zadig™ XDR

bitCorp™

Zadig™ XDR

The integrated cybersecurity solution for medium and large companies.

ZADIG is an all-in-one solution consisting of three modules:

- **IDS-IPS system enriched with proprietary and customizable Artificial Intelligence models**
- **cross-platform centralized end point protection (HIDS)**
- **integration of data typically related to SIEM systems**

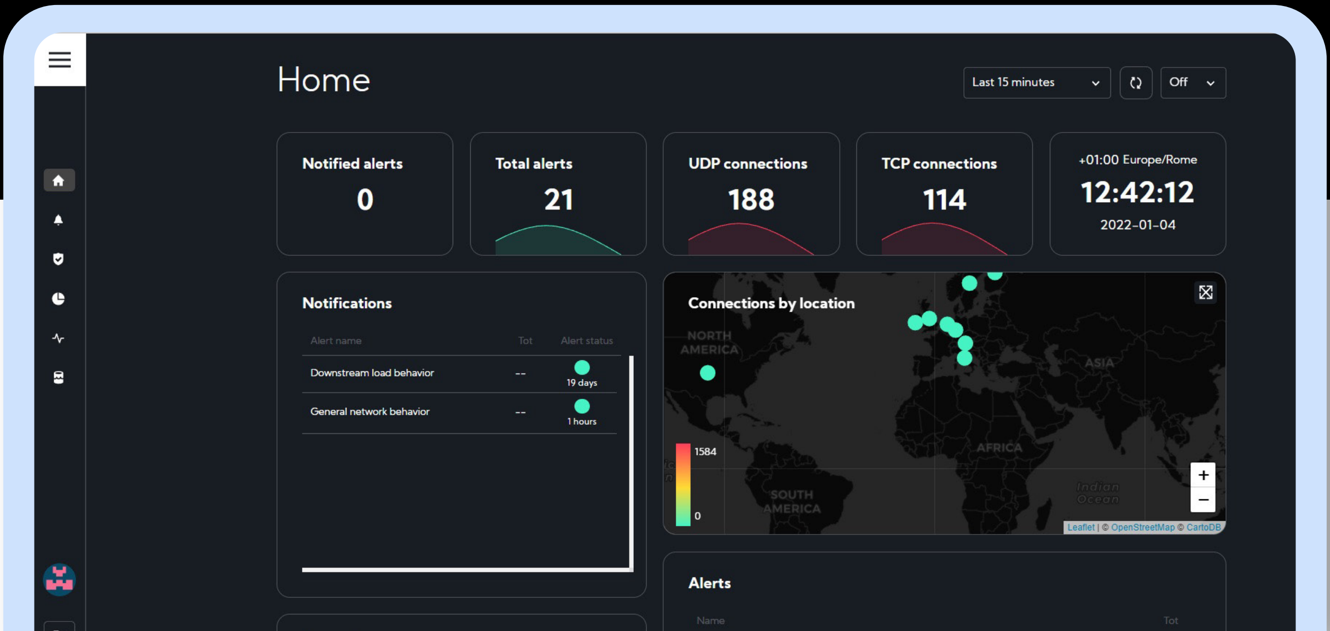
The versatility of ZADIG allows you to purchase the solution in its entirety or just for individual module, integrating each component with any safety systems already in use.

IDS - IPS

ZADIG's IDS-IPS is an integrated system that monitor the network by sending alerts for suspicious activities (IDS) while acting promtly to block the packet's traffic based on their content (IPS).

Monitoring takes place on both sides, the signature and the behavioral basis. Thanks to this last function – developed through artificial learning models – **ZADIG not only identifies and neutralizes known threats, but is also able to understand if there is an attack in progress by interpreting anomalies in the regular behavior of the monitored infrastructure.** This functionality is useful because it adapts to the changing conditions in which it operates, such as the increase in the size or characteristics of the customer's infrastructure.

Zadig, in addition to making use of a powerful system of pattern that matches the signatures (i.e. a byte-by-byte recognition of known fingerprints), also allows, thanks to a specific Turing-complete scripting language with specific events, to manipulate network packets to adapt in the most effective way to any matching discrepancies that may exist on the customer's infrastructure, thus creating an ad-hoc protection solution at the highest levels of efficiency and effectiveness.



Home

Last 15 minutes: Off

Notified alerts	Total alerts	UDP connections	TCP connections	+01:00 Europe/Rome
0	21	188	114	12:42:12 2022-01-04

Notifications

Alert name	Tot	Alert status
Downstream load behavior	--	● 19 days
General network behavior	--	● 1 hours

Connections by location

Alerts

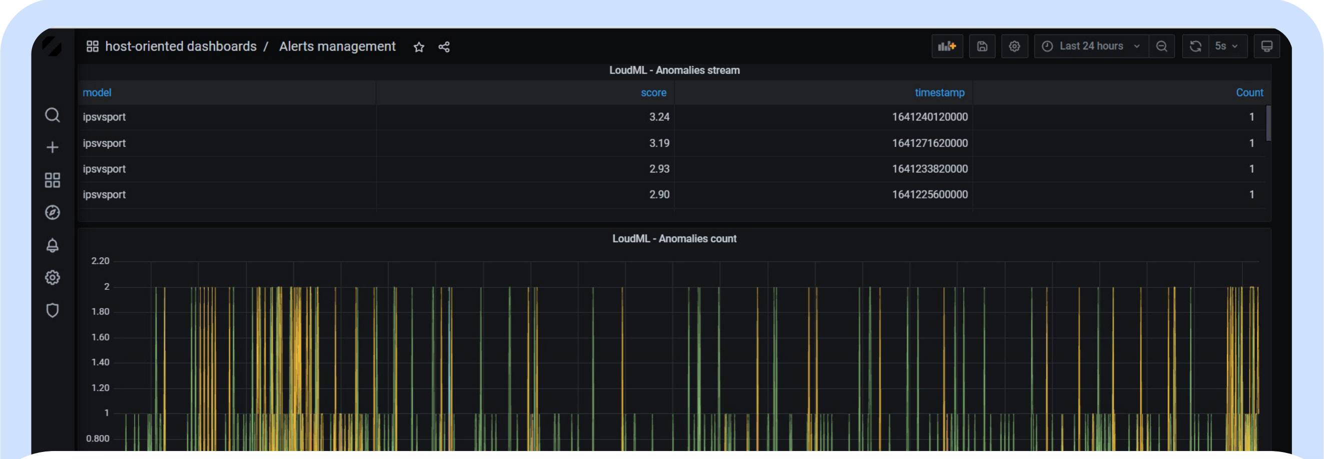
Name	Tot

This aspect is of particular importance in the case, for example, of obsolete software environments, therefore no longer upgradable or adaptable with specific integration layers which, due to the deployment specifications adopted by the customer, may present vulnerabilities not solvable by the original suppliers.

On top of the AI models included in ZADIG, we offer customized mathematical solutions adapted to any specific type of network, production process or usage that carachterize the specific work enviroment of the client.

This is made possible thanks to the observation and monitoring of the network and the ways in which it is used. Therefore, both automated models and rules, will be adatped and implemented according to the type of use observed.

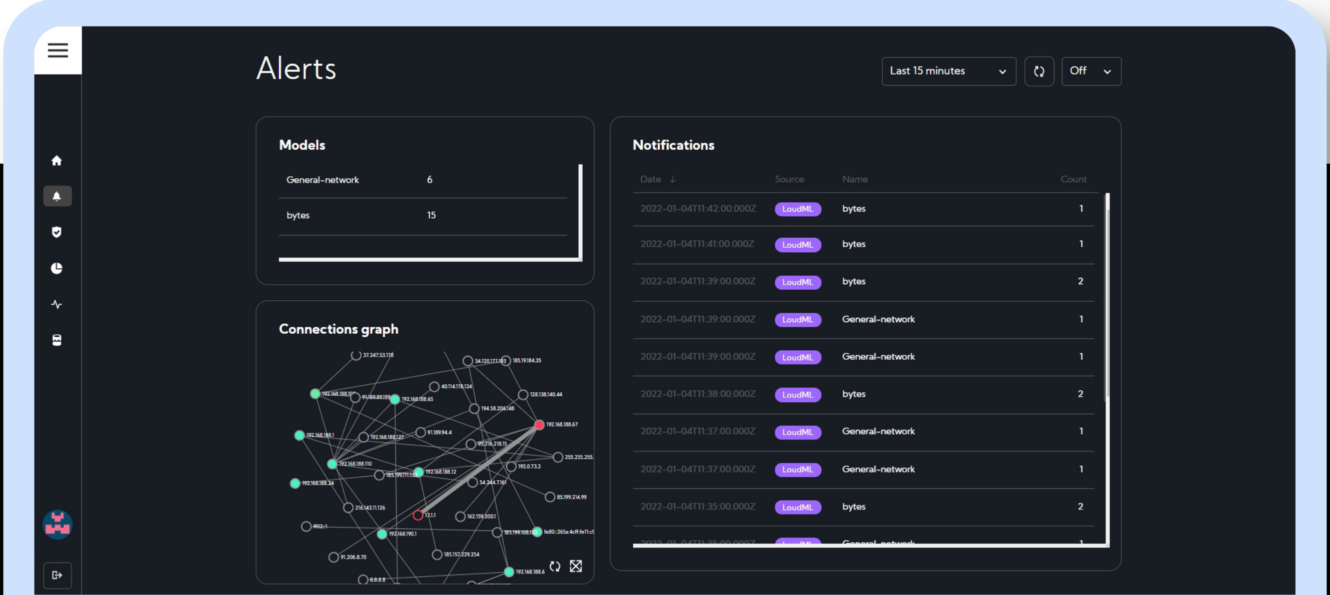
ZADIG's IDS-IPS is also powered by a set of feeds maintained and distributed by open source communities as a further guarantee of constant updating against the most recent attack's techniques exploited by attackers.



LoudML - Anomalies stream

model	score	timestamp	Count
ipsvsport	3.24	1641240120000	1
ipsvsport	3.19	1641271620000	1
ipsvsport	2.93	1641233820000	1
ipsvsport	2.90	1641225600000	1

LoudML - Anomalies count



Alerts

Models

General-network	6
bytes	15

Connections graph

Notifications

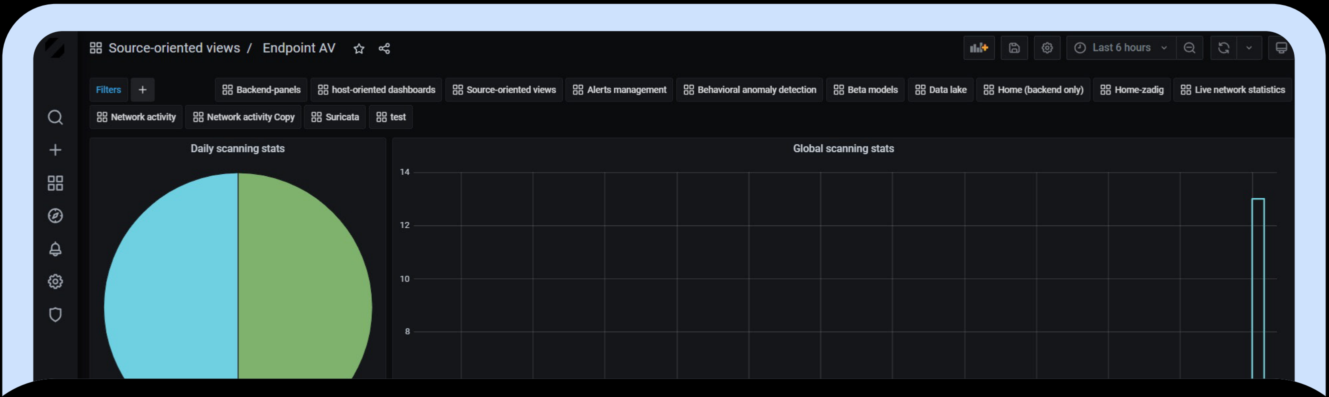
Date ↓	Source	Name	Count
2022-01-04T11:42:00.000Z	LoudML	bytes	1
2022-01-04T11:41:00.000Z	LoudML	bytes	1
2022-01-04T11:39:00.000Z	LoudML	bytes	2
2022-01-04T11:39:00.000Z	LoudML	General-network	1
2022-01-04T11:39:00.000Z	LoudML	General-network	1
2022-01-04T11:38:00.000Z	LoudML	bytes	2
2022-01-04T11:37:00.000Z	LoudML	General-network	1
2022-01-04T11:37:00.000Z	LoudML	General-network	1
2022-01-04T11:35:00.000Z	LoudML	bytes	2
2022-01-04T11:35:00.000Z	LoudML	General-network	1

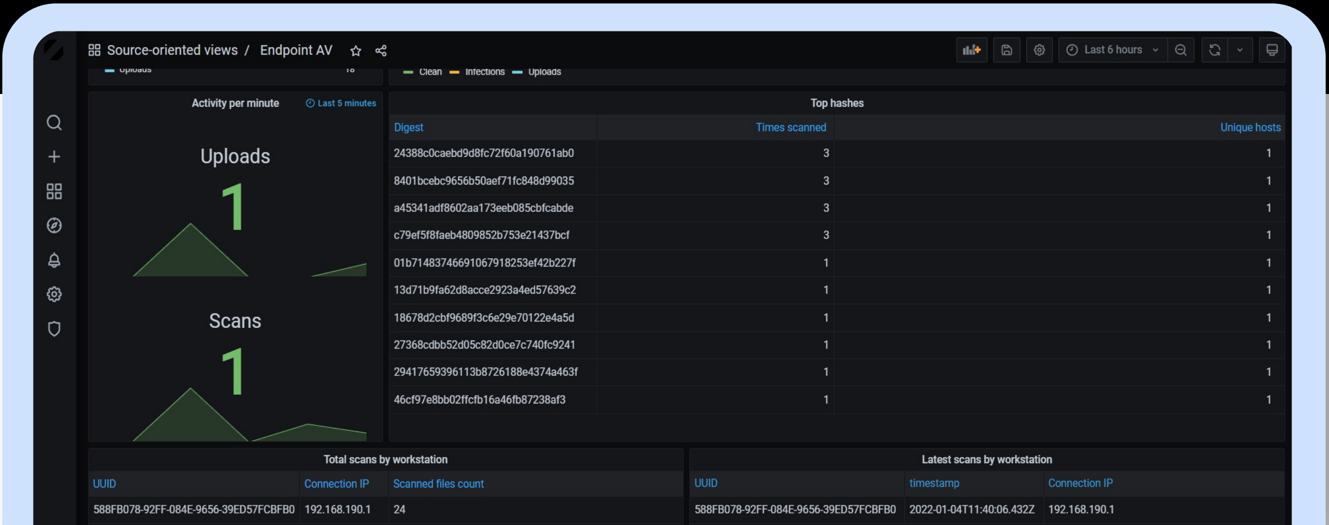
End Point management and protection

ZADIG also offers HIPS (Host-based Intrusion Prevention System) functions.

This means that it is able to extend its protective shield to each endpoint present in the monitored network (PC, server, NAS, etc.) thanks to his continuous scanning and monitoring of filesystems, processes and much more with a centralized API that aggregates the data collected and provides artificial intelligence functions to identify and intervene on anomalous behaviors of suspicious nature.

In this way, ZADIG effectively replaces the typical features of a professional antivirus product: the IDS identifies a threat on the endpoint and the IPS intervenes by neutralizing any attempt to spread across the network, for example by isolating the infected machine.





Top hashes

Digest	Times scanned	Unique hosts
24388c0caebd9d8fc72f60a190761ab0	3	1
8401bcebc9656b50aef71fc848d99035	3	1
a45341adf8602aa173eeb085cbfcabde	3	1
c79ef5f8faeb4809852b753e21437bcf	3	1
01b71483746691067918253ef42b227f	1	1
13d71b9fa62d8acce2923a4ed57639c2	1	1
18678d2cbf9689f3c6e29e70122e4a5d	1	1
27368cdbb52d05c82d0ce7c740fc9241	1	1
29417659396113b8726188e4374a463f	1	1
46cf97e8bb02ffcfb16a46fb87238af3	1	1

Total scans by workstation

UUID	Connection IP	Scanned files count
588FB078-92FF-084E-9656-39ED57FCBFB0	192.168.190.1	24

Latest scans by workstation

UUID	timestamp	Connection IP
588FB078-92FF-084E-9656-39ED57FCBFB0	2022-01-04T11:40:06.432Z	192.168.190.1

Anti Ransomware

Italy is second among the European countries hit by cyber attacks among them nearly about 900 a week are ransomware-type attacks.

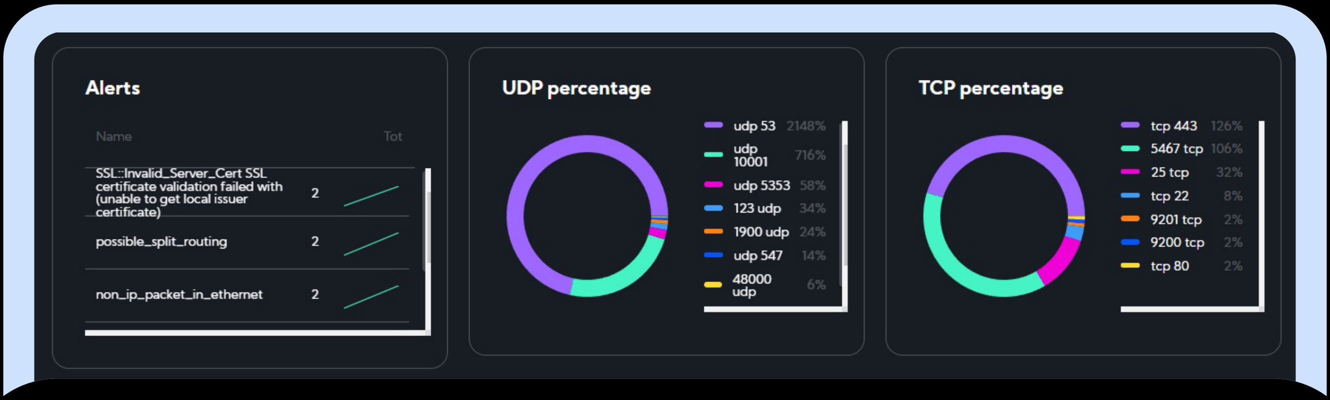
ZADIG allows you to protect the infrastructure of your company effectively thanks to a system capable of intervening in a preventive manner in the event of specific conditions that unequivocally indicate the presence of preparatory acts for the attack.

In these cases, ZADIG automatically isolates the compromised device and allows the activation of a series of recovery measures capable of restoring the latest version of the files before the attempted attack.

Integration con IoT

The versatility of ZADIG allows you to extend your monitoring and analysis capabilities to any system equipped with sensors, such as IoT technology.

ZADIG is in fact able to analyze any type of input data: it is therefore sufficient to imagine, instead of a PC, any system based on telemetry or sensors to have an effective monitoring of any system based on IoT, such as smart building, smart wasting, etc.



Alerts

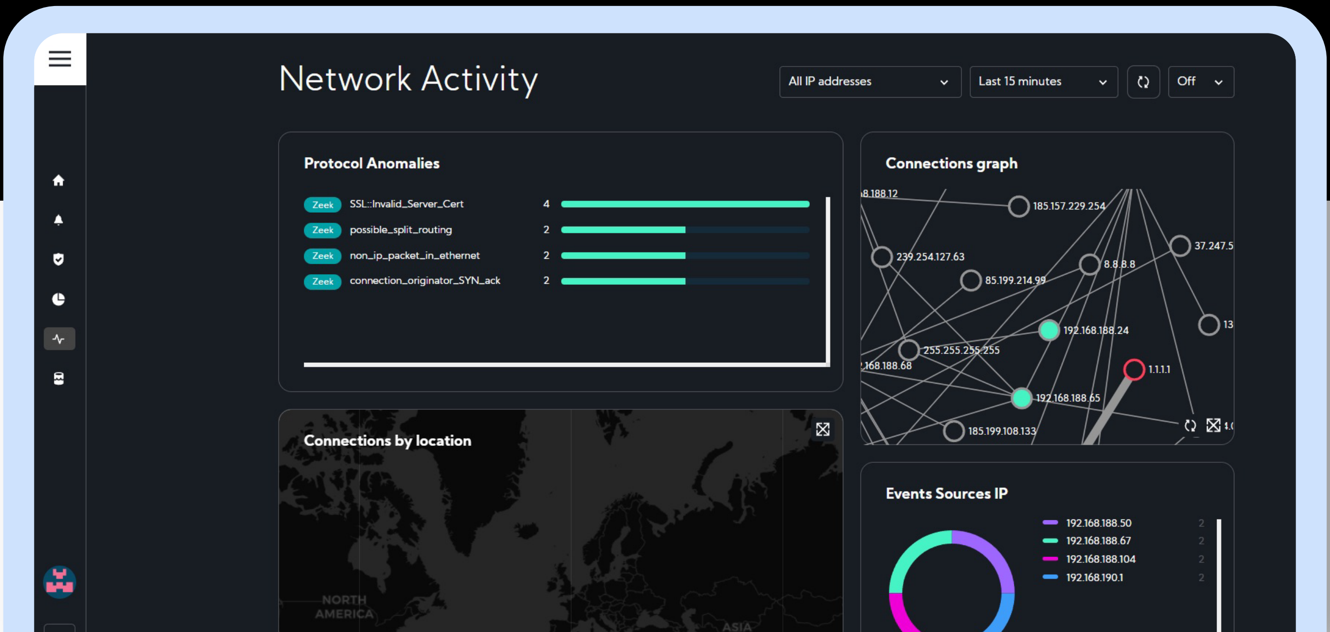
Name	Tot
SSL::Invalid_Server_Cert SSL certificate validation failed with (unable to get local issuer certificate)	2
possible_split_routing	2
non_ip_packet_in_ethernet	2

UDP percentage

udp 53	2148%
udp 10001	716%
udp 5353	58%
123 udp	34%
1900 udp	24%
udp 547	14%
48000 udp	6%

TCP percentage

tcp 443	126%
5467 tcp	106%
25 tcp	32%
tcp 22	8%
9201 tcp	2%
9200 tcp	2%
tcp 80	2%



Network Activity

All IP addresses | Last 15 minutes | Off

Protocol Anomalies

Zeek	SSL::Invalid_Server_Cert	4
Zeek	possible_split_routing	2
Zeek	non_ip_packet_in_ethernet	2
Zeek	connection_originator_SYN_ack	2

Connections graph

Connections by location

Events Sources IP

192.168.188.50	2
192.168.188.67	2
192.168.188.104	2
192.168.190.1	2

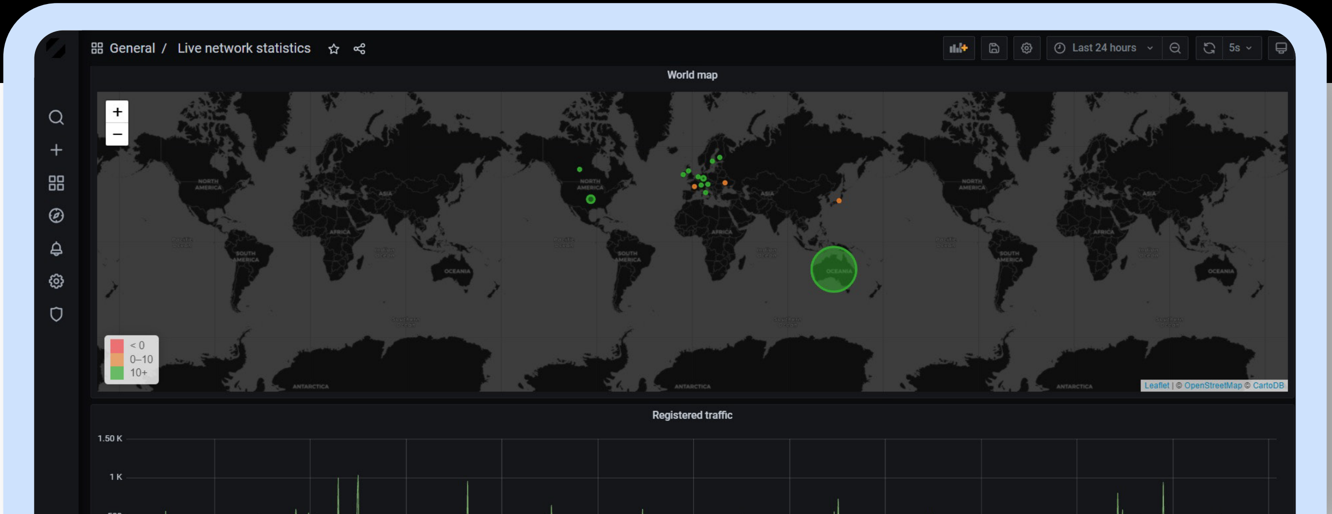
Log Aggregation and Analytics

The log data collected by ZADIG flow into a management and analysis system which, thanks to a very advanced hardware equipped with NIC up to 10Gbit / sec of traffic (equivalent to approximately the information in transit for 625 compressed and transmitted 4K HDR video streams simultaneously from the most well-known platforms) coming from a mirror port of one or more switches, makes correlations between the various data sources in search of relevant events.

Furthermore, thanks to its great scalability, it is possible to coordinate the flow of data from different subnets to the same site while maintaining a single information aggregator.

The ZADIG Log Aggregation and Analytics system allows you to analyze data from different types of sources and is equipped with a control dashboard that allows the user to interact quickly and intuitively with all the information that ZADIG functions produces, including the incident management events, threat intelligence feeds, telemetry, error reporting, etc.

The log retention policies can also be customized according to the needs and storage availability of the individual customer.



Remediation

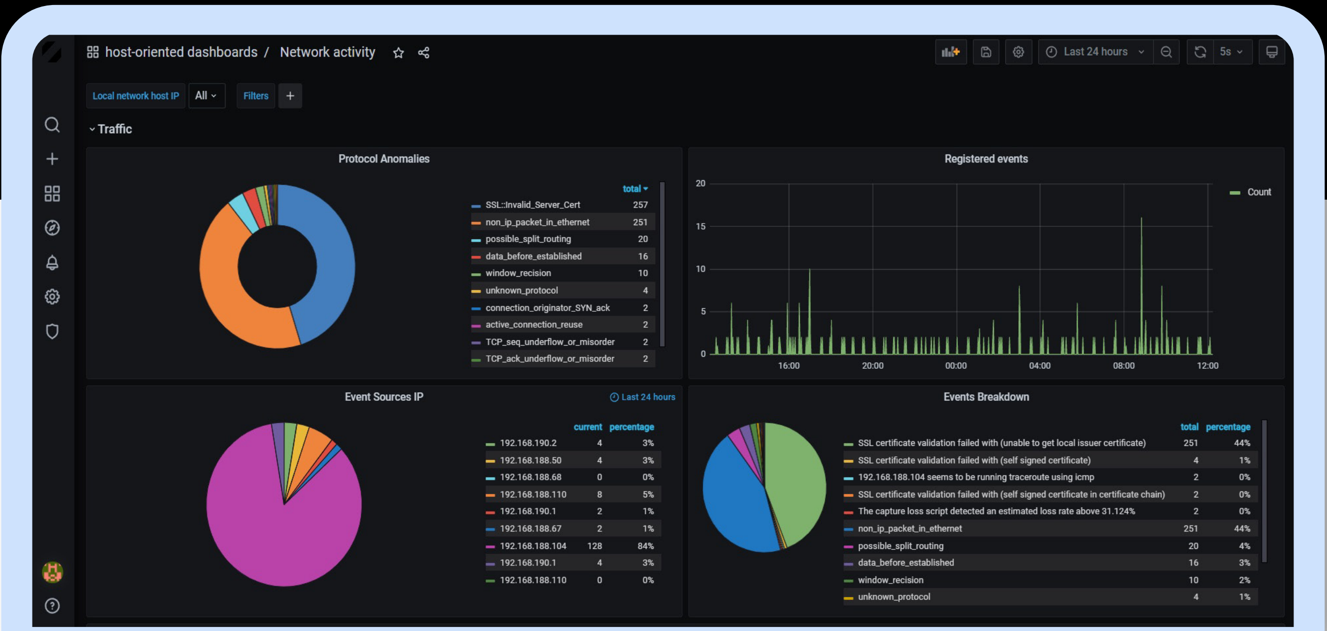
The reason for the costant activity of ZADIG's IPS is to neutralize all threats.

Remediation can be automated (for example by isolating the suspected infected machine followed by the recovery of it's data) or customized according to the needs of the individual user.

The alerts are shared to the various systems through a wide range of communication channels chosen by the customer based on possible integration, including e-mails, instant messaging platforms or other M2M-type platforms such as webhooks.

After any hostile activities, bitCorp analysts can be hired to carry out a series of activities, such as:

- **generation of customized protection rules**
- **data and log integrity check**
- **reporting and recovery of quarantined systems**



Protocol Anomalies

	total
SSL::Invalid_Server_Cert	257
non_ip_packet_in_ethernet	251
possible_split_routing	20
data_before_established	16
window_recision	10
unknown_protocol	4
connection_originator_SYN_ack	2
active_connection_reuse	2
TCP_seq_underflow_or_misorder	2
TCP_ack_underflow_or_misorder	2

Event Sources IP

	current	percentage
192.168.190.2	4	3%
192.168.188.50	4	3%
192.168.188.68	0	0%
192.168.188.110	8	5%
192.168.190.1	2	1%
192.168.188.67	2	1%
192.168.188.104	128	84%
192.168.190.1	4	3%
192.168.188.110	0	0%

Events Breakdown

	total	percentage
SSL certificate validation failed with (unable to get local issuer certificate)	251	44%
SSL certificate validation failed with (self signed certificate)	4	1%
192.168.188.104 seems to be running traceroute using icmp	2	0%
SSL certificate validation failed with (self signed certificate in certificate chain)	2	0%
The capture loss script detected an estimated loss rate above 31.124%	2	0%
non_ip_packet_in_ethernet	251	44%
possible_split_routing	20	4%
data_before_established	16	3%
window_recision	10	2%
unknown_protocol	4	1%

Real innovation

ZADIG is the result of real and constant research carried out by bitCorp. A research that starts from the updated knowledge of the methodologies of cyber attacks, even the most sophisticated and recent.

Integrated ransomware prevention

ZADIG allows you to prevent and protect yourself against the most frequent computer threat, the "Ransomware", thanks to a proprietary system capable of identifying the preparatory acts with which this type of attack is carried out.

The integration of the alerts produced by ZADIG with back-up and recovery systems allows the implementation of automated recovery processes of any data type storage to the state working prior to the attempted attack .

A.I. modeling in-house

Each model of artificial intelligence employed by ZADIG is made directly by bitCorp. Depending on your needs, we create customized templates and scripts to respond effectively to every peculiarity of the asset to be protected.

Personalized Remediation

ZADIG does not propose a standard remediation model, but operates according to the criteria and processes established by the client.

Stop false alarms

In addition to employing standard methodologies to limit false positives, such as Splunk's playbooks, bitCorp has proprietary hierarchical-clustering and PAM-clustering algorithms that help automatically reduce false positive alarms.

In addition, operators can also modify the alert thresholds, if necessary, to customize the profiles based on the specifications, characteristics and nature of the network.

Integration with IoT systems

The ability of ZADIG to analyze any type of data allows it to exploit its monitoring potential by integrating sources from any infrastructure equipped with sensors and telemetry.

A suitable use for smart building projects, smart wasting, smart lighting, etc.

Customizable Dashboard

The data consultation dashboard available at the ZADIG Log Aggregation and Analytics can be modified according to the customer's needs and the type of query that is required.

About us

Microsoft Partner
Microsoft

IBM PartnerWorld

vmware PARTNER
TECHNOLOGY ALLIANCE

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

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

Team

Christian Persurich, PhD
Co-founder

Gianluca Tirozzi, PhD
Co-founder

Dr.ssa Greta Scarpa
Chief Executive Officer

Ing. Andrea Brancaleoni
Chief Commercial Officer

Ing. Gabriele Pegoraro
Chief Innovation Officer

Ing. Luca Piccirillo
Software & Network
Security Engineer

Marco Ferrarini, PhD
Big Data Analyst

Dott. Luis Ibanez
Software & Network
Security Engineer

Paola Trovisi
Responsabile Amministrativa

Gabriele Piazzolla
Linux/UNIX
System Expert

Ing. Nancy Laurenda
Software & TELCO Engineer

Ing. Aurelio Loris Canino
Software & TELCO Engineer

Dr.ssa Marilù Pagano
Copywriter e
Social Media Manager

Bitcorp was born as an advanced security solution for government and private companies.

It is a creative intelligence laboratory capable of interpreting individual needs and providing the most appropriate solutions of both offensive and defensive nature, working prevalently in- but not limited to- the IT and Telco industries.

9001
ISO
CERTIFIED

Information Security Management System
ISO
27001
Certified

CERTIFIED
ISO
45001:2018
COMPANY

ENVIRONMENTAL MANAGEMENT SYSTEM
ISO 14001

bitCorp™

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

Sede di Milano
Galleria del Corso 4, 20121 – Milano

Sede di Roma
via Ludovisi 16, 00187 – Roma

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

www.bitcorp.it