



THE INTEGRATED
CYBERSECURITY SOLUTION
FOR MEDIUM
AND LARGE COMPANIES.



Company

VISION

bitCorp is a cybersecurity firm forged by the expertise of former intelligence operatives.

At bitCorp we redefine digital defense with a distinctive edge, setting ourselves apart from competitors through a profound understanding of hacking methodologies and yet-to-be-discovered vulnerabilities.

Our founders, seasoned veterans from the lawful interception market, infuse bitCorp with a wealth of experience that transcends conventional cybersecurity paradigms. This unique background equips us with insights that propel us beyond the competition, enabling us to stay one step ahead in the ever-evolving landscape of cyber threats.

Secured by Professional Strikers

ZADIG XDR

At the core of our offerings stands our flagship product ZADIG XDR – the Intrusion Prevention Detection System (IPDS). What makes our XDR a game-changer is its unparalleled customization capabilities. Unlike traditional solutions, our system isn't just adaptive; it's a cybersecurity chameleon, tailoring its defenses to precisely match the needs of our clients. From industry-specific nuances to unique organizational challenges, bitCorp delivers security that is as individual as our clients themselves.

As you navigate the digital frontier, trust bitCorp to be your vigilant guardian. Our commitment goes beyond conventional security measures; we strive to provide an experience where protection is seamlessly integrated, intelligence is at the forefront, and customization is not just a feature but a philosophy.

Welcome to a new era of cybersecurity. Welcome to bitCorp.

Company

CHRISTIAN PERSURICH, PHD CEO

A former intelligence operator, Criminologist and researcher at the Università Cattolica del Sacro Cuore, he has 20 years' experience, in Italy and abroad, in countering terrorist events and carrying out complex investigations into violent crimes (murders, kidnappings, etc.).

He follows the Confucius maxim "Choose a job you love, and you will never have to work a day in your life."

GIANLUCA TIROZZI, PHD PRESIDENTE

A former intelligence worker and researcher in Social Sciences at IESE, Business School of the University of Navarra, he has gained experience in foreign theaters of operation in information source and human resources management, specializing in countering Islamist terrorism.

A profound connoisseur of the Arabic language and pan-Islamic cultures, his motto is "one man's luck is always another man's."



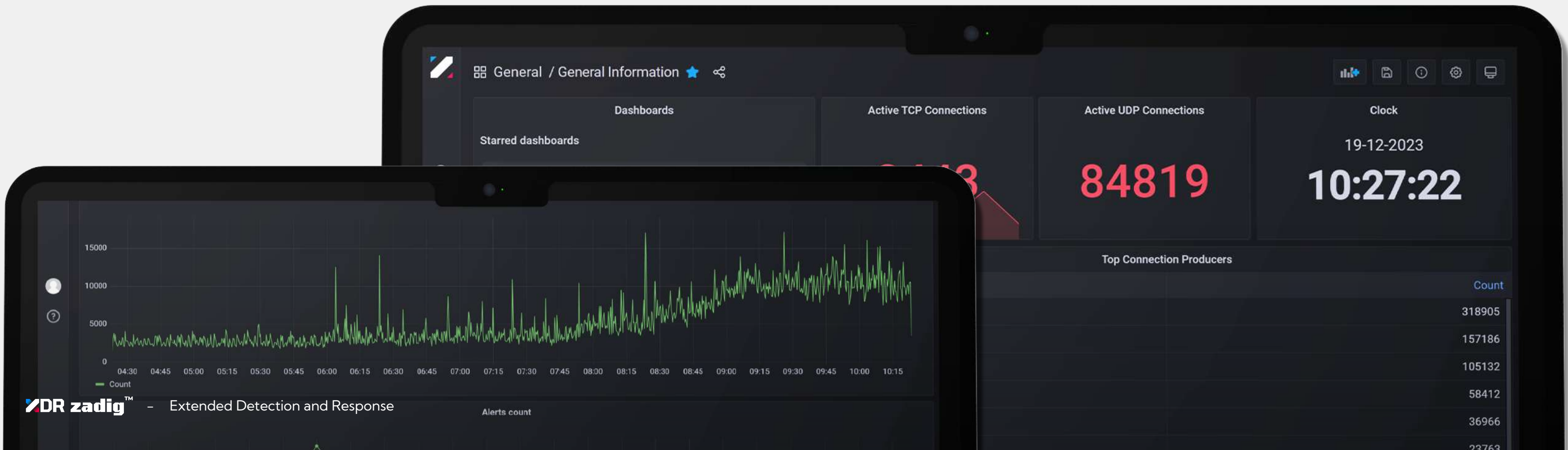
Introduction

Our Extended Detection and Response (XDR) solution, called ZADIG XDR, integrates a range of advanced cybersecurity features for effective and real-time recognition of threats.

ZADIG XDR is a modular platform on which monitoring, detection, and response processes can be designed based on the threat models that characterize an organization's business. This is possible thanks to various modules that

allow observation of phenomena occurring on the network, devices, and services. To handle scenarios that don't allow for the static definition of a potential problem, the ZADIG XDR system is also equipped with an Artificial Intelligence engine capable of assessing anomalous phenomena and predicting their recurrence.

The Log Aggregation and Analytics system of ZADIG XDR enables the analysis of data from various sources and features a control dashboard that allows the user to interact quickly and intuitively with all the information collected by the solution, including incident management events, threat intelligence feeds, logs from network devices, and error reporting.



Data Ingestion Pipeline

INGESTION PIPELINE

ZADIG XDR provides an efficient data ingestion pipeline that automates the data collection process, ensuring that data from various sources is integrated, processed, and then stored consistently according to defined requirements.

Our XDR solution is highly flexible and enables the integration of data from numerous types of sources (e.g., logs from other environments/manufacturers). In fact, the component responsible for managing the ingestion pipeline can collect data from different sources through input plugins such as syslog or TCP. **The collection of data from a new source can be configured at any time**, even after the actual implementation of the XDR platform, to accommodate any changes in the monitored organization's infrastructure.

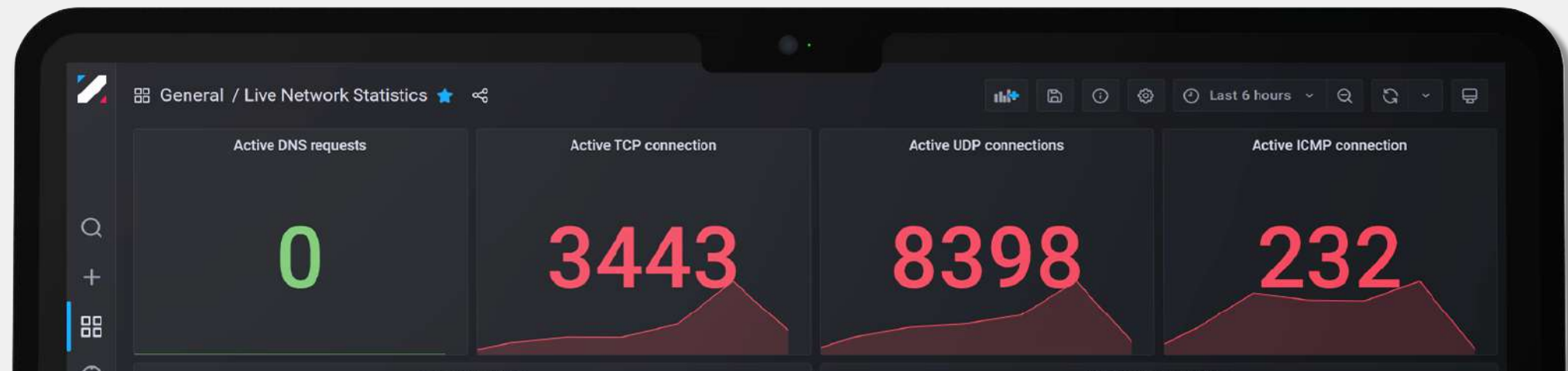
The main log ingestion

methodologies supported are:

- **SYSLOG Collector**
- **CSV Collector**
- **DB Collector**
- **FTP Collector**
- **NetFlow Collector**
- **Windows Event Collector**
- **Kafka Collector**
- **HTTP**
- **Log collection using Filebeat**

The solution natively integrates **Kafka as the log collection technology**. For example, it is used for ingesting monitored data from its integrated IDPS module (when applicable). **The collection methodology is based on the SYSLOG protocol** for integrating logs from other devices or equipment within the infrastructure, **and a file-based collection methodology** for integrating logs from other components that produce a textual alert feed in files.

Furthermore all other collection approaches can be easily activated based on specific requirements.



Data Ingestion Pipeline

Below is an example of a Logstash configuration file that enables the integration of logs from a network firewall with pfSense operating system installed:

```
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 addition, our XDR solution **provides native support for integration with Azure AD**. To efficiently collect logs from Azure Active Directory (AD), it is necessary to configure Azure Monitor to export logs to Event Hub. The system features an already optimized pipeline for collecting data from Event Hub.

For integrating logs from Microsoft AD, activation of a Windows service on the on-premises domain controller server is required. This software is responsible for collecting and sending logs to the ingestion component.

In cases where any other Identity solution does not directly support log integration with our XDR solution and if that solution integrates data into a Security Information and Event Management (SIEM), it would be possible to collect these logs by configuring the SIEM as an additional direct data source for the XDR platform."

Data Ingestion Pipeline

DATA REPOSITORY

The XDR solution is designed to interact with data repositories located on-premises or in the cloud. Specifically, the data repositories natively integrated into the solution include **AWS Opensearch, Microsoft Azure Log Analytics, and on-premises Elasticsearch**. These repositories support a distributed search engine with an HTTP web interface and documents in JSON format.

The data pipeline management component will need to interact with the aforementioned repository to store data sent from each source using a dedicated output plugin. The only information required by the plugin to correctly save the data within the repository is the address or DNS name of the repository and the index/table containing the data.

Below is an extract from the configuration file to save data to an Opensearch cluster on 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
}
```

Below is an extract from the configuration file to save data to 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"
}
```

When the repository is in the cloud, through a log collection adapter, also deployed directly in the cloud, it is possible to integrate data sources, supporting various protocols such as Syslog (CEF, LEEF, CISCO, CORELIGHT, or RAW - UDP, TCP, or Secure TCP, allowing for the configuration of a minimum TLS 1.2 version), CSV, Databases (MySQL, PostgreSQL, MSSQL, or Oracle), Cloud (AWS, Azure, Google), Files and Folders, FTP, NetFlow, and Windows Events.

On-premises, there are potential log aggregators that simply collect data from sources at the site, apply completely customizable parsing logic to the data, and send the result to the cloud. All of this happens in real-time without any information being temporarily stored locally.

Data Ingestion Pipeline

The on-premise log aggregators support reliable deployment

and are compatible with the following hypervisors

both cloud and private:

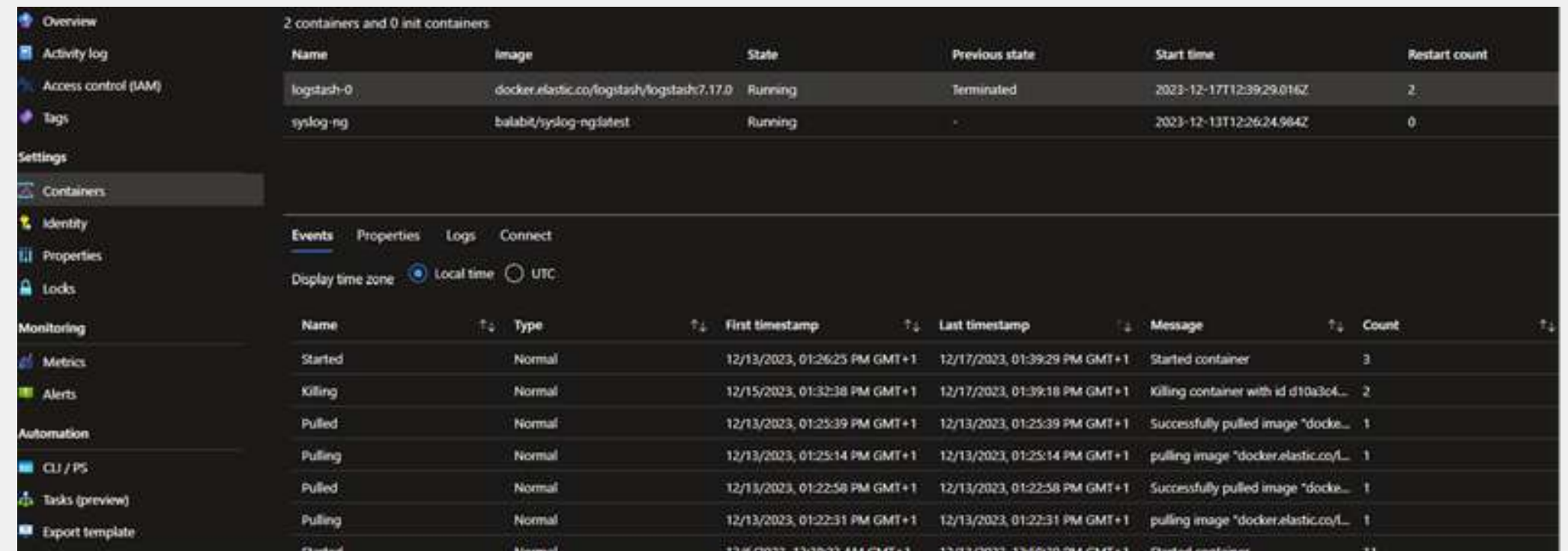
- Amazon Web Services (AWS)
- Microsoft Azure
- Microsoft Hyper-V
- VMware ESXi

It's possible to deploy the log aggregators on a virtual machine (VM) or on a container.

Below is an example of deploying the log aggregator on a virtual machine running on Amazon Web Services (AWS):



Below is an example of deploying the log aggregators on containers on Microsoft Azure:



Data Ingestion Pipeline

DATA RETENTION POLICY

ZADIG XDR natively stores data on Elasticsearch or an equivalent cloud storage. The system allows the creation of a lifecycle policy on the data to activate a specific retention policy, fully customizable according to the needs of the specific organization receiving the solution.

The data is stored within the repository, divided by indices, and it is possible to set a specific retention policy on each index. For example, generic data (not related to cybersecurity incidents) is stored in ad-hoc created database indices, possibly categorized, on which a retention policy of choice can be applied (e.g., at least 30 days). Data of another nature, such as those related to cybersecurity incidents, is stored in different indices to which a longer retention period can be applied (e.g., at least 180 days).

In order to retain data (even just specific types) for an unlimited time, the retention policy needs to be set accordingly.

Our XDR solution allows the division of data retention into hot and cold, and considering some types of repositories, it enables the addition of the warm retention state.

The categorization is managed as follows:

- **Hot:** The index is continuously updated and frequently queried.
- **Warm:** The index is no longer updated but is still queried.
- **Cold:** The index is neither updated nor queried.

DATA AND COMMUNICATION CONFIDENTIALITY

The data maintained in the cloud repository is handled with full respect for privacy. They are stored in the organization's cloud space under monitoring and **encrypted both in transit and at rest using sophisticated encryption algorithms** such as AES-256. Access to them is managed granularly and guaranteed only to entities that require access for the functionality of the entire solution.

Communications between various components of the solution are fully encrypted using the TLS protocol. The minimum version of the TLS protocol that can be used for encrypting data in transit is TLS v1.2. Each input plugin is configured to accept encrypted communications; in the event the plugin does not support TLS, a dedicated TLS proxy is provided for secure data reception. Similarly, our XDR solution transmits data to the repository using the TLS protocol.

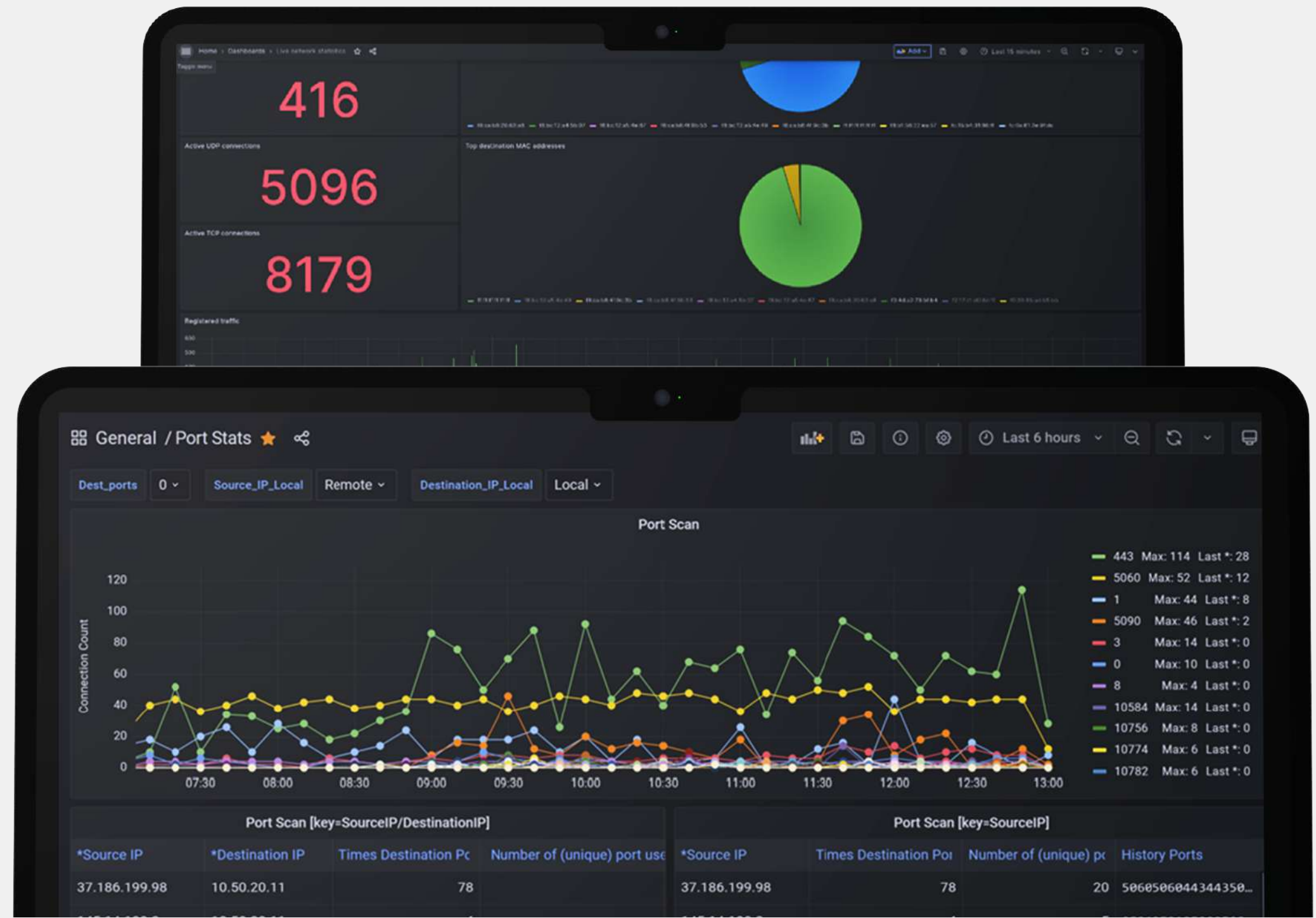
It is specified that each component integrated into our XDR solution offers APIs for automation.

Management interface

ZADIG XDR is managed through a web-based graphical interface. The management dashboard of our XDR solution provides analysts with the visualization of various types of information.

The interface natively integrates the display of priority events by setting up a dedicated section for alerts on the platform's homepage. Through alerts, analysts can access the history and contextual information necessary for researching the cause-and-effect chains that triggered the alert. In this context, all available data sources, such as threat intelligence tools, RSS feeds from alarm triage platforms, ticketing platforms, and public discussion forums, can be activated.

Below are two examples of dashboards:



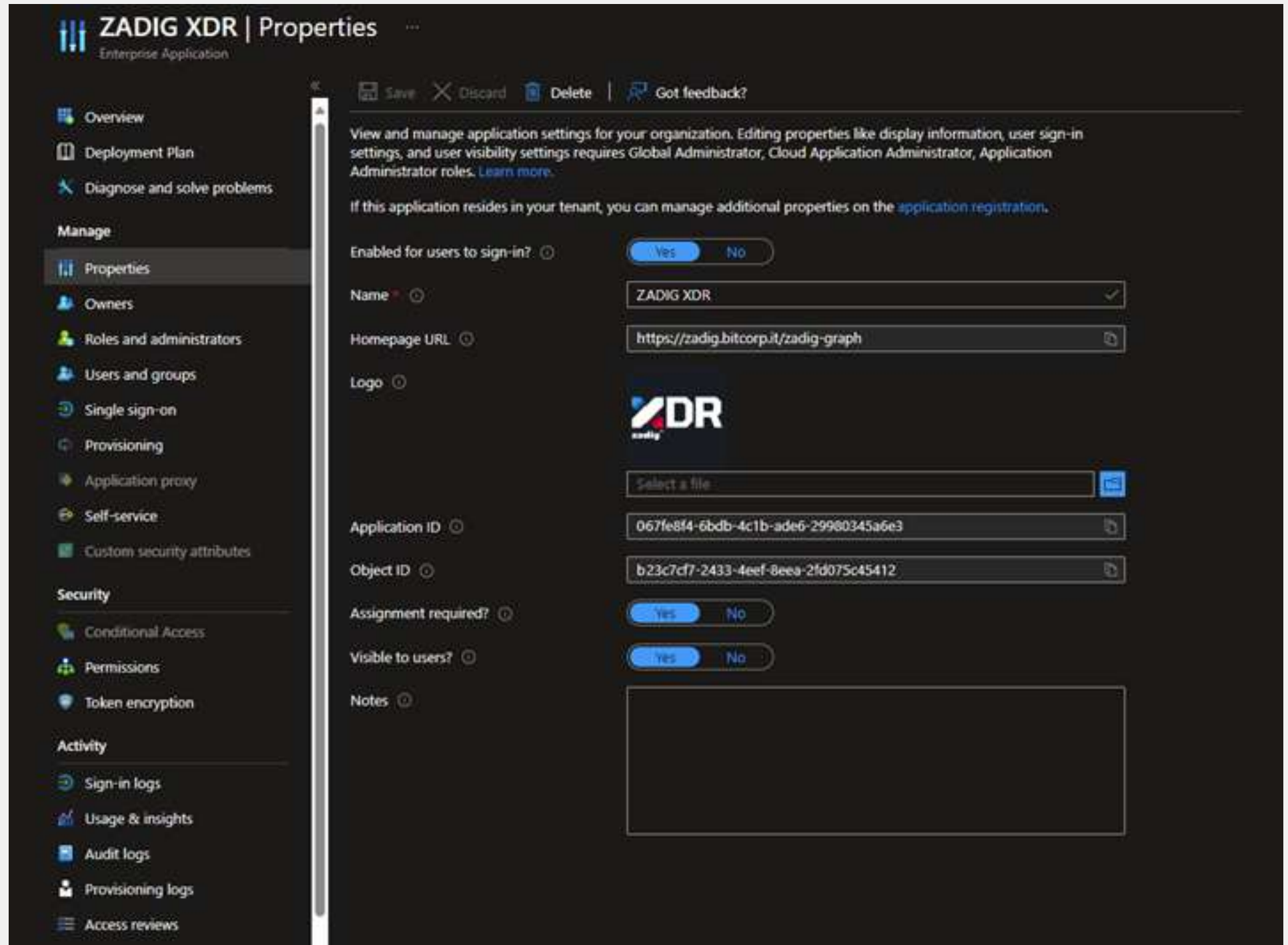
Management interface

SINGLE SIGN ON ACCESS (SSO)

To access the management platform, SAML and OAuth2 protocols are supported for access management through Single Sign-On (SSO) with Multi-Factor Authentication (MFA) support.

For illustrative purposes, the following are the main steps to use the Azure AD tenant as the identity provider. To configure access to the management portal via SSO, it is necessary to create an application on Azure AD. To enable a user in the directory for access, the user must be included as enabled for access through the 'Users and groups' menu option.

Below is an example screenshot of an Enterprise Application for managing SSO access:



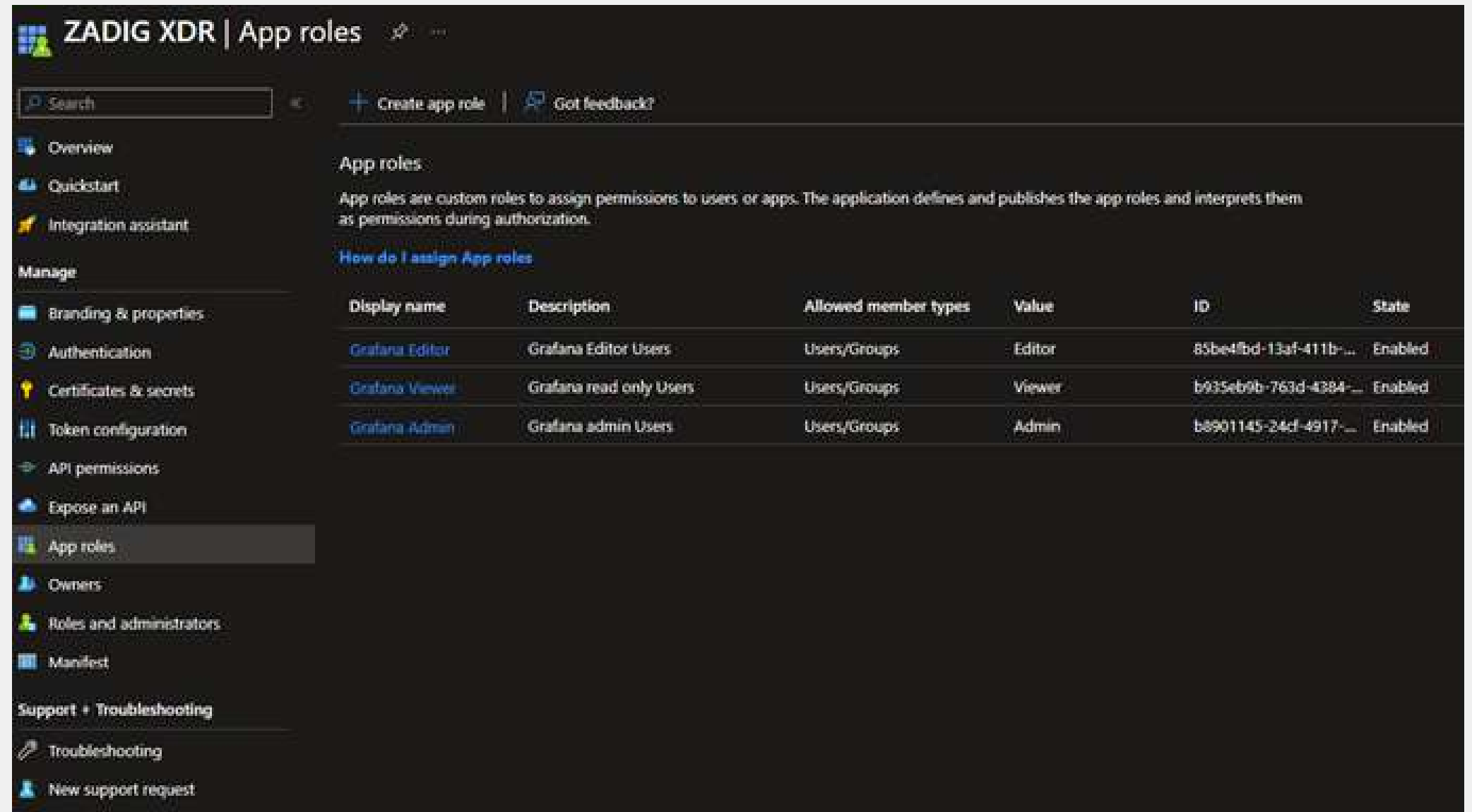
Management interface

The enterprise application allows the definition of roles assignable to users in the directory for access to the management platform.

Here is an example of possible roles that can be defined.

After configuring the application on the tenant, it is necessary to enable Azure AD OAuth2.0 in the configuration file of the visualization component of the XDR solution.

Once the environment is configured for Single Sign-On (SSO) with Azure AD, from the Enter ID portal, all sign-in records made by various users can be viewed.



The screenshot shows the 'ZADIG XDR | App roles' page in the Azure AD portal. The page title is 'ZADIG XDR | App roles'. Below the title, there is a search bar, a '+ Create app role' button, and a 'Got feedback?' link. The main content area is titled 'App roles' and contains a descriptive paragraph: 'App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.' Below this, there is a link 'How do I assign App roles'. A table lists the defined app roles:

Display name	Description	Allowed member types	Value	ID	State
Grafana Editor	Grafana Editor Users	Users/Groups	Editor	85be4fbd-13af-411b-...	Enabled
Grafana Viewer	Grafana read only Users	Users/Groups	Viewer	b935eb9b-763d-4384-...	Enabled
Grafana Admin	Grafana admin Users	Users/Groups	Admin	b8901145-24cf-4917-...	Enabled

The left sidebar contains navigation options: Overview, Quickstart, Integration assistant, Manage (Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest), and Support + Troubleshooting (Troubleshooting, New support request).

Management interface

ROLE BASED ACCESS CONTROL (RBAC)

As previously specified, **for access to the management dashboard of our XDR solution, it is expected that each user is associated with a role with specific permissions.** The list of possible predefined base roles that can be assigned to each user is defined below. **It is noted that the list can be customized by adding specific roles** to meet the needs of the organization receiving the solution:

- **Admin:** has access to all organization resources, including dashboards, users, and teams.
- **Editor:** can view and edit dashboards, folders, and playlists.
- **Viewer:** can only view dashboards and playlists.

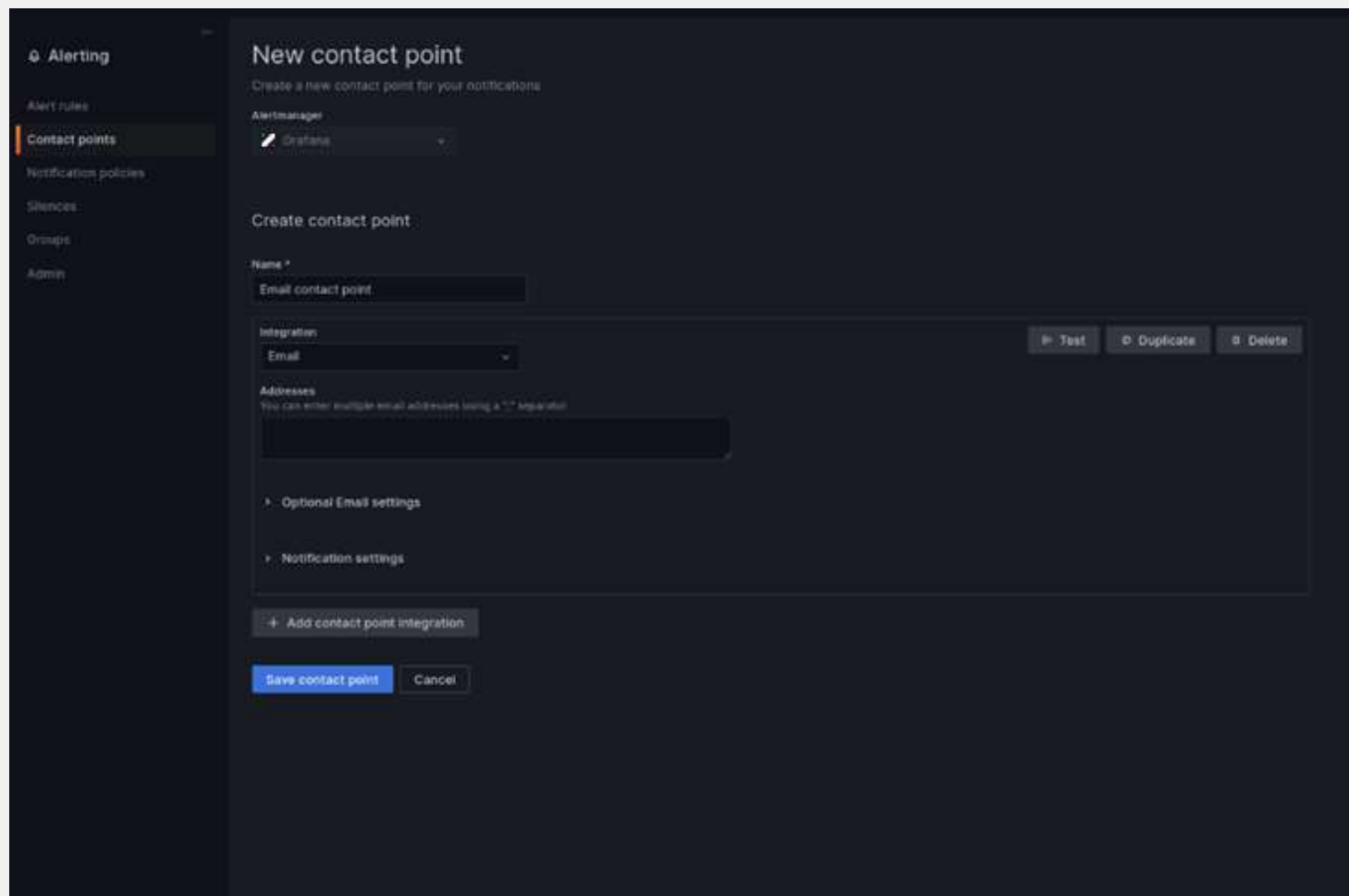
The permissions mapped to each of the three roles are available in the following table:

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		

Notification of alarms and reporting

The management dashboard of our XDR solution provides the functionality to define the so-called contact points to which alert notifications can be sent. Each contact point allows configuring the methodology of sending the notification.

Below is a screenshot showing the configuration of a contact point with email notification method:



Many other notification channels are supported, such as Telegram, Slack, Discord, and Webhook for any other Instant Messaging (IM) platform.

From the management platform, it is possible to configure alerts to monitor specific events relevant to the scenario under consideration.

Each alert can be associated with a notification policy active on a contact point. By doing so, the activation of the alert will be automatically notified to the selected contact point. The contact point could be another system or network device capable of responding to the alert. Indeed, through the activation of Webhook, it is possible to notify the incident by enriching the message with metadata and useful information, for example, to network devices (firewalls) to apply countermeasures parameterized on the metadata itself (blocking a specific IP address).

For each alert, **it is possible to configure a notification sending methodology**, choosing one or more contact points. In addition, **the generation of an alert in the XDR is appropriately notified to other active cybersecurity systems on the infrastructure (SIEM, SOAR).** Simultaneously with the notification, a series of information (metadata) useful for the generation of a security report is provided to the aforementioned systems, including all necessary contextual information, including a screenshot snippet of the graphical display of the alert that triggered the alarm. The actual generation of the report is delegated to the SOAR module, which triggers the relevant document production as deemed appropriate.

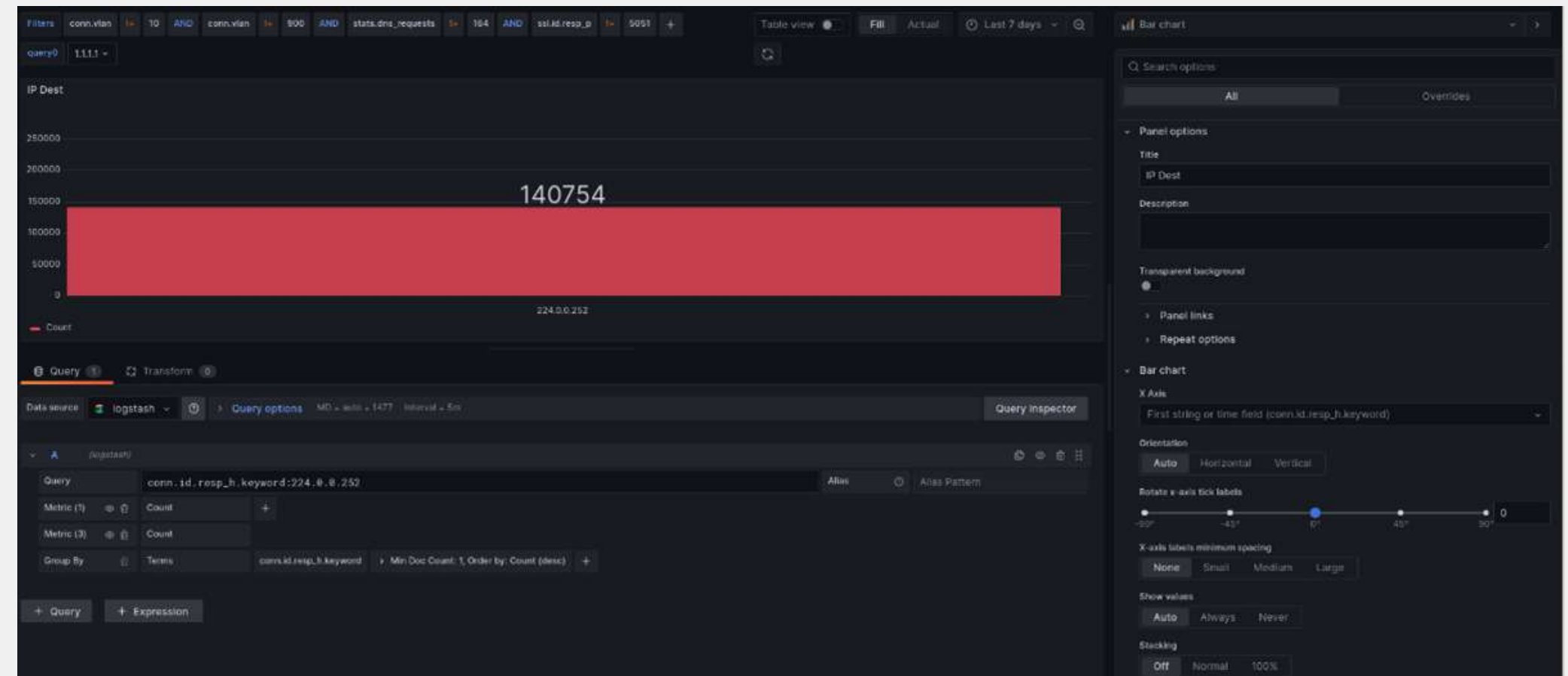
Threat Detection

The identification of threats occurs through two distinct approaches:

- 1. Signature-Based:** Static recognition based on known malicious patterns, with regularly updated signature files.
- 2. Behavioral-Based:** Dynamic recognition using Machine Learning models.

Both approaches also work on historical data stored within the repository, which can be queried for the entire set retention period. The management platform enables manual search for Indicators of Compromise (IOC) in the collected data. For instance, knowing that a specific destination IP is an IOC, indicating evidence of some type of attack or threat. The management platform of our XDR solution allows the generation of specific queries to search for this data within all destination IPs associated with connections.

Below is an example query to perform the search just mentioned, assuming you want to search for the destination IP 224.0.0.252:



Threat Detection

The query is set to also return the count of the number of connections involving that IP. Additionally, as mentioned earlier, the platform allows the configuration of an alert that **sends a notification each time the IP appears within a connection.**

The solution integrates Machine Learning models designed for the detection of anomalous behaviors within the monitored infrastructure. To ensure adequate performance metrics, these models are trained using data from the infrastructure itself, regardless of their source (logs from network devices, network traffic intercepted by the probe, logs from identity solutions, events from the static ISD component, etc.). The solution comes with a series of pre-configured models for incident detection, although it is possible to develop additional ML models for the specific recognition of anomalous behaviors characteristic of the business of the monitored organization.

The models can be configured to work on a specific input bucket, which corresponds to a series of indices in the data repository. Each model, configured in this way, is able to learn the standard behavior of the network through data from multiple sources to detect suspicious behaviors on devices not directly monitored (devices on which no agent has been installed). This is crucial for monitoring the behavior of devices owned by guest or occasional users who, for obvious reasons, are not directly monitored by the cybersecurity solutions implemented by the organization.

Below the JSON related to one of the integrated models in the XDR solution is shown below:

```
{
  "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
  }
}
```


Threat Detection

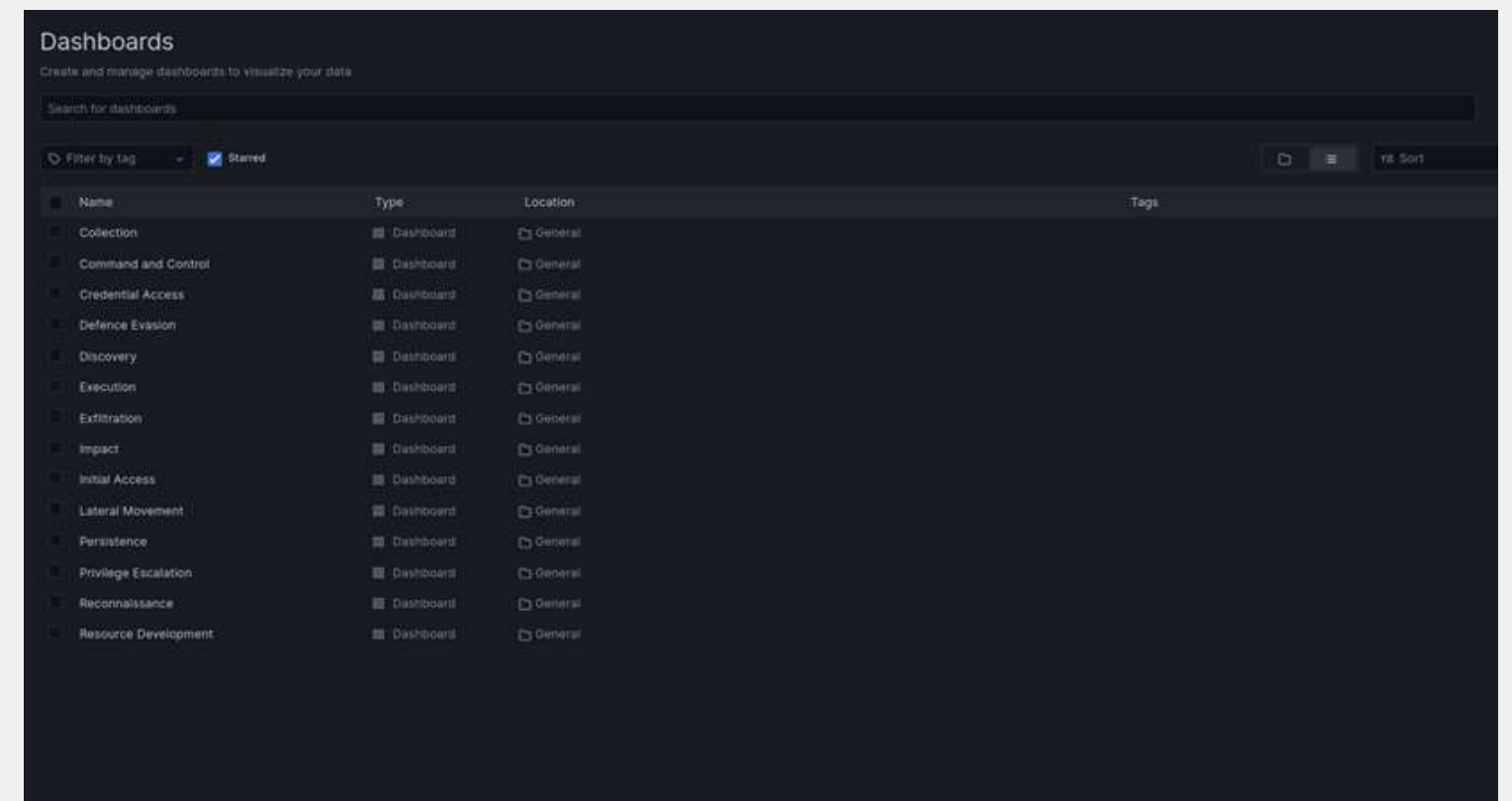
Below is an example of configuration input and output buckets. The first indicates the set of data on which the model will be trained, while the second represents the container in which the model will store the predictions made:

```
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  
  
#
```

Furthermore, the Machine Learning models used by the XDR solution assign a score to each predicted event. The assigned score indicates the **priority and, therefore, the severity of the recently occurred event**. Once a certain score threshold is surpassed, the event is considered anomalous and, therefore, prioritized.

Using ML models, the solution performs behavioral-based recognition of Indicators of Compromise (IOC). Each IOC can be modified, and it's possible to add new custom indicators based on what was mentioned in the previous requirement, assigning the corresponding ATT&CK category each time.

Each macro-category defined by the framework is associated with a specific dashboard on the platform. Each dashboard contains a series of visualizations, each set up to detect IOCs of attacks and threats related to the category associated with the dashboard itself.



Data Parsing and Querying

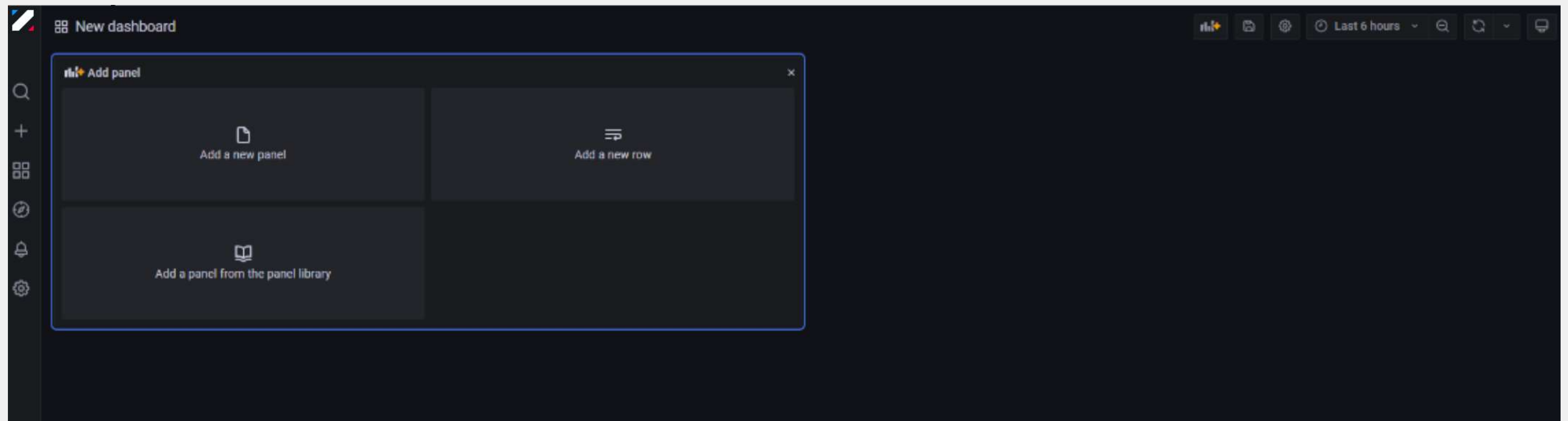
Our XDR solution includes standard process and a specific language for executing queries aimed at analyzing available information.

Various pieces of information can be organized into dashboards, each containing different visualization panels.

set up a search query to be executed on a specific data source, i.e., on a specific index or table present in the data repository.

Each panel must be associated with a visualization through which to display the data.

The screen for creating a panel allows you to

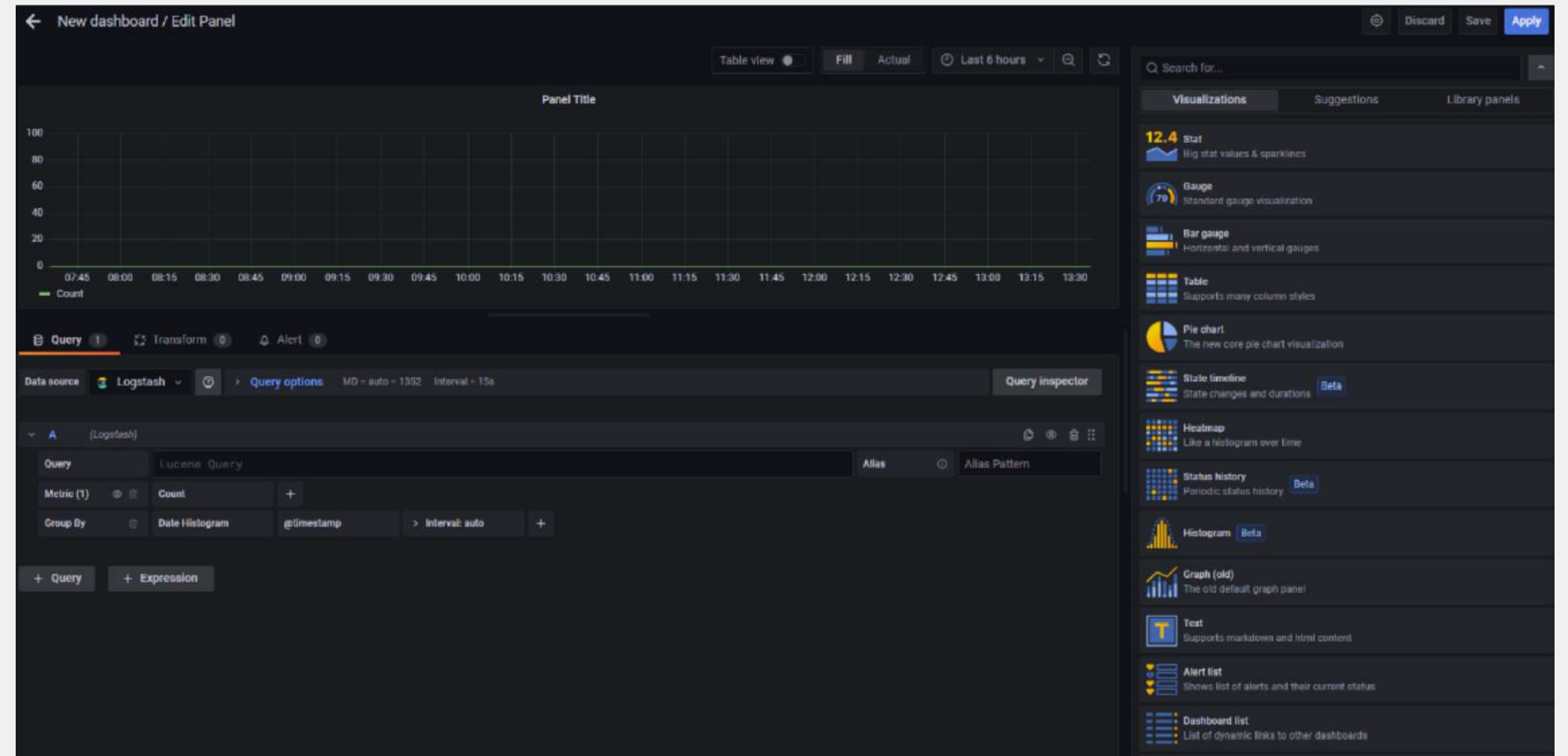


Data Parsing and Querying

Below is the screen for creating a panel:

The query language provided by our solution supports also, the following features: **filtering to identify specific conditions, selecting a subset of fields to display, transforming certain fields returned by the query, calculating averages, counts, etc., the ability to sort results, and handling deduplicates.** There is a set of predefined queries. Each query can be associated with a dashboard to enable continuous monitoring or to run it on-demand on data within a specific time interval.

Each query can be transformed into a BIOC (Behavioral Indicator of Compromise), associating an alert with it. This allows monitoring and detecting new suspicious events or searching for that BIOC in existing data that triggers it.



Data Parsing and Querying

DATA PARSING

There is a specific platform available for managing files containing the configuration of parsing rules, effectively filters applied to raw data ingested by the data ingestion component. These filters **allow the elimination of potentially unnecessary data, aiming to reduce storage costs**. Additionally, they enable data enrichment with tags that can be used by the rest of the collection flow. For example, below is an extract of the configuration that adds tags if certain conditions are met:

```
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}" ]  
  }  
}
```

Data Parsing and Querying

Parsing filters also allow the addition of valuable information for threat detection, such as geolocation of an IP address. Below is a snippet of the configuration created to fulfill the purpose mentioned.

```
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] {  
        geoup {  
            source => "[destination][ip]"  
  
#MMR#            database => "/var/lib/GeoIP/GeoLite2-City.mmdb"  
            target => "[destination][geo]"  
        }  
  
        geoup {  
            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™

DR

EDR MODULE



EDR MODULE

ZADIG XDR offers an EDR (Endpoint Detection and Response) software. It consists of a set of projects that implement a unified cross-platform service core, combining multiple (possibly native) modules and is consistently distributed across various target platforms. The actual agent is designed to operate in the background and respond to various types of events.

The XDR solution includes a **persistent agent** whose data is displayed and managed through a unified platform with endpoint management and protection features. It allows correlation with data from all other integrated sources. **Initially designed to support file system access events, it can easily accommodate other event sources.**

The solution supports non-persistent installations to the extent that the client already has an automatic application deployment management solution. **Alerts generated by the platform can be processed by SOAR to activate agent distribution profiles on devices involved in the alert.**



EDR MODULE

MODULE INSERTION

The resolution of dependencies is done through autovac using a configuration file. All modules can be considered event producers (generators) or consumers (handlers). They all expose or connect to some common interfaces. Depending on the target platform and desired features, it is possible to configure a different set of modules for dependency resolution based on the distribution.

NATIVE EXTENSIONS:

Modules may depend on specific features or APIs of the platform. In this case, the module provides all the required native extensions, e.g., bindings, libraries, drivers, or additional applications. In no case should other interfacing modules be concerned with how such platform specificity is implemented; everything remains hidden within the module.

APP HOSTS

The composition root is part of a library that can be referenced by various types of application hosts. This makes it easier to develop, test, and deploy the agent within multiple minimal wrappers that best suit the endpoint device. For example, the same base code of the agent service can be run as a console application or background service.

USER APPLICATIONS

A certain number of features require user interactions. Their implementation is part of platform-specific applications that best match various use cases across different classes of endpoint devices.

CONFIGURATION

The core service of the agent may include a module that requires out-of-package parameters to be set for the module to be functional. User applications must have write access – under certain conditions – to shared configuration locations that the core agent may read at startup.

Since the core of the agent service will likely run with elevated system privileges, the user application may need to request elevated rights to write to the shared configuration location.

EDR MODULE

THE INTERACTION WITH THE CORE SERVICE

The core service of the agent may include event management modules that require asynchronous user interactions for reporting service status, alerting, or making decisions. User applications are associated with these types of modules and provide the necessary user interface and integrations with platform shell APIs.

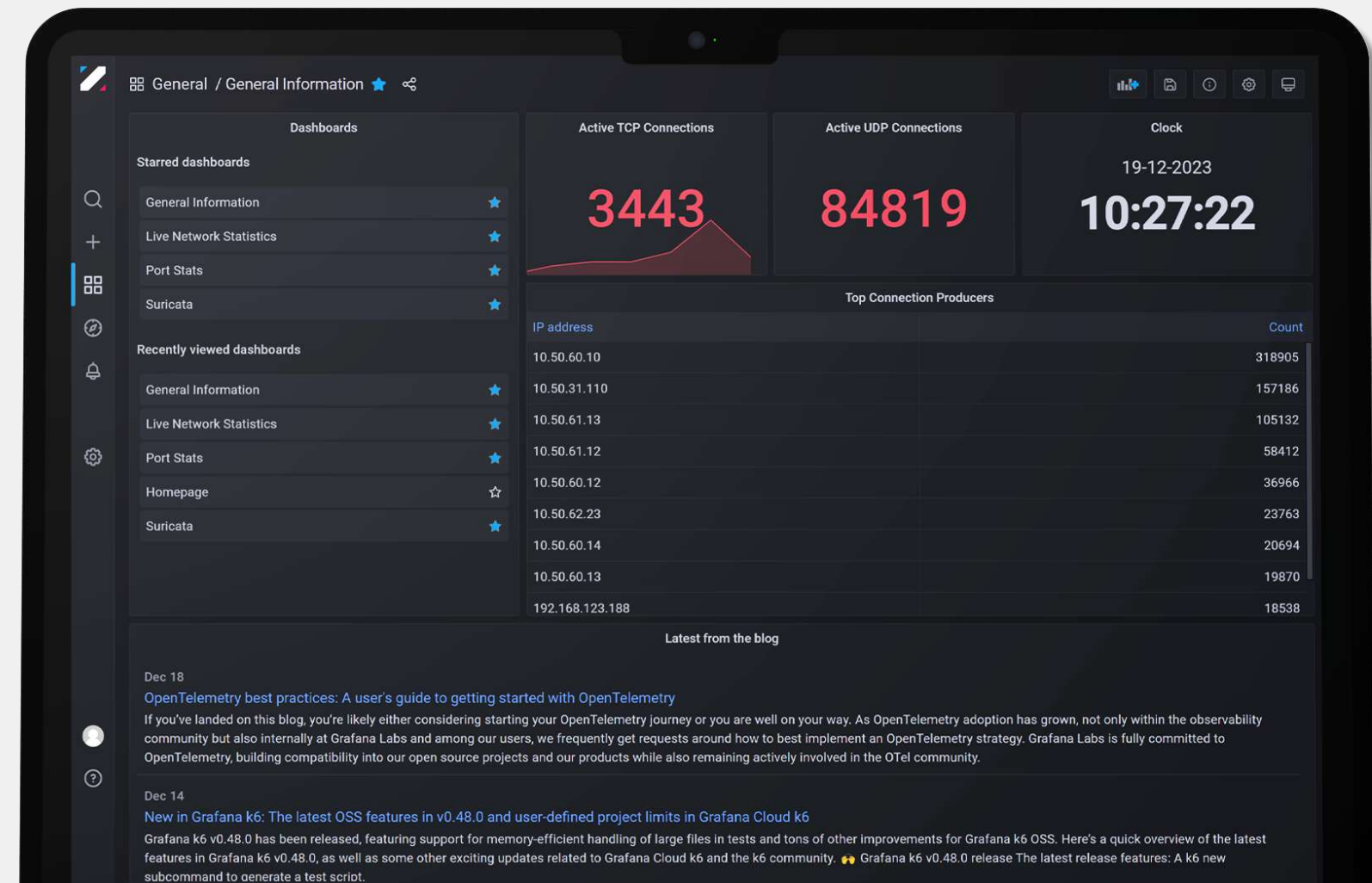
DISTRIBUTION MODEL

Each platform allows for various distribution models. It was necessary to choose some that efficiently provide both the basic agent service worker (with all its modules) and the user application.

The packaged implementation seems to be quite convenient for external requirements, as each operating system currently provides a way to bundle our two components into a single distributable item.

FUNCTIONALITIES AVAILABLE WITH PACKAGE DISTRIBUTION

Packaged applications can benefit from platform features such as automatic updates, easy uninstallation, and the delivery and licensing of optimized packages (which could be useful in the future if various modules are installed as additional plug-ins).





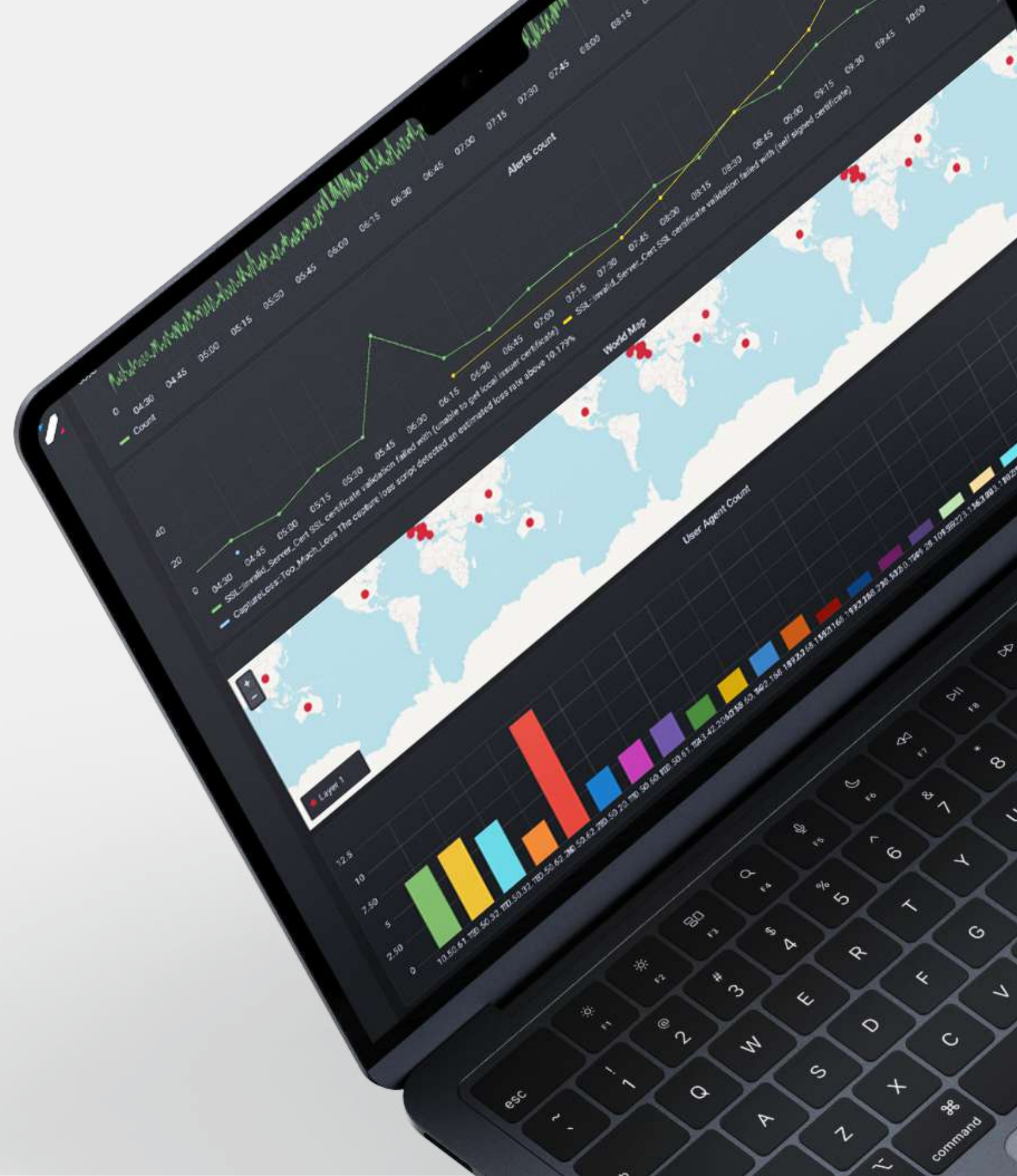
SOAR MODULE



SOAR Module

The SOAR functionality in ZADIG XDR is a cybersecurity tool designed to automate cyber attack prevention and incident response.

Our SOAR solution is an innovative security automation platform that combines human intelligence with Artificial Intelligence to ensure the highest level of protection. The solution integrates various playbooks that perform event triage from any SIEM, EDR, or another managed source. You can use a webhook to send alerts to the platform, and each alert is processed to identify and extract relevant indicators.



Case and Incident Management (CIM) Application

The CIM serves as a central point of interaction for a security team. You can use this application independently or in combination with a solution such as the SOC.

HOW IT WORKS

The Application of Case and Incident Management (CIM), as part of the SOC Solution, serves as the central point of interaction for the security team. The application provides the following practical capabilities:

- Unified triage of signals from alert triage, fraud triage, and manual playbook creation with automations for record creation;
- Interfaccia di arricchimento dell'Intelligence sulle minacce (TI);
- Various starting points for orchestration;
- Signal triage, case management, incident management, investigation details, Knowledge Base articles, remediation, correlation, and post-intervention activity reports;
- Dedicated spaces for customizations;
- Automatic collection of metrics;
- Advanced modes for troubleshooting and fine-tuning;

THE MAIN PAGE OF THE CIM

After logging in, follow these steps to access the CIM homepage.

1. Select your tenant.

If you have access to multiple tenants, make sure you are in the correct tenant. If you have access to only one tenant, the correct tenant will be automatically selected.

2. Choose the **SOC Solutions** workspace or the desired workspace.
3. In the left navigation pane, click on **APPLICATION RECORDS**.
4. Select **Case and Incident Management**.
5. Choose a CIM record from the list of CIM records in the default report.

You can view a record in the CIM application. You can immediately see the details of the record in the left panel, including signal type, threat intelligence verdict, signal source, etc. Additionally, there are expandable and collapsible sections that provide further information about the record.

Case and Incident Management (CIM) Application

ACTIONS FOR CREATING THE RECORD.

When a new record is created in the CIM application, two automation actions are performed to enrich the signal with observable verdicts and an automatic brief.

AUTOMATIC BRIEF

The event record in the CIM application is associated with an automatically generated summary.

ORCHESTRATION START POINTS

These represent natural points in the lifecycle of the record within the Case and Incident Management application where configurable automation/orchestration can ideally take place.

TYPE: SIGNAL

Records arrive in the application as Signals. Signals represent an incoming event from a Security Information and Event Management (SIEM) system or an Endpoint Detection and Response (EDR) system, a reported phishing email, or an ad-hoc indication of manually created suspicious activity. An incoming signal must have one of the following values as its source:

- Alert
- Email Phishing
- Manual

To claim the record, click on Claim.

- To claim the record and take further actions

Once claimed, you become the Current Owner, and the record's status is updated to "In Progress." After assessing the activity, you can escalate the record to a case if it's a true positive or if other thresholds are met (thresholds are determined by your organization's policies).

Case and Incident Management (CIM) Application

REQUEST THE ASSIGNMENT OF THE RECORD TO TAKE FURTHER ACTIONS

TYPE: CASE

The elevation to a case simply changes the value of the Type to "Case." It is important to emphasize again that this is a significant starting point for Orchestration.

While working on a case, it might be an excellent opportunity to identify additional signals or cases that may be related. Currently, the Correlation function in the SOC Solution is a simple reference field. Future versions of the SOC Solution will seek to expand Correlation capabilities.

TYPE : INCIDENT

Under certain circumstances, when working on a case, an operator may choose to Declare an Incident. Generally, this happens when a specified impact threshold is reached, requiring additional steps, reporting, communication to stakeholders, etc.

1. To declare an incident, click on Declare Incident.

This changes the Type value to Incident. Additionally, a red banner appears at the top of the record to emphasize the criticality of the record.

As the incident is mitigated, the incident can be de-escalated. De-escalating an incident is an indication that the incident has been mitigated, and response teams can suspend emergency operations.

1. To de-escalate an incident, click on De-Escalation of the Incident.

CUSTOMIZATION

The new CIM provides a dedicated space where you can add custom fields without affecting the look and feel of the main application space.

CUSTOM FIELDS

The application provides some example fields to demonstrate possible use cases for this section.

Case and Incident Management (CIM) Application

METRICS

The solution has the ability to capture hyper-granular metrics. During the lifecycle of a record, there are strategic points where a data point or timestamp is captured. The expected flow and data capture points are visible in this diagram:



GRANULAR METRIC FIELDS

In the record, you can view the metrics. Click on the Hyper-Granular Metrics tab. These metrics feed various dashboard reports, such as MTTD, MTTR, Dwell Time, etc.

ADVANCED MODE

The CIM application has an Advanced checkbox that, when selected, displays the managed functionality, widgets, and references of the application.

There are six additional expandable and compressible sections on a CIM record. The following documentation provides details on each section and how it interacts within the CIM record.

INVESTIGATIVE DETAILS

The "Investigative Details" section contains a fillable summary field for the current record, which would be included in an automatically generated After-Action Report (AAR) (see Post Incident Activity section). Additionally, this could be used for other use cases such as the Collaboration Solution. The Investigation Comments section displays comments not included in the AAR but are contained in the SOAR solution. The Attack Phases section provides a place to input or review the MITRE ATT&CK Technique/Tactic pairs used to populate the MITRE dashboard in the SOC Solution. You can also manually populate the Drag-and-Drop Evidence Locker section with various files related to the investigation.

Case and Incident Management (CIM) Application

KNOWLEDGE BASE ARTICLES

As the name suggests, the Knowledge Base section contains previously created remediation steps by the user for this record. Using this section, you can access lessons learned and other tips about that record or something that has related information (e.g., a similar signal type). Existing Knowledge Base Articles (KBA) include the tracking ID for the corresponding KBA, alarm title, context summary, guidance, and the last update date.

1. To add a new KBA to the current record, in the Knowledge Base Articles table, click the **plus** icon.
2. Click the **magnifying glass** icon to search for a KBA.
3. If necessary, click the **trash** can icon to delete a KBA from the record.
4. To ensure you have the latest and best set of KBA for that record after making changes to your investigation, such as MITRE ATT&CK mappings, click **Update Knowledge Base Links**.

THREAT INTELLIGENCE

INTELLIGENCE VERDICT

If observables are discovered in the incoming signal through an alarm or phishing email, those observables are automatically analyzed and enriched by the configured threat intelligence providers through the Threat Intelligence application (see the Threat Intelligence application for more details). Based on the results from the chosen Primary Intelligence Provider, the most critical verdict is passed to the Intelligence Verdict value. The criticality of the verdict is ordered from most critical to least critical:

- Malicious
- Suspicious
- Benign
- Unknown

The Threat Intelligence section displays the enrichment results from the Primary Intelligence Provider for each analyzed observable (widget) and allows the user to perform ad-hoc enrichment of the observable (Observable, Observable Type, Add Observable) during the investigation development. This is the simplest option for viewing the associated threat intelligence for a specific CIM record.

Case and Incident Management (CIM) Application

This section also allows exporting TI data. In the drop-down menus, select the desired Indicator Selector, Result Selector, Vendor Selector, and Filter Operator. Once you have the desired information, click Export to download the data in a .csv file. The .csv file provides the following TI details on the selected data:

- Tracking ID
- Indicator
- Permalink (A resource such as an observable enrichment on VirusTotal/Recorded Future)
- Tool (e.g., VirusTotal)
- Label (e.g., Malicious, Suspicious, etc.)
- Score
- Last Update

REMEDY

The Case and Incident Management (CIM) application has a Remedy section with various tabs, executing eight different playbooks for remediation actions on a CIM record. As an orchestrator, this provides a way to take various remediation actions based on the information in the CIM record.

BLOCK/UNBLOCK OBSERVABLES

As an orchestrator, you need to complete the configurations for the CIM - Block Observables playbook before updating the CIM record. The first action is a placeholder. If you want to replace this action with a remediation action or a nested playbook, configure the action for the task you want to perform against the observables that will be configured later in the CIM record.

1. From ORCHESTRATION, click on **Playbook**.
2. Search and open the **CIM - Block Observables playbook**.
3. In the placeholder of the first action, replace and configure the desired remedy.

Case and Incident Management (CIM) Application

This can be a nested playbook or an action you have already configured. For example, a playbook that invokes a firewall to block IP addresses or isolate hosts on EDR. The playbook receives the tracking ID for the current ticket and the values you are passing. Other playbook actions generate the output response and update the CIM record. Now, go to the desired record and scroll down to the Remedy section and the Block/Unblock Observables tab.

1. On this tab, enter the observables you want to block, then click **Block Observables**.

Once you click the button, it runs a playbook and returns the results in the Block Observables Response field with a response showing what the playbook did and what it acted on with a date/time.

To unblock an observable, follow the steps above for the CIM - Unblock Observables playbook and enter the observables you want to unblock, then click Unblock Observables. Again, the response is displayed with a date/time.

Important! While orchestrators need to create nested playbooks and/or actions within the CIM - Block Observables and CIM - Unblock Observables playbooks, operators can edit the content of the Remedy tab in the CIM record. Modifying the observables of the CIM record does not require orchestrator-level access. The same applies to all playbooks run in the Remedy tab.

DISABLE/ENABLE USERS

This tab functions similarly to the Block/Unblock Observables tab. Orchestrators must first access the CIM - Disable Users or CIM - Enable Users playbooks to replace the placeholder action with a configured nested playbook or action that achieves the desired outcome.

1. Navigate to the desired CIM record and go to the **Remediation section**.
2. On the Disable/Enable Users tab, enter the users you want to disable and/or enable.
3. Click on **Disable Users and/or Enable Users**.

This runs the appropriate playbook and returns the results in the Disable Users Response and/or Enable Users Response fields, providing a response showing what the playbooks did and what they acted upon with the date/time.

Case and Incident Management (CIM) Application

ISOLATE/UNISOLATE HOST

This tab also works like the Block/Unblock Observables tab. Orchestrators must first access the CIM – Isolate Host or CIM – Reunite Host playbooks to replace the placeholder action with a configured nested playbook or action that achieves the desired outcome.

1. Navigate to the desired CIM record and the **Remediation section**.
2. On the Isolate/Reunite Host tab, enter the hosts you want to isolate or reunite.

This is common with EDR use cases.

1. Click on **Isolate Hosts and/or Unite Hosts**.

This runs the appropriate playbook and returns the results in the Isolate Hosts and/or Unite Hosts Response fields with a response showing what the playbooks did and what they acted on with date/time.

ALERT MANAGERS

This section works like the Block/Unblock Observables tab. Orchestrators must first access the CIM – Alert Managers playbook to replace the placeholder action with a configured playbook or nested action that performs the desired outcome.

1. Navigate to the desired CIM record and **Remediation section**.
2. In the Notify Managers tab, enter the email address of the manager to notify them of a security event.
3. Click on **Notify Managers**.

This executes the appropriate playbook and returns the results in the Alerted Managers Response field with a response showing what the playbook did and what it acted upon with date/time.

Case and Incident Management (CIM) Application

SIEM SEARCH

This tab functions similarly to the Block/Unblock Observables tab. Orchestrators must first access the CIM - Query SIEM playbook to replace the placeholder action with a configured playbook or nested action that performs the desired outcome.

1. Navigate to the desired CIM record and go to the **Remediation section**.
2. In the SIEM tab, enter the SIEM query data.

A good use case is to investigate an IP address (observable) to see if it appears elsewhere in your environment. Enter the observable in the SIEM query field and click the button to run the playbook and obtain the results.

1. Click on **Query SIEM**

This runs the appropriate playbook and returns the results in the SIEM Query Response field, showing what your SIEM has returned and a table that can display SIEM events in standardized JSON format. The table also allows the option to filter based on columns or values.

CORRELATION

Our SOAR solution can correlate records, allowing you to compare a new record with a previous record that has correlation keys. In the Case and Incident Management (CIM) application, correlation information is present in the CIM record in a designated section and on the Support tab.

A correlation action occurs whenever a record is created. From the Support tab on a CIM record, the Correlation Support Field section accommodates 13 key correlation fields (observables) from the Process Alerts or Process Emails playbooks. After correlation takes place, the SOAR executes a playbook that extracts the tracking IDs for the correlated records.

In the sample record, CIM-241 displays the Correlation section with related tracking IDs in CIM-244, CIM-243, CIM-245, and CIM-242 records. The title, status, intelligence verdict, manual verdict, and brief automated information for each record are displayed in the table of the Correlations.

1. To view a specific record in detail, click on the corresponding tracking ID.

Case and Incident Management (CIM) Application

The selected record opens in a popup window. Click outside the window to return to your current record.

The informations are not only displayed in this section, but there is also a widget under the AUTOMATED BRIEF section called Records. The Records section provides a more visual representation of the current and related records with record details highlighting important data and the option to export the data of that record to a .csv file.

POST INCIDENT ACTIVITY

In a Case and Incident Management (CIM) record, this section has a 'Generate Post-Incident Report' button.

When you click this button, the SOAR collects data points from your record, passes them to a script that generates an HTML report, and then converts that report into an easily understandable PDF file as a Post-Incident Actions Report (AAR).

1. From the Post-Incident Actions section, click on Generate Post-Incident Report.
2. Click on the Download icon to download the PDF or click directly on the file name to preview the file.

The PDF opens after downloading or previewing. The file has a user-friendly layout that includes the following information for that record:

- Case Number
- Automatic Brief
- Investigation Summary
- Remediation Actions Taken
- Timeline Summary
- Incident Handler Information

If you have a local copy of an AAR and want to add it to the record, simply drag the file into the After Action Report section.

Tip: If an orchestrator wants to adjust the information returned in the AAR PDF file, you can navigate and open the CIM - Generate After Action Report playbook, click on the Generate HTML Report action, and click Configure. From the Script panel, using HTML, you can modify the returned data.

Case and Incident Management (CIM) Application

THREAT INTELLIGENCE APPLICATION

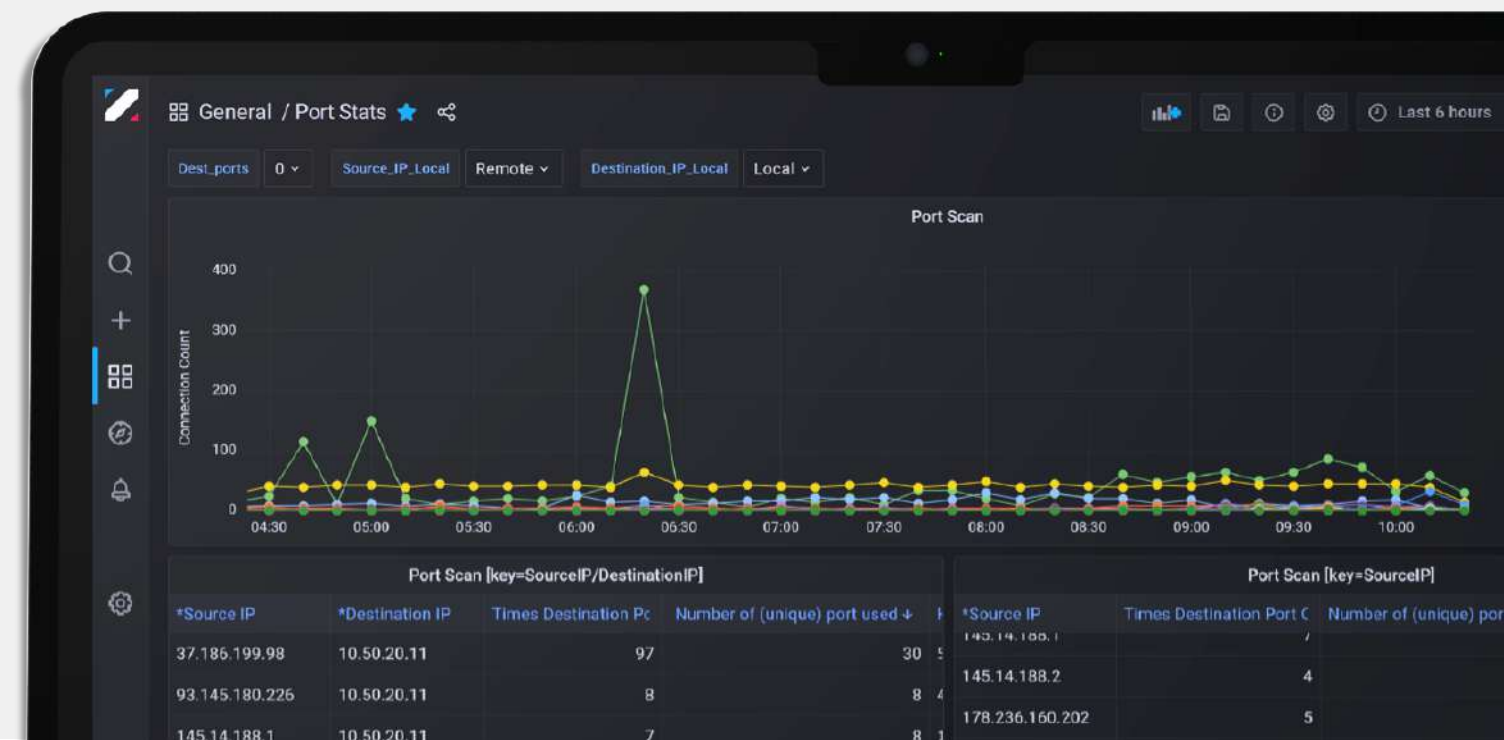
The Threat Intelligence (TI) application enriches observables from CIM. All unique observables from an incoming signal in the CIM application generate a new TI record.

PRIMARY INTELLIGENCE PROVIDER

Based on the observable type value, the appropriate Primary Intelligence Provider (PIP) is selected. The resulting enrichment is at the top of the application. The PIP enrichment values determine the Intelligence Verdict, as mentioned in the Case and Incident Management application.

OTHER PROVIDERS

Once again, based on the observable type value, other intelligence providers enrich the observable. The results from these providers, while not contributing to the Primary TI Verdict, are visible directly in the TI Record in a dedicated expandable widget. Key enrichment details are displayed with the ability to click on the widget card to expand and view the raw JSON.



Script

Tip: For Boolean and Null data types, we recommend importing JSON and using `json.loads()` to make sure the data is loaded correctly. Since all playbook data is in JSON format and Python does not natively support all JSON data types.

Use the Script's native controlled action and write in Python to:

- manipulate data and boundary cases.
- Reduce complexity by using JSONata.
- Use the most common programming language safely today to perform simple tasks.

When configuring input, consider using the Python Chatbot, which uses ChatGPT's Open AI to help you formulate transformations and custom Python code.

NATIVE SCRIPT ACTION CONFIGURATION

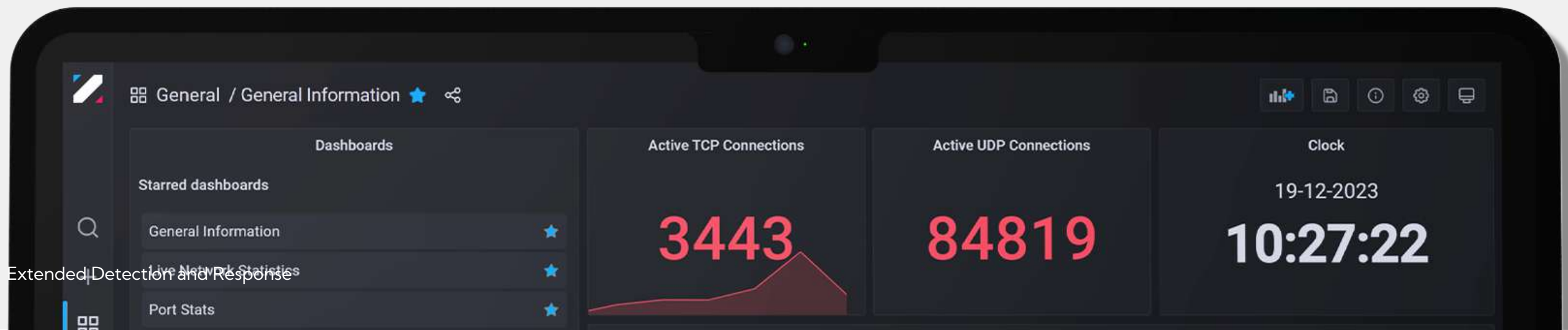
Now it is time to begin the basic configuration for the native Script action.

You have already created a playbook and are ready to manipulate data from a property.

1. From your playbook, click on **Add an action**.
2. From the ACTION panel, click on the **Action** drop-down menu.
3. Select **Scripts** and click on **Configure**

The Script window opens.

The Script window has three tabs: Script, Outputs, and Test. The Script tab has the Input pane (on the left side) and the Script pane (on the right side).



Script

SCRIPT INPUT

With the native Script action, you can build and map static data inputs and playbook properties to reference data in the Python Script.

The playbook properties you can add are:

- String
- Boolean Number
- Object
- Array

Before you can test, configure your Script inputs. Let's look at a quick example on how to configure inputs and use the Script pane.

1. From the Scripts tab, in the Input pane, click on Add property to define inputs, including any sub-inputs.
2. Click on the pencil icon to change the name of the property.
3. Write your code in the Script panel

SCRIPT TESTING

Want to test your Script before continuing to build the playbook? In the Script action, from the Test tab, you can now see the Inputs on the left and the Script on the right.

The Result pane at the bottom shows the results of the test. The results vary, so in addition to the base of property types, and depending on the inputs selected, the outputs of the action may return additional properties. These are the discovered outputs, which you can promote and/or delete from the Outputs tab.

Script

ATTACHED SCRIPT

If you need to return an attachment or use it as input in the native Script action, follow the instructions below:

ATTACHED IN OUTPUT

In your playbook, follow the instructions below to set up an attached in output:

c. From the **Action** drop-down menu, select **Script**.

Call this action **Return attachment** and click on **Configure**. There are two ways to write Python code to return an attachment. Let's see both of them!

1. On the Script tab, enter the following code:

```
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
```

You can get the size of the attachment using the `.size()` method, and you can get the MIME type of the attachment using the `.mimetype()`. You can get the name of the attachment using the `.file_name` property. Everything is shown in the code above.

pythonCopy code

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

1. Click **Apply** to save the changes.

INPUT ATTACHMENT

You can use an input attachment in a Python script using a native Script action.

1. From the **Action** drop-down menu, select **Script**

Call this action **Input Attachment** and click on **Configure**.

1. Click on **Add properties** and select **Attachment**.

Click on the pencil icon to change the name. For example, you can change the name to **file1**.

1. Click on **Select a property** and select **Playbook Properties**.

Script

The playbook properties drawer opens and based on the example, you would select the object for **first_file**. Then go back to Inputs and repeat steps 4 and 5, but add the object for **second_file**.

1. In the Scripts tab, enter the following code:

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()
```

You can get the size of the attachment using the **.size()** method, and you can get the MIME type of the attachment using the **.mimetype()**. Both are shown in the code above.

You can also write the code as follows:

pythonCopy code

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

2. Click **Apply** to save the changes.

Now both files are mapped.



ENABLE TWO-FACTOR AUTHENTICATION (2FA)

Two-Factor Authentication, or 2FA, adds an extra layer of security to user accounts. Each time users log in, they will need a password and a verification code.

It is possible to enforce dual-factor authentication throughout the organization. Users will then be required to configure 2FA and will not be able to disable the setting.

If you choose not to globally enforce 2FA, individual users will be able to enable the configuration of 2FA.

GLOBALLY ENABLE TWO-FACTOR AUTHENTICATION

To globally enable two-factor authentication:

1. From the administration area, click > to expand Settings, then select **Accounts**.
2. Select the Sessions and Security tab and expand **AUTHENTICATION**.
3. Activate **Impose organization-wide** to enable 2FA for everyone accessing the solution from your organization.

FURTHER ACTIONS OF ADMINISTRATORS FOR 2FA

Administrators can reset the 2FA configuration for users as needed. To reset the individually configured 2FA account for a user, log in and open the User page. Open the user's profile page and select the Authentication tab.

Click on Reset.

The user will be prompted to set up a new instance of 2FA once they attempt to log in again.

Administrators can also exempt specific users from using 2FA. To do this, log in to the specific user and activate the **Exempt** switch in the authentication user profile window.

Security and Compliance of SOAR Solution

Our SOAR enables secure access and management of content. Technical and physical controls within the SOAR solution prevent disclosure of content and unauthorized access to it. The infrastructure is continuously monitored, and security personnel internal and external conducts regular vulnerability testing.

Our SOAR platform extensively uses automation and security response to report suspicious activity in all customer environments. Internally, confidentiality requirements are communicated to employees through training and policies. Employees are required to attend security awareness training, which includes information, policies, and procedures related to protecting our customers' data.

SAFETY

Our solution provides several security features to ensure the confidentiality, integrity and availability of customer information.

REST DATA

Here is how our SOAR solution protects your data at rest:

- All client data and application snapshots are encrypted with the AES256 algorithm before being stored on disk.
- Allows complete snapshots of the instance that support disaster recovery and restoration of the application state known as "good."
- Entries in the credential library, as well as user and asset passwords, are encrypted at rest before being stored in the solution database, using the AES encryption algorithm with a 256-bit key and a 256-bit salt.

DATA IN MOTION

All client data and application snapshots are encrypted with the AES256 algorithm before being stored on disk.

Allows complete snapshots of the instance that support disaster recovery and restoration of the application state known as "good."

Entries in the credential library, as well as user and asset passwords, are encrypted at rest before being stored in the solution database, using the AES encryption algorithm.

Security and Compliance of SOAR Solution

SAML/SSO

We support the provision of local user accounts, Open LDAP, Microsoft Active Directory and SAML 2.0.

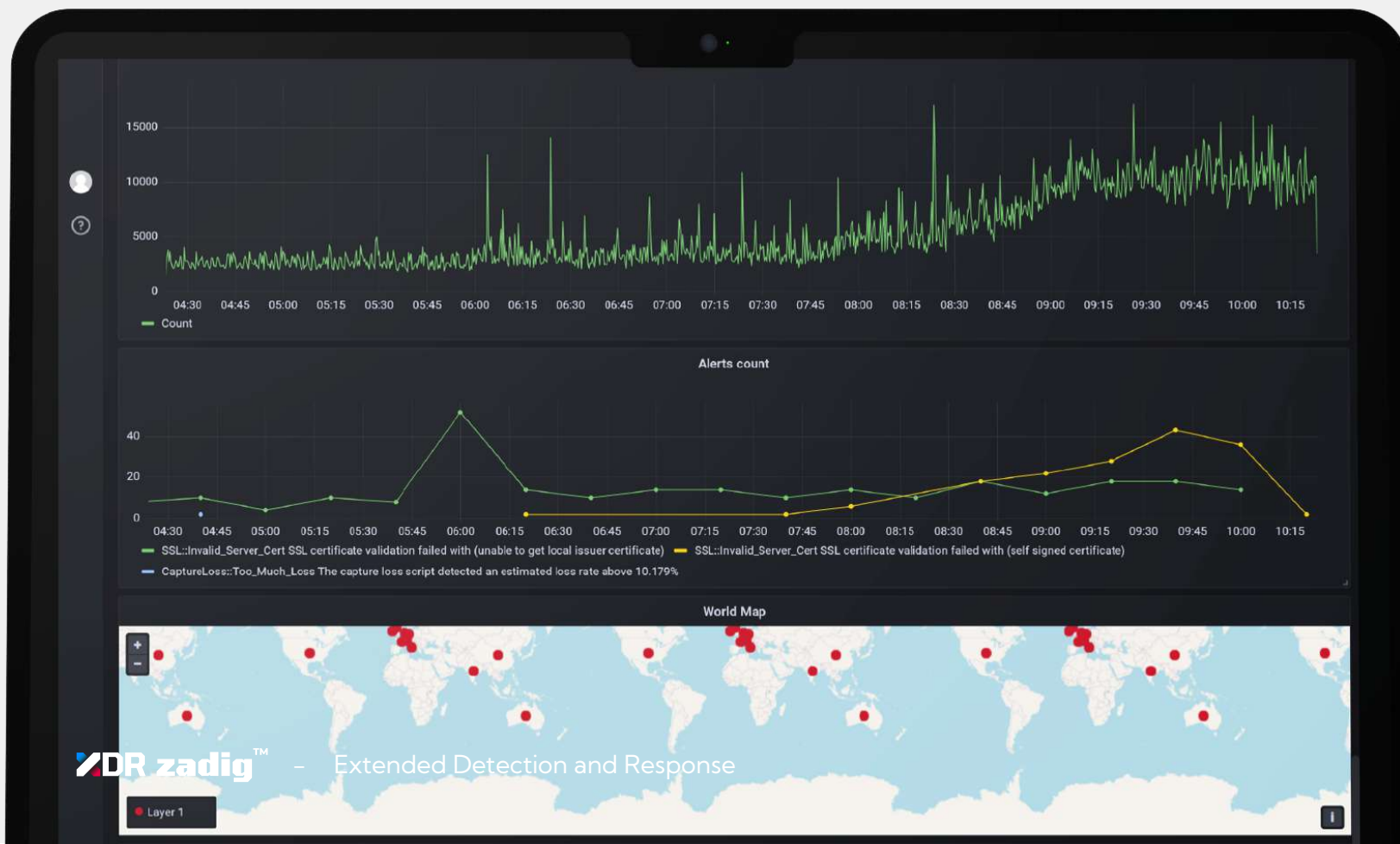
TWO-FACTOR AUTHENTICATION

We support the provision of local user accounts, Open LDAP, Microsoft Active Directory and SAML 2.0.

ROLE-BASED ACCESS CONTROL

The SOAR solution restricts access to information using Role-Based Access Control (RBAC). You can apply RBAC to any level of objects: workspaces, dashboards, reports, applications, records, and individual records. Granular controls down to the individual field level are supported, and all components support the ability to restrict access by user, group, or role. SOAR can dynamically adjust authorizations on the basis of per-record based on user/group field values. For example, if a record is assigned to Group A, only Group A and administrators will have access to that record. If the record assignment changes to Group B, then only Group B and administrators will have access to the records.

Administrators also have the option of separating the account administrator from the orchestrator and playbook designer.



Workspaces and Dashboards

Users manage the SOAR solution by working with records on workspaces, dashboards and cards.

WORKSPACES

Workspaces are customizable areas within the platform where you can organize and access the tools and features you use regularly. Workspaces can include applications, dashboards, records, reports and charts. Administrators can change the default workspace and dashboards for users. All users can switch to different workspaces and dashboards based on the permissions they set.

DASHBOARD

Dashboards are a visual representation of records, reports, and charts associated with applications in the workspace. A workspace can have multiple dashboards, and users can view different dashboards by selecting the DASHBOARD or WORKSPACE navigation icon and choosing another dashboard from the list. Users have access only to workspaces, dashboards, records, and reports if they have been authorized by an administrator. If an existing dashboard or report is not visible, an administrator should verify that the user has been assigned the correct permissions.

CARD

A card is a report or HTML object associated with a dashboard. You can have multiple cards on a single dashboard. Cards are fully customizable and can be resized and reordered on the dashboard by administrators or users with appropriate access. Users can click within a card to view a list of records associated with that chart or report, or click on a data point within a chart to view a filtered list of records corresponding to that data. Several different types of charts are available to display information about records in a meaningful way, making dashboards, cards, and charts powerful tools for finding records quickly and displaying data.


TRANSPORT ENCRYPTED PROTOCOL (TEP)

bitCorp has five patents including the Transport Encrypted Protocol (TEP), an innovative high-security modular data transmission protocol in which blockchain is applied to telecommunications for the first time.

Protected by EU and US patents, it is able to cover the entire OSI stack and integrate transparently into virtually any datalink and offers, without the need for further integrations, full guarantees of confidentiality, integrity and message delivery.

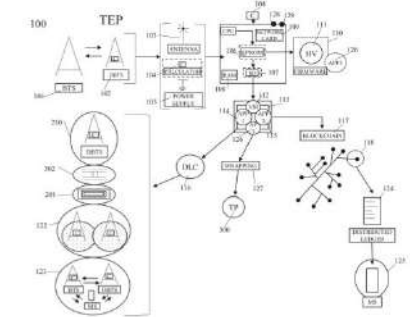
Designed for military purposes, TEP allows the creation of secure mesh networks even in contexts with a low level of trust, without any type of centralization and in general without single points-of-failure.

Finally, its very high reorganization speed and its enormous fault tolerance make it particularly suitable for real-time applications, such as the management of smart grids or use with Autonomous Car (AC). Furthermore, thanks to the use of blockchain, it is invulnerable to DDoS, Man-in-the-Middle and Spoofing attacks.



US011799659B2

<p>(12) United States Patent Pegoraro</p> <p>(54) METHOD, ARCHITECTURE AND DEVICES FOR THE REALIZATION OF AN ENCRYPTED COMMUNICATION PROTOCOL OF ENCRYPTED DATA PACKETS NAMED 'TRANSPORT ENCRYPTED PROTOCOL' (TEP)</p> <p>(71) Applicants: Gabriele Edmondo Pegoraro, Luino (IT); Christian Fabio Persurich, Milan (IT); Gianluca Tirozzi, Florence (IT)</p> <p>(72) Inventor: Gabriele Edmondo Pegoraro, Luino (IT)</p> <p>(73) Assignees: Gabriele Edmondo Pegoraro, Luino (IT); Christian Fabio Persurich, Milan (IT); Gianluca Tirozzi, Florence (IT)</p> <p>(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 253 days.</p> <p>(21) Appl. No.: 17/059,348</p> <p>(22) PCT Filed: May 24, 2019</p> <p>(86) PCT No.: PCT/IB2019/054343 § 371 (c)(1), (2) Date: Nov. 27, 2020</p> <p>(87) PCT Pub. No.: WO2019/229612 PCT Pub. Date: Dec. 5, 2019</p> <p>(65) Prior Publication Data US 2021/0243031 A1 Aug. 5, 2021</p> <p>(30) Foreign Application Priority Data May 28, 2018 (IT) 10201800005763</p> <p>(51) Int. Cl. H04L 9/08 (2006.01) H04L 9/32 (2006.01) (Continued)</p>	<p>(10) Patent No.: US 11,799,659 B2</p> <p>(45) Date of Patent: Oct. 24, 2023</p> <p>(52) U.S. CL. CPC H04L 9/3239 (2013.01); H04L 9/0825 (2013.01); H04L 63/166 (2013.01); (Continued)</p> <p>(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)</p> <p>(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)</p> <p>FOREIGN PATENT DOCUMENTS WO 2017/182844 A1 10/2017</p> <p>OTHER PUBLICATIONS IBM, Type 1 vs. Type 2 hypervisors https://www.ibm.com/topics/hypervisors (Year: 2018).*</p> <p>(Continued)</p> <p><i>Primary Examiner</i> — Carl G Colin <i>Assistant Examiner</i> — Andrew Suh (74) <i>Attorney, Agent, or Firm</i> — Maier & Maier, PLLC</p> <p>(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</p> <p>(Continued)</p>
--	--



Products



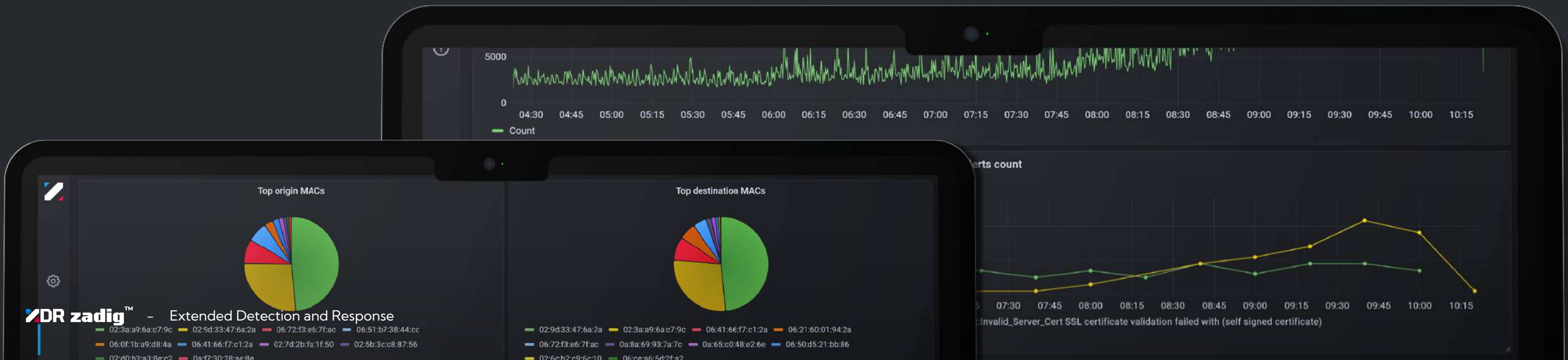
Hybrid Intrusion Detection Prevention System conceived for monitoring large IT infrastructures.



Plug & Play cybersecurity platform intended for SMEs, particularly for those companies which have poor or null cybersecurity competences.



Plug & Play cybersecurity software intended for SMEs and free lance professionals.





bitCorpTM

Legal HQ: Via Monte Bianco 2/A, 20149, Milano

Representative HQ: Galleria del Corso 4, 20121, Milano

Labs: Via Carlo Freguglia 10, 20122, Milano

www.bitcorp.it