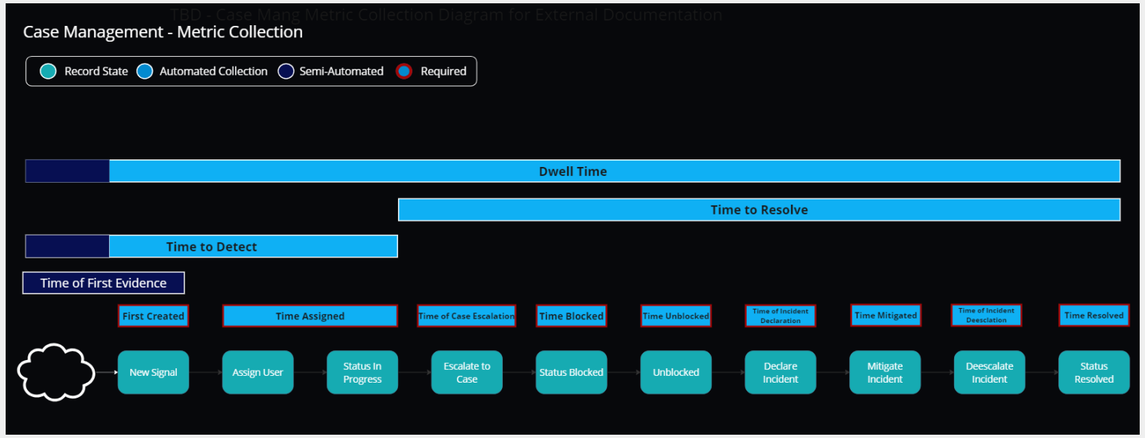
CAMPI PERSONALIZZATI

L'applicazione fornisce alcuni campi di esempio per dimostrare i possibili casi d'uso per questa sezione.

Applicazione di Gestione di Casistiche e Incidenti (CIM)

METRICHE

La soluzione ha la capacità di catturare metriche iper-granulari. Durante il ciclo di vita di un record, esistono punti strategici in cui viene catturato un punto dati o un timestamp. Il flusso previsto e i punti di acquisizione dati sono visualizzabili in questo diagramma:



CAMPI METRICHE GRANULARI

Nel record, è possibile visualizzare le metriche. Clicca sulla scheda Metriche Granulari. Queste metriche alimentano vari report di dashboard, come MTTD, MTTR, Dwell Time, ecc.

MODALITÀ AVANZATA

L'applicazione CIM dispone di una casella di controllo Avanzata che, quando selezionata, mostra la funzionalità, i widget e i riferimenti gestiti dell'applicazione.

Ci sono sei sezioni aggiuntive espandibili e comprimibili su un record CIM. La documentazione seguente fornisce dettagli su ciascuna sezione e su come interagisce nel record CIM.

DETTAGLI INVESTIGATIVI

La sezione Dettagli Investigativi contiene un campo di riepilogo compilabile per il record corrente e che verrebbe incluso in un rapporto di azioni successive (AAR) generato automaticamente (vedi sezione Attività Post Incidente). Inoltre, questo potrebbe essere utilizzato per altri casi d'uso come la Soluzione di Collaborazione. La sezione Commenti dell'Investigazione mostra i commenti che non sono inclusi nell'AAR ma sono contenuti nella soluziione SOAR. La sezione Fasi di Attacco fornisce un luogo per inserire o rivedere le coppie Tecnica/Tattica MITRE ATT&CK utilizzate per alimentare il pannello MITRE nella Soluzione SOC. Puoi anche popolare manualmente la sezione di trascinamento e rilascio Blocco delle prove con file vari correlati all'indagine.

Applicazione di Gestione di Casistiche e Incidenti (CIM)

ARTICOLI DELLA KNOWLEDGE BASE

Come suggerisce il nome, la sezione Knowledge Base contiene passi per il rimedio precedentemente creati dall'utente per questo record. Utilizzando questa sezione, è possibile accedere a lezioni apprese e altri suggerimenti su quel record o su qualcosa che ha informazioni correlate (ad esempio, un tipo di segnale simile). Gli Articoli della Knowledge Base esistenti (KBA) contengono l'ID di tracciamento per il corrispondente KBA, il titolo dell'allarme, il riepilogo del contesto, la guida e l'ultima data di aggiornamento.

1. Per aggiungere un nuovo KBA al record corrente, nella tabella degli Articoli della Knowledge Base, clicca sull'icona **plus**.
2. Clicca sull'icona **lente d'ingrandimento** per cercare un KBA.
3. Se necessario, clicca sull'icona **cestino** per eliminare un KBA dal record.
4. Per assicurarti di avere l'ultimo e migliore set di KBA per quel record dopo le modifiche apportate alla tua indagine come mappature MITRE ATT&CK, clicca su **Aggiorna Collegamenti** Knowledge Base.

INTELLIGENCE SULLE MINACCE

VERDETTO DI INTELLIGENCE

Se vengono scoperti osservabili nel segnale in entrata tramite un allarme o un'e-mail di phishing, quegli osservabili vengono automaticamente analizzati e arricchiti dai fornitori di TI configurati attraverso l'applicazione TI (vedi l'applicazione Threat Intelligence per ulteriori dettagli). In base ai risultati del Fornitore di Intelligence Primaria scelto, il verdetto più critico viene passato al valore di Verdetto di Intelligence. La criticità del verdetto è ordinata da più a meno critica:

- Malevolo
- Sospetto
- Benigno
- Sconosciuto

La sezione Threat Intelligence visualizza i risultati di arricchimento del Fornitore di Intelligence Primaria per ciascun osservabile analizzato (widget) e consente all'utente di eseguire un arricchimento ad-hoc dell'osservabile (Osservabile, Tipo di Osservabile, Aggiungi Osservabile) durante lo sviluppo dell'indagine. Questa è l'opzione più semplice per visualizzare l'IT associata a un record CIM specifico.

Applicazione di Gestione di Casistiche e Incidenti (CIM)

Questa sezione permette anche l'esportazione dei dati TI. Nei menu a discesa, seleziona l'Indicatore Selettore desiderato, il Selettore Risultati, il Selettore Fornitore e l'Operatore Filtri.
Una volta ottenute le informazioni desiderate, clicca su Esporta per scaricare i dati in un file .csv. Il file .csv fornisce i dettagli TI seguenti sui dati selezionati:

- ID di tracciamento
- Indicatore
- Permalink (Una risorsa come un arricchimento osservabile su VirusTotal/Recorded Future)
- Strumento (ad esempio, VirusTotal)
- Etichetta (ad esempio, Malevolo, Sospetto ecc.)
- Punteggio
- Ultimo Aggiornamento

RIMEDIO

L'applicazione Case and Incident Management (CIM) ha una sezione Rimedio con diverse schede, che eseguono otto playbook diversi per azioni di rimedio per un record CIM. Come orchestratore, questo fornisce un modo per intraprendere varie azioni di rimedio in base alle informazioni del record CIM.

BLOCCA/SBLOCCA OSSERVABILI

Come orchestratore, è necessario completare le configurazioni per il playbook CIM – Blocca Osservabili prima di aggiornare il record CIM. La prima azione è un segnaposto. In caso si voglia sostituire questa azione con un'azione di rimedio o un playbook nidificato. Successivamente, configurare l'azione per il compito che si desidera eseguire contro gli osservabili che si configureranno successivamente nel record CIM.

1. Da ORCHESTRAZIONE, fai clic su **Playbook.**
2. Cerca e apri il playbook **CIM – Blocca Osservabili.**
3. Nel segnaposto della prima azione, sostituisci e configura il rimedio desiderato.

Applicazione di Gestione di Casistiche e Incidenti (CIM)

Questo può essere un playbook nidificato o un'azione che hai già configurato. Ad esempio, un playbook che richiama un firewall per bloccare gli indirizzi IP o isolare gli host su EDR. Il playbook riceve l'ID di tracciamento per il ticket corrente e i valori che stai passando. Le altre azioni del playbook generano la risposta in uscita e aggiornano il record CIM. Ora vai al record desiderato e scorri fino alla sezione Rimedio e alla scheda Blocca/Sblocca Osservabili.

1. In questa scheda, inserisci gli osservabili che desideri bloccare, quindi fai clic su **Blocca Osservabili.**

Una volta cliccato il pulsante, esegue un playbook e restituisce i risultati nel campo Risposta Blocca Osservabili con una risposta che mostra cosa ha fatto il playbook e su cosa ha agito con data/ora.

Per sbloccare un osservabile, segui i passaggi sopra per il playbook CIM – Sblocca Osservabili e inserisci gli osservabili che desideri sbloccare, quindi fai clic su Sblocca Osservabili. Ancora una volta, la risposta viene visualizzata con una data/ora.

Importante! Mentre gli orchestratori devono creare i playbook nidificati e/o le azioni all'interno dei playbook CIM – Blocca Osservabili e CIM – Sblocca Osservabili, gli operatori possono modificare il contenuto della scheda Rimedio nel record CIM. La modifica degli osservabili del record CIM non richiede un accesso di livello orchestratore. Lo stesso vale per tutti i playbook che vengono eseguiti nella scheda Rimedio.

DISABILITA/ABILITA UTENTI

Questa scheda funziona come la scheda Blocca/Sblocca Osservabili. Gli orchestratori devono prima accedere ai playbook CIM – Disabilita Utenti o CIM – Abilita Utenti per sostituire l'azione segnaposto con un playbook o un'azione annidata configurata che esegue l'esito desiderato.

1. Naviga al record CIM desiderato e alla sezione **Rimedi.**
2. Nella scheda Disabilita/Abilita utenti, inserisci gli utenti che desideri disabilitare e/o abilitare.
3. Clicca su **Disabilita Utenti e/o Abilita Utenti.**

Ciò esegue il playbook appropriato e restituisce i risultati nei campi Risposta Disabilita Utenti e/o Risposta Abilita Utenti con una risposta che mostra cosa hanno fatto i playbook e su cosa hanno agito con data/ora.

Applicazione di Gestione di Casistiche e Incidenti (CIM)

ISOLA/RIUNISCI HOST

Questa scheda funziona anche come la scheda Blocca/Sblocca Osservabili. Gli orchestratori devono prima accedere ai playbook CIM – Isola Host o CIM – Riunisci Host per sostituire l'azione segnaposto con un playbook o un'azione annidata configurata che esegue l'esito desiderato.

1. Naviga al record CIM desiderato e alla sezione **Rimedi.**

2. Nella scheda Isola/Riunisci Host, inserisci gli host che desideri isolare o riunire.

Questo è comune con i casi d'uso EDR.

1. Clicca su **Isola Hosts e/o Riunisci Hosts.**

Ciò esegue il playbook appropriato e restituisce i risultati nei campi Risposta Isola Hosts e/o Risposta Riunisci Hosts con una risposta che mostra cosa hanno fatto i playbook e su cosa hanno agito con data/ora.

AVVISA I MANAGER

Questa scheda funziona come la scheda Blocca/Sblocca Osservabili. Gli orchestratori devono prima accedere al playbook CIM – Avvisa i Manager per sostituire l'azione segnaposto con un playbook o un'azione annidata configurata che esegue l'esito desiderato.

1. Naviga al record CIM desiderato e alla sezione **Rimedi.**

2. Nella scheda Avvisa i Manager, inserisci l'indirizzo email del manager per avvisare il manager di un evento di sicurezza.

3. Clicca su **Avvisa i Manager**.

Ciò esegue il playbook appropriato e restituisce i risultati nel campo Risposta Manager Avvisati con una risposta che mostra cosa ha fatto il playbook e su cosa ha agito con data/ora.

Applicazione di Gestione di Casistiche e Incidenti (CIM)

RICERCA SIEM

Questa scheda funziona come la scheda Blocca/Sblocca Osservabili. Gli orchestratori devono prima accedere al playbook CIM - Query SIEM per sostituire l'azione segnaposto con un playbook o un'azione annidata configurata che esegue l'esito desiderato.

1. Naviga al record CIM desiderato e alla sezione **Rimedi.**

2. Nella scheda Ricerca SIEM, inserisci i dati della query SIEM.

Un buon caso d'uso è eseguire un'indagine su un indirizzo IP (osservabile) per vedere se si verifica in altri luoghi nel tuo ambiente. Inserisci l'osservabile nel campo di query SIEM e clicca sul pulsante per eseguire il playbook e ottenere i risultati.

1. Clicca su **Query SIEM.**

Ciò esegue il playbook appropriato e restituisce i risultati nel campo Risposta Query SIEM con una risposta che mostra cosa ha restituito il tuo SIEM e una tabella che può visualizzare eventi SIEM in formato JSON standardizzato. La tabella consente anche la possibilità di filtrare in base a colonne o valori.

CORRELAZIONE

La nostra soluzione SOAR può correlare record, consentendo di confrontare un nuovo record con un record precedente che ha chiavi di correlazione. Nell'applicazione di Case and Incident Management (CIM), sono presenti informazioni sulla correlazione nel record CIM in una sezione designata e sulla scheda Supporto.

Un'azione di correlazione si verifica ogni volta che viene creato un record. Dalla scheda Supporto su un record CIM, la sezione Campo di Supporto Correlazione accoglie 13 campi chiave di correlazione (osservabili) dai playbook Process Alerts o Process Emails. Dopo che avviene la correlazione, il SOAR esegue un playbook che estrae gli ID di tracciamento per i record correlati.

Nel record di esempio, CIM-241 mostra la sezione Correlazione con gli ID di tracciamento correlati nei record CIM-244, CIM-243, CIM-245 e CIM-242. Le informazioni del titolo, dello stato, del verdetto di intelligence, del verdetto manuale e delle informazioni brevi automatizzate di ciascun record vengono visualizzate nella tabella delle Correlazioni.

1. Per vedere un record specifico in dettaglio, clicca sull'ID di tracciamento corrispondente.

Applicazione di Gestione di Casistiche e Incidenti (CIM)

Il record selezionato si apre in una finestra popup. Clicca fuori dalla finestra per tornare al tuo record attuale.

Le informazioni non vengono visualizzate solo in questa sezione, ma c'è anche un widget sotto la sezione BREVE AUTOMATIZZATA chiamato Records. La sezione Records fornisce una rappresentazione più visuale dei record attuali e correlati con dettagli del record che evidenziano dati importanti e l'opzione di esportare i dati di quel record in un file .csv.

ATTIVITÀ POST INCIDENTE

Su un record di Case and Incident Management (CIM), questa sezione ha un pulsante Genera Report Dopo le Azioni.

Quando clicchi su questo pulsante, il SOAR raccoglie i punti dati dal tuo record, li passa a uno script che genera un report HTML, quindi converte quel report in un file PDF facilmente comprensibile come report dopo azioni (AAR).

1. Dalla sezione Attività Post Incidente, clicca su Genera Report Dopo le Azioni.

2. Clicca sull'icona Download per scaricare il PDF o clicca direttamente sul nome del file per visualizzare anteprima del file.

Il PDF si apre dopo il download o la visualizzazione. Il file ha un layout di facile lettura che include le seguenti informazioni per quel record:

- Numero di caso
- Breve automatico
- Riepilogo dell'indagine
- Azioni di rimedio intraprese
- Riepilogo della cronologia
- Informazioni sull'handler dell'incidente

Se hai una copia locale di un AAR e vuoi aggiungerla al record, trascina semplicemente il file nella sezione Rapporto Dopo le Azioni.

Suggerimento: Se un orchestratore desidera regolare le informazioni restituite nel file PDF AAR, è possibile navigare e aprire il playbook CIM – Genera Rapporto Dopo le Azioni, cliccare sull'azione Genera Rapporto HTML e cliccare su Configura. Dal pannello Script, utilizzando HTML, è possibile modificare i dati restituiti.

Applicazione di Gestione di Casistiche e Incidenti (CIM)

APPLICAZIONE THREAT INTELLIGENCE

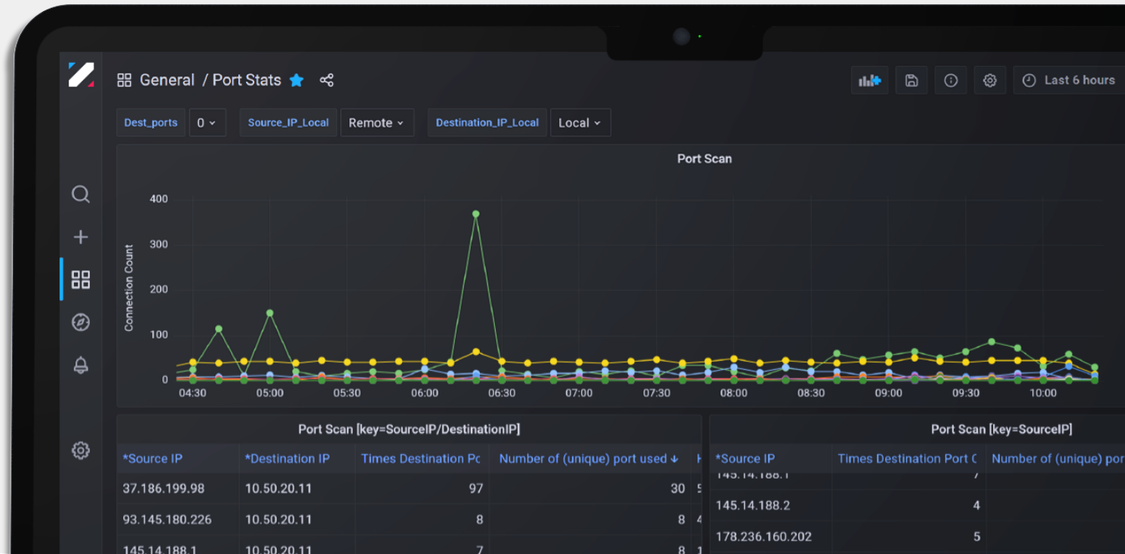
L'applicazione TI arricchisce gli osservabili provenienti da CIM. Tutti gli osservabili univoci provenienti da un segnale in entrata nell'applicazione CIM generano un nuovo record TI.

FORNITORE PRINCIPALE DI INTELLIGENCE

In base al valore del tipo osservabile, viene selezionato il Fornitore Principale di Intelligence (PIP) appropriato. L'arricchimento risultante è in cima all'applicazione. I valori dell'arricchimento PIP determinano il Verdetto di Intelligence, come menzionato in Applicazione di Case and Incident Management.

ALTRI FORNITORI

Di nuovo, in base al valore del tipo osservabile, altri fornitori di intelligence arricchiscono l'osservabile. I risultati di questi fornitori, pur non contribuendo al Verdetto Primario di TI, sono visibili direttamente nel Record TI in un'apposita widget espandibile. I dettagli chiave dell'arricchimento sono visualizzati con la possibilità di fare clic sulla card del widget per espandere e visualizzare il JSON grezzo.



Script

Suggerimento: Per i tipi di dati Boolean e Null, consigliamo di importare JSON e utilizzare json.loads() per assicurarsi che i dati vengano caricati correttamente. Poiché tutti i dati del playbook sono in formato JSON e Python non supporta nativamente tutti i tipi di dati JSON.

Utilizzate l'azione nativa controllata dello Script e scrivete in Python per:

- manipolare dati e casi limite.
- ridurre la complessità utilizzando JSONata.
- utilizzare il linguaggio di programmazione più comune in sicurezza oggi per svolgere compiti semplici.

Durante la configurazione degli input, considerate l'uso del Chatbot Python, che utilizza ChatGPT's Open AI per aiutarvi a formulare trasformazioni e codice Python personalizzato.

CONFIGURAZIONE DELL'AZIONE NATIVA SCRIPT

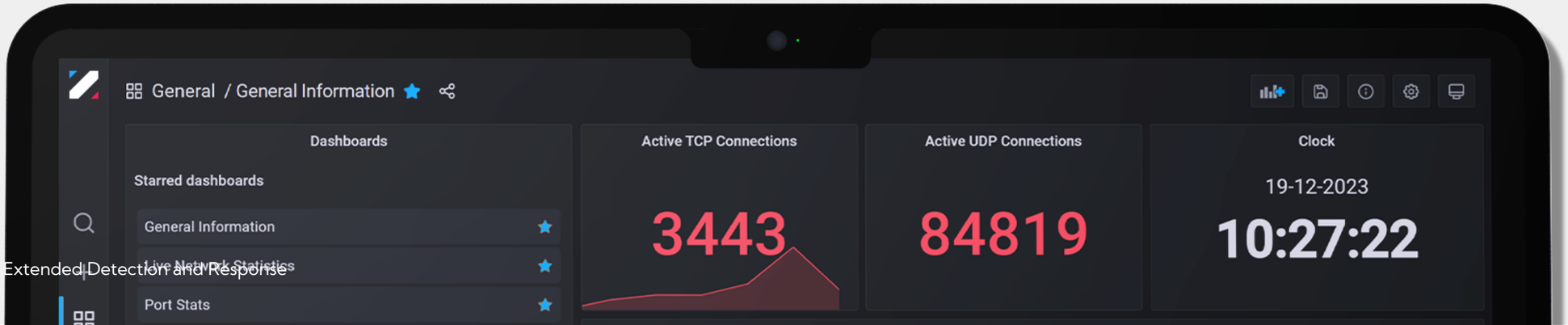
È ora di iniziare la configurazione di base per l'azione nativa Script.

Avete già creato un playbook e siete pronti a manipolare i dati da una proprietà.

1. Dal vostro playbook, cliccate su **Aggiungi un'azione.**
2. Dal pannello **AZIONE**, cliccate sul menu a discesa **Azione**.
3. Selezionate **Script** e cliccate su **Configura**.

La finestra Script si apre.

La finestra Script ha tre schede: Script, Outputs e Test. La scheda Script ha il riquadro degli Input (sul lato sinistro) e il riquadro dello Script (sul lato destro).



Script

INPUT DELLO SCRIPT

Con l'azione nativa Script, potete costruire e mappare input di dati statici e di proprietà del playbook per fare riferimento ai dati nello Script Python.

Le proprietà dei playbook che potete aggiungere sono:

- Stringa
- Numero Booleano
- Oggetto
- Array

Prima di poter effettuare il test, configurate i vostri input dello Script. Vediamo un rapido esempio su come configurare gli input e utilizzare il riquadro dello Script.

1. Dalla scheda Script, nel riquadro degli Input, cliccate su Aggiungi proprietà per definire gli input, inclusi eventuali sotto-input.
2. Cliccate sull'icona matita per modificare il nome della proprietà.
3. Scrivete il vostro codice nel pannello Script.

TEST DELLO SCRIPT

Volete testare il vostro Script prima di continuare a costruire il playbook? Nell'azione Script, dalla scheda Test, potete ora vedere gli Input a sinistra e lo Script a destra.

Il riquadro Risultato nella parte inferiore mostra i risultati del test. I risultati variano, quindi oltre alla base dei tipi di proprietà, e a seconda degli input selezionati, gli output dell'azione possono restituire proprietà aggiuntive. Queste sono gli output scoperti, che potete promuovere e/o eliminare dalla scheda Outputs.

Script

ALLEGATO SCRIPT

Se avete bisogno di restituire un allegato o utilizzarlo come input nell'azione nativa Script, seguite le istruzioni seguenti:

ALLEGATO IN OUTPUT

Nel vostro playbook, seguite le istruzioni seguenti per configurare un allegato in output:

c Dal menu a discesa **Azione**, selezionate **Script**.

Chiamate questa azione **Restituisci allegato** e cliccate su **Configura**. Ci sono due modi per scrivere Python code per restituire un allegato. Vediamo entrambi!

1. Nella scheda Script, inserite il seguente codice:

```python
with action_inputs['file1'].open() as file1:
action_outputs['file1_text'] = file1.read()
action_outputs['file1_size'] = file1.size()
action_outputs['file1_mimetype'] = file1.mimetype()
action_outputs['file1_filename'] = file1.file_name
```

Potete ottenere la dimensione dell'allegato utilizzando il metodo **.size()**, e potete ottenere il tipo MIME dell'allegato utilizzando il metodo **.mimetype()**. Potete ottenere il nome dell'allegato utilizzando la proprietà **.file_name.** Tutto è mostrato nel codice sopra.

pythonCopy code

file2 = action_inputs['file2'].open() action_outputs['file2_text'] = file2.read() file2.close()

1. Cliccate su **Applica** per salvare le modifiche.

ALLEGATO IN INPUT

Potete utilizzare un allegato in input in uno script Python utilizzando un'azione nativa Script.

1. Dal menu a discesa **Azione**, selezionate **Script**.

Chiamate questa azione **Allegato di input** e cliccate su **Configura**.

1. Cliccate su **Aggiungi proprietà** e selezionate **Allegato**.

Cliccate sull'icona matita per modificare il nome. Ad esempio, potete cambiare il nome in **file1**.

1. Cliccate su **Seleziona una proprietà** e selezionate **Proprietà del playbook**.

Script

Il cassetto delle proprietà del playbook si apre e in base all'esempio, selezionereste l'oggetto per **first_file**. Poi tornate a Inputs e ripetete i passaggi 4 e 5, ma aggiungete l'oggetto per **second_file**.

1. Nella scheda Script, inserite il seguente codice:

pythonCopy code

```
with action_inputs['file1'].open() as file1: action_outputs['file1_text'] =
file1.read() action_outputs['file1_size'] = file1.size()
action_outputs['file1_mimetype'] = file1.mimetype()
```

Potete ottenere la dimensione dell'allegato utilizzando il metodo **.size()**, e potete ottenere il tipo MIME dell'allegato utilizzando il metodo **.mimetype()**. Entrambi sono mostrati nel codice sopra.

Potete anche scrivere il codice come segue:

pythonCopy code

```
file2 = action_inputs['file2'].open() action_outputs['file2_text'] =
file2.read() file2.close()
```

2. Cliccate su **Applica** per salvare le modifiche.

Ora entrambi i file sono mappati.

MFA

ABILITARE L'AUTENTICAZIONE A DUE FATTORI (2FA)

L'Autenticazione a Due Fattori, o 2FA, aggiunge uno strato aggiuntivo di sicurezza agli account utente. Ogni volta che gli utenti effettuano l'accesso, avranno bisogno di una password e di un codice di verifica.

È possibile imporre l'autenticazione a doppio fattore in tutta l'organizzazione. Gli utenti saranno quindi tenuti a configurare il 2FA e non saranno in grado di disabilitare l'impostazione.

Se si sceglie di non imporre globalmente il 2FA, gli utenti singoli saranno in grado di abilitare la configurazione del 2FA.

ABILITARE GLOBALMENTE L'AUTENTICAZIONE A DUE FATTORI

Per abilitare globalmente l'autenticazione a due fattori:

1. Dall'area di amministrazione, clicca su > per espandere Impostazioni, quindi seleziona **Account**.

2. Seleziona la scheda Sessioni e Sicurezza ed espandi **AUTENTICAZIONE**.

3. Attiva **Imponi in tutta l'organizzazione** per attivare il 2FA per tutti coloro che accedono alla soluzione dalla tua organizzazione.

ULTERIORI AZIONI DEGLI AMMINISTRATORI PER IL 2FA

Gli amministratori possono reimpostare la configurazione del 2FA per gli utenti secondo necessità. Per reimpostare l'account 2FA configurato individualmente per un utente, accedi e apri la pagina Utente. Apri la pagina del profilo dell'utente e seleziona la scheda Autenticazione. Clicca su **Reimposta**.

L'utente sarà invitato a configurare una nuova istanza di 2FA una volta che tenterà di effettuare nuovamente l'accesso.

Gli amministratori possono anche esentare utenti specifici dall'uso del 2FA. Per farlo, accedi all'utente specifico e attiva l'interruttore **Esenta** nella finestra del profilo utente dell'autenticazione.

Sicurezza e Conformità della soluzione SOAR

Il nostro SOAR consente di accedere e gestire in modo sicuro i contenuti. I controlli tecnici e fisici all'interno della soluzione SOAR impediscono la divulgazione dei contenuti e l'accesso non autorizzato agli stessi. L'infrastruttura è monitorata continuamente, e il personale di sicurezza interno ed esterno effettua regolarmente test di vulnerabilità.

La nostra piattaforma SOAR utilizza ampiamente l'automazione e la risposta alla sicurezza per segnalare attività sospette in tutti gli ambienti dei clienti. Internamente, i requisiti di riservatezza vengono comunicati ai dipendenti attraverso formazione e policy. I dipendenti sono tenuti a seguire la formazione sulla consapevolezza della sicurezza, che include informazioni, policy e procedure relative alla protezione dei dati dei nostri clienti.

SICUREZZA

La nostra soluzione fornisce diverse funzionalità di sicurezza per garantire la confidenzialità, l'integrità e la disponibilità delle informazioni dei clienti.

DATI A RIPOSO

Ecco come la nostra soluzione SOAR protegge i tuoi dati a riposo:

- Tutti i dati del cliente e gli snapshot dell'applicazione sono crittografati con l'algoritmo AES256 prima di essere archiviati su disco.
- Consente snapshot completi dell'istanza che supportano il ripristino in caso di disastro e il ripristino dello stato dell'applicazione conosciuto come "buono".
- Le voci nella libreria delle credenziali, così come le password degli utenti e degli asset, sono crittografate a riposo prima di essere archiviate nel database della soluzione, utilizzando l'algoritmo di crittografia AES con una chiave da 256 bit e un salt da 256 bit.

DATI IN MOVIMENTO

Tutti i dati del cliente e gli snapshot dell'applicazione sono crittografati con l'algoritmo AES256 prima di essere archiviati su disco.
Consente snapshot completi dell'istanza che supportano il ripristino in caso di disastro e il ripristino dello stato dell'applicazione conosciuto come "buono".
Le voci nella libreria delle credenziali, così come le password degli utenti e degli asset, sono crittografate a riposo prima di essere archiviate nel database della soluzione, utilizzando l'algoritmo di crittografia AES.

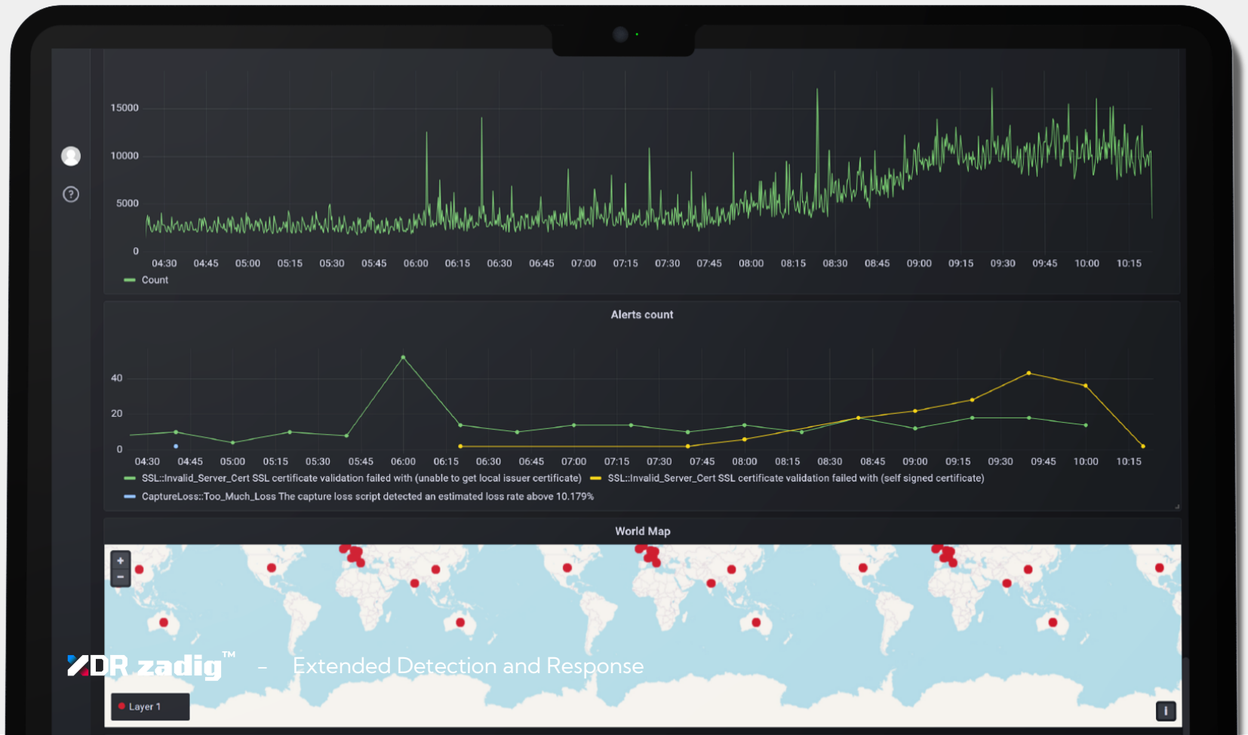
Sicurezza e Conformità della soluzione SOAR

SAML/SSO

Supportiamo la fornitura di account utente locale, Open LDAP, Microsoft Active Directory e SAML 2.0.

AUTENTICAZIONE A DUE FATTORI

Supportiamo la fornitura di account utente locale, Open LDAP, Microsoft Active Directory e SAML 2.0.



CONTROLLO DEGLI ACCESSI BASATO SUI RUOLI

La soluzione SOAR limita l'accesso alle informazioni utilizzando il Controllo degli Accessi Basato sui Ruoli (RBAC). Puoi applicare RBAC a ogni livello di oggetti: spazi di lavoro, dashboard, report, applicazioni, record e record individuali. Sono supportati controlli granulari fino al livello del singolo campo, e tutti i componenti supportano la possibilità di limitare l'accesso tramite utente, gruppo o ruolo.
Il SOAR può regolare dinamicamente le autorizzazioni su base per-record in base ai valori dei campi dell'utente/gruppo. Ad esempio, se un record è assegnato a Gruppo A, solo Gruppo A e gli amministratori avranno accesso a quel record. Se l'assegnazione del record cambia in Gruppo B, allora solo Gruppo B e gli amministratori avranno accesso ai record.

Gli amministratori hanno anche la possibilità di separare l'amministratore dell'account dall'orchestratore e dal progettista del playbook.

Spazi di lavoro e Dashboard

Gli utenti gestiscono la soluzione SOAR lavorando con record su spazi di lavoro, dashboard e card.

SPAZI DI LAVORO

Gli spazi di lavoro sono aree personalizzabili all'interno della piattaforma in cui è possibile organizzare e accedere agli strumenti e alle funzionalità che si utilizzano regolarmente. Gli spazi di lavoro possono includere applicazioni, dashboard, record, report e grafici. Gli amministratori possono cambiare lo spazio di lavoro e le dashboard predefinite per gli utenti. Tutti gli utenti possono passare a diversi spazi di lavoro e dashboard in base alle autorizzazioni impostate.

DASHBOARD

Le dashboard sono una rappresentazione visiva di record, report e grafici associati alle applicazioni nello spazio di lavoro. Uno spazio di lavoro può avere più dashboard, e gli utenti possono visualizzare diverse dashboard selezionando l'icona di navigazione DASHBOARD o WORKSPACE e scegliendo un'altra dashboard dalla lista. Gli utenti hanno accesso solo a spazi di lavoro, dashboard, record e report se sono stati autorizzati da un amministratore. Se una dashboard o un report esistente non è visibile, un amministratore dovrebbe verificare che all'utente siano state assegnate le autorizzazioni corrette.

CARD

Una card è un report o un oggetto HTML associato a una dashboard. Puoi avere più card su una singola dashboard. Le card sono completamente personalizzabili e possono essere ridimensionate e riordinate sulla dashboard da amministratori o utenti con accesso appropriato. Gli utenti possono fare clic all'interno di una card per visualizzare un elenco di record associati a quel grafico o report, o fare clic su un punto dati all'interno di un grafico per visualizzare un elenco filtrato di record corrispondenti a quei dati. Sono disponibili vari tipi di grafici diversi per visualizzare le informazioni sui record in modo significativo, rendendo dashboard, card e grafici strumenti potenti per trovare record rapidamente e visualizzare dati.

Brevetti

TRANSPORT ENCRYPTED PROTOCOL (TEP)

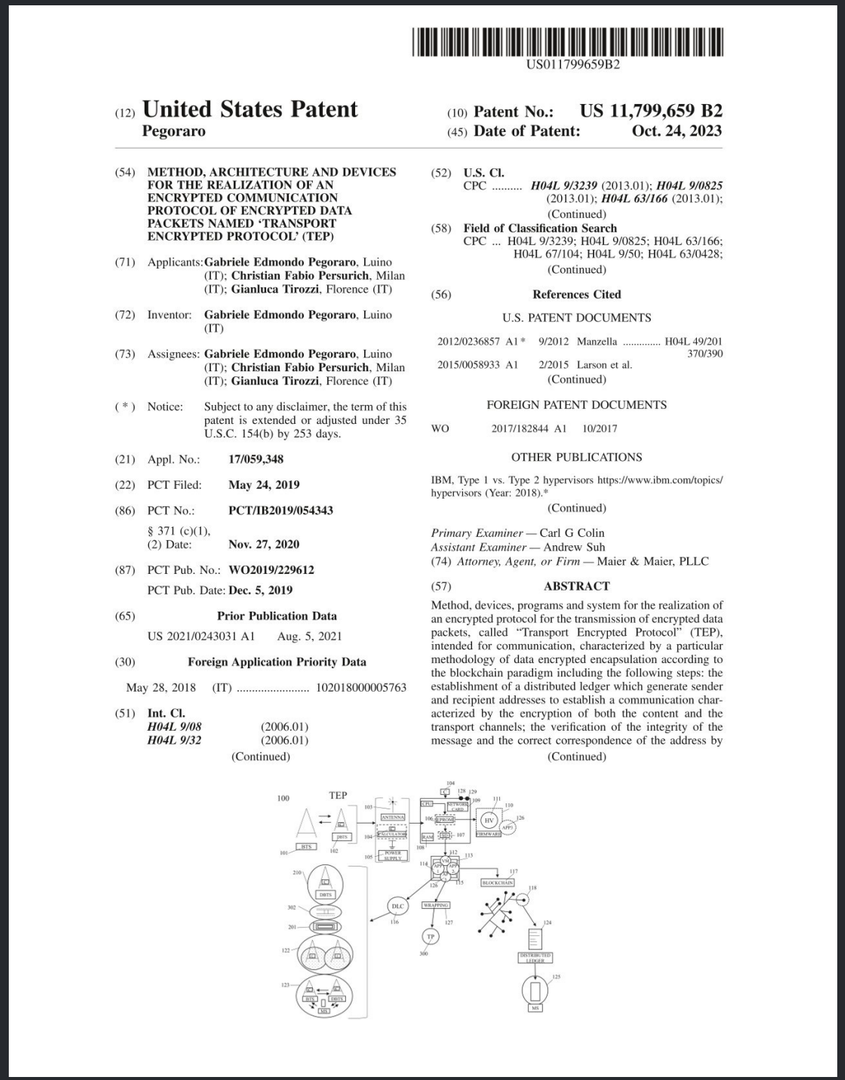
bitCorp dispone di cinque brevetti tra cui il Transport Encrypted Protocol (TEP), un innovativo protocollo di trasmissione dati modulare ad alta sicurezza in cui per la prima volta viene applicata la blockchain alle telecomunicazioni.

Tutelato da brevetto UE e USA, è in grado di coprire l'intera pila OSI e di integrarsi in modo trasparente in virtualmente qualsiasi datalink ed offre, senza bisogno di ulteriori integrazioni, piene garanzie di confidenzialità, integrità e recapito dei messaggi.

Ideato per scopi militari, il TEP permette la creazione di reti mesh sicure anche in contesti a basso livello di fiducia, senza alcun tipo di centralizzazione e in generale senza singoli point-of-failure.

La sua altissima velocità di riorganizzazione e la sua enorme tolleranza ai guasti lo rende infine particolarmente indicato per applicazioni real-time, quali ad esempio la gestione di smart grid o l'utilizzo con Autonomous Car (AC).

Inoltre, grazie all'impiego della blockchain, è impermeabile ad attacchi DDoS, Man-in-the-Middle e Spoofing.



US011799659B2

(12) **United States Patent**
Pegoraro

(10) **Patent No.: US 11,799,659 B2**
(45) **Date of Patent: Oct. 24, 2023**

(54) **METHOD, ARCHITECTURE AND DEVICES FOR THE REALIZATION OF AN ENCRYPTED COMMUNICATION PROTOCOL OF ENCRYPTED DATA PACKETS NAMED 'TRANSPORT ENCRYPTED PROTOCOL' (TEP)**

(71) Applicants: **Gabriele Edmondo Pegoraro**, Luino (IT); **Christian Fabio Persurich**, Milan (IT); **Gianluca Tirozzi**, Florence (IT)

(72) Inventor: **Gabriele Edmondo Pegoraro**, Luino (IT)

(73) Assignees: **Gabriele Edmondo Pegoraro**, Luino (IT); **Christian Fabio Persurich**, Milan (IT); **Gianluca Tirozzi**, Florence (IT)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 253 days.

(21) Appl. No.: **17/059,348**

(22) PCT Filed: **May 24, 2019**

(86) PCT No.: **PCT/IB2019/054343**
§ 371 (c)(1),
(2) Date: **Nov. 27, 2020**

(87) PCT Pub. No.: **WO2019/229612**
PCT Pub. Date: **Dec. 5, 2019**

(65) **Prior Publication Data**
US 2021/0243031 A1 Aug. 5, 2021

(30) **Foreign Application Priority Data**
May 28, 2018 (IT) 102018000005763

(51) **Int. Cl.**
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***H04L 9/3239*** (2013.01); ***H04L 9/0825*** (2013.01); ***H04L 63/166*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC ... H04L 9/3239; H04L 9/0825; H04L 63/166; H04L 67/104; H04L 9/50; H04L 63/0428;
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

2012/0236857 A1 * 9/2012 Manzella H04L 49/201 370/390
2015/0058933 A1 2/2015 Larson et al.
(Continued)

FOREIGN PATENT DOCUMENTS

WO 2017/182844 A1 10/2017

OTHER PUBLICATIONS

IBM, Type 1 vs. Type 2 hypervisors https://www.ibm.com/topics/hypervisors (Year: 2018).*
(Continued)

Primary Examiner — Carl G Colin
Assistant Examiner — Andrew Suh
(74) *Attorney, Agent, or Firm* — Maier & Maier, PLLC

(57) **ABSTRACT**

Method, devices, programs and system for the realization of an encrypted protocol for the transmission of encrypted data packets, called "Transport Encrypted Protocol" (TEP), intended for communication, characterized by a particular methodology of data encrypted encapsulation according to the blockchain paradigm including the following steps: the establishment of a distributed ledger which generate sender and recipient addresses to establish a communication characterized by the encryption of both the content and the transport channels; the verification of the integrity of the message and the correct correspondence of the address by
(Continued)

Products

XDR zadig™

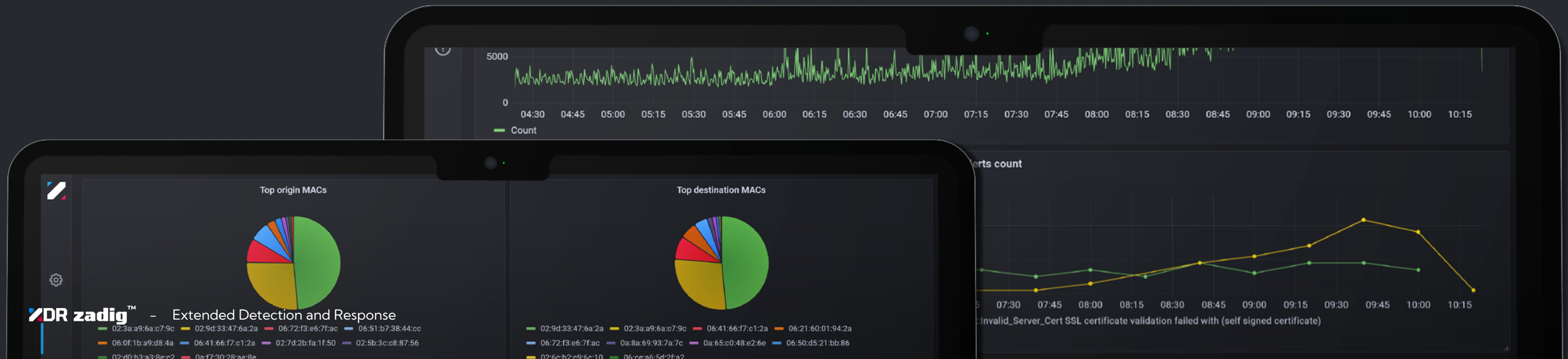
Intrusion Detection Prevention System modulabile ibrido (software+hardware) ideato per monitorare grandi infrastrutture di rete, tipicamente del segmento Large Enterprise e PMI.

SMART zadig™

Declinazione di ZADIG XDR, soluzione ibrida destinata a un segmento di mercato caratterizzato da infrastrutture più semplificate con poche o scarse competenze in cybersecurity, quali micro imprese.

N

Soluzione cybersecurity totalmente software destinata a studi professionali e liberi professionisti



XDR zadig™ – Extended Detection and Response

bitCorp™

Sede Legale: Via Monte Bianco 2/A, 20149, Milano
Sede di Rappresentanza: Galleria del Corso 4, 20121, Milano
Sede Operativa: Via Carlo Freguglia 10, 20122, Milano

www.bitcorp.it