EXEIN

IoMT Cybersecurity for Tomorrow's Healthcare

Exein S.p.A

Rome
Piazzale Flaminio 19,
00196, Italy

San Francisco
535 Mission St 14th floor,
94105, CA

Karlsruhe
10 Ludwig-Erhard-Allee
76131, Germany

WHITEPAPER | Q4 2023

Table of Contents

1. The Baseline

IoMT stands for the Internet of Medical Things. It refers to the interconnected network of medical devices and applications that communicate with each other and healthcare information technology systems through the internet.

IoMT devices include a wide range of medical equipment, wearables, sensors, and other technologies designed to collect and exchange healthcare data for monitoring, diagnosis, and treatment purposes. However, the widespread adoption of these technologies has brought about unprecedented security challenges, making the healthcare sector one of the most vulnerable industries to cyber threats.

This white paper examines the developing cyber threats in the healthcare industry, with a focus on the vulnerabilities of IoMT devices.

2. IoMT

IoMT integrates various medical devices and applications with healthcare IT systems through online networks, enabling machine-to-machine communication via Wi-Fi-equipped devices.

Through interconnected devices, IoMT promotes a data-driven, patient-centered approach to medicine, significantly impacting key areas of healthcare such as:

1 Remote Patient Monitoring

IoMT allows healthcare professionals to remotely collect and monitor patient health data, reducing the need for in-person visits. This enhances accessibility to healthcare and contributes to the early detection of potential health issues.

2 Heart-rate Monitoring

IoMT devices deliver consistent heart rate monitoring, significantly boosting patient mobility and convenience. This uninterrupted monitoring empowers individuals to carry on with their daily activities, while also providing crucial health insights promptly and reliably.

3 Glucose Monitoring

IoMT devices revolutionize glucose monitoring by providing continuous, automated tracking. This doesn't just streamline the process, it guarantees instant access to real-time data on patients' glucose levels.

4 Parkinson's Disease Monitoring

IoMT sensors continuously collect data on Parkinson's symptoms, helping patients lead more independent lives and providing critical information for effective treatment.

5 Connected Inhalers

IoMT-connected inhalers monitor and manage conditions like asthma, reminding patients to carry their inhalers and tracking attack frequencies.

6 Ingestible Sensors

These sensors gather data from within the human body in a non-invasive manner, providing assistance in specific diagnosing conditions.

7 Robotic Surgery

The Internet of Medical Things (IoMT) has opened up new possibilities in the field of healthcare, with robots playing a crucial role. These IoMT-connected robots are designed to assist surgeons in carrying out complex procedures, significantly improving patient outcomes. They have the potential to revolutionize surgical procedures by providing greater precision and reducing the risk of complications.

3. Security Challenges and Trends

Predictions indicate that the global Internet of Medical Things (IoMT) market could increase to $187.60 billion by 2028, a significant jump from $41.17 billion in 2020.

However, this growth brings security concerns. Each healthcare device connected to the network potentially opens a new pathway for cyber threats. IT and security experts in healthcare are aware and are trying to reduce this risk.

A report by the Ponemon Institute confirms this. It identifies the top three cybersecurity worries:

64%

Unsecure Medical Device

64% of respondents in the survey acknowledged this as a problem.

60%

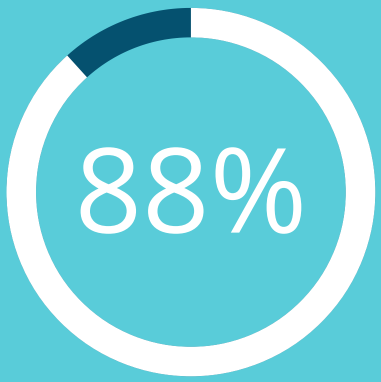
Ransomware

60% of respondents in the survey acknowledging this as a problem

59%

Mobile Apps

59% of respondents in a survey acknowledging this as a problem



Of Cyberattacks involve IoMT

In recent times, there has been a notable surge in cyber attacks targeting healthcare systems, thereby amplifying the risks associated with the exposure of patients and hospital information, as well as potential service disruptions.

This escalation in security threats can be largely attributed to the substantial proliferation of Internet of Medical Things devices.

88% of cyberattacks on healthcare systems involve IoMT and 12% are rooted in IoT according to the Ponemon Institute. This could be anything from pacemakers to glucose monitoring.

These devices often lack updates, making the risk of an infection more prominent. A recent FBI study found that there are an average of 6 vulnerabilities per medical device.

Although recalls were issued for critical devices like pacemakers, more than 40% of medical devices have reached end of life and offer little to no security patches or upgrades.

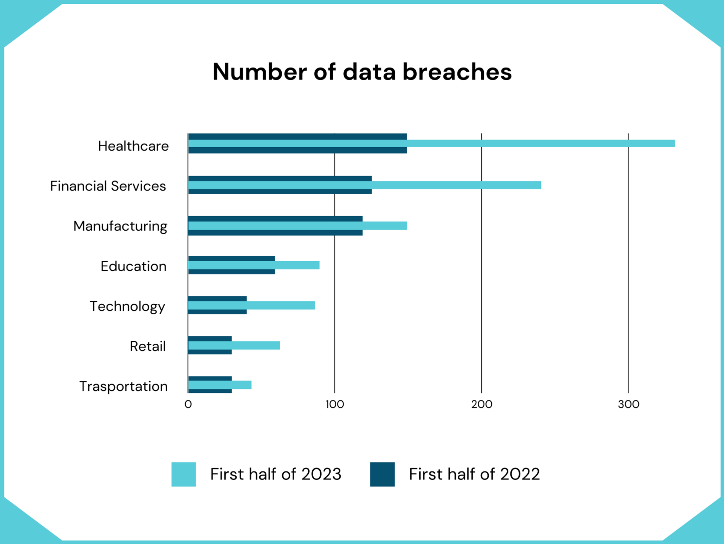
6

Vulnerabilities per medical device

4. The Cost of Insecure IoMT

The average cost of a data breach is $4 million, but in healthcare, it soars to an average of $10 million.

Healthcare organizations had 379 compromises in the first half of 2023, compared to 161 in the prior year's first half.



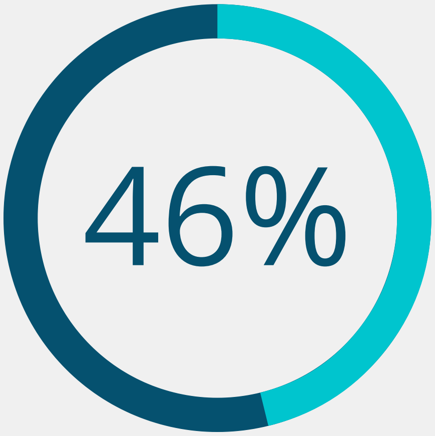
This implies that a healthcare data breach is not just one of the most expensive incidents, but also one of the most common these days. Cyber incidents disrupt healthcare in various ways, including:

1 Increased Data Loss

Healthcare institutions risk significant patient data loss, leading to worse outcomes and delayed care and legal issues.

2 Increased Death Rates

Cyber incidents can lead to rise in mortality rates. Hospitals affected by attacks face higher death rates, damaging their reputation and trust.



companies faced reputational damage after a cyber incident

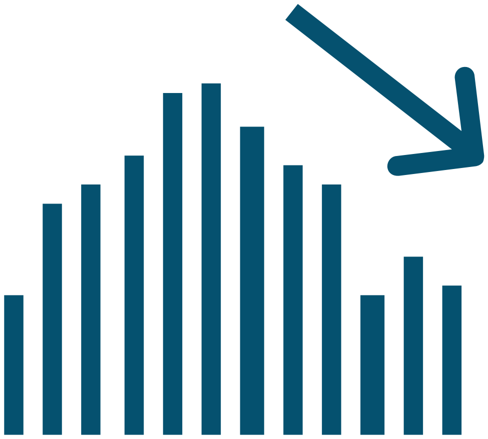
3 Reputational

Cybersecurity breaches can harm reputation and trust. According to ENISA, 46% of companies faced reputational damage after a cyber incident.

For healthcare institutions, this could mean regulatory fines and fewer patients scheduling non-emergency care.

4 Recovery Costs

The estimated recovery cost for healthcare institutions after a cyberattack averages $10 million per incident, which is higher than in any other industry. The Ponemon Institute reports that these costs include lost staff time (25%), regular operations disruptions (23%), IT asset damage or theft (21%), remediation and technical support (16%), and time spent rectifying patient care (15%).



5. The Omnibus Spending Bill

The 2023 Omnibus Spending Bill, a key funding bill for U.S. government operations, includes an important section focused on improving the security of medical devices. This aspect is particularly vital for healthcare cybersecurity, considering the potential involvement of Protected Health Information in IoMT devices.

Building on the previous PATCH Act, the bill gives FDA the authority to enforce mandatory cybersecurity rules specifically designed for IoMT devices in the healthcare field.

Manufacturers seeking FDA pre-market approval must now ensure ongoing device security throughout its life cycle, involving timely software updates and vulnerability monitoring.

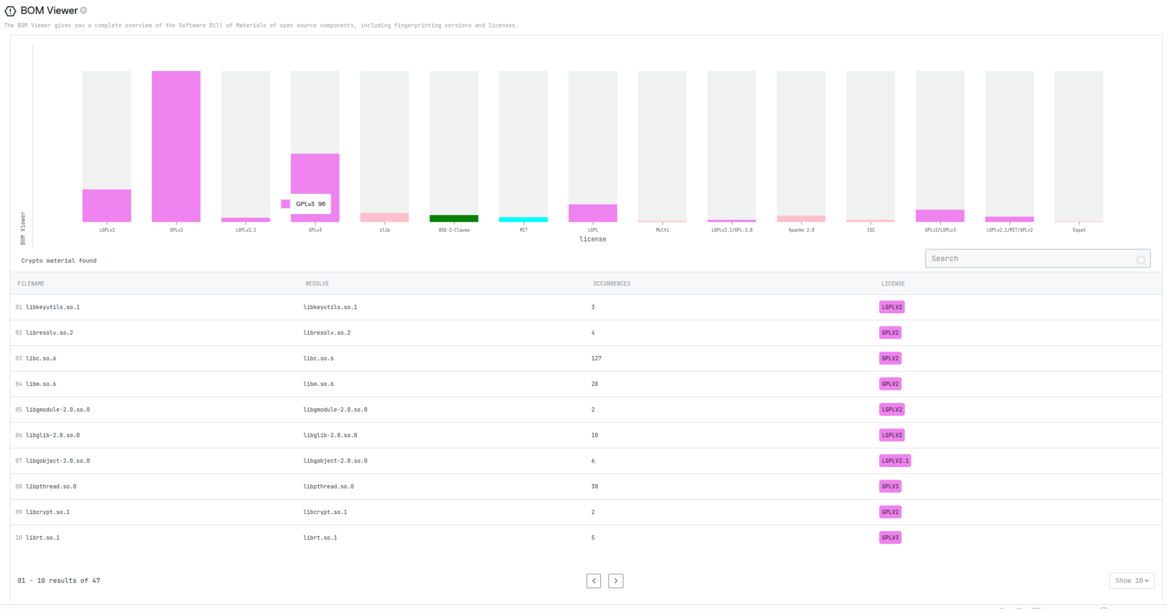
A crucial step is the submission of a Software Bill of Materials (SBOM), detailing all components—open-source and proprietary—helping manufacturers to address potential vulnerabilities.

Post-market, manufacturers are obligated to track and address new vulnerabilities, including coordinated disclosure and prompt resolution of any identified exploits, ensuring the functionality and security of IoMT devices.

Regarding the pre-market obligations, our solution, Exein Analyzer, plays a crucial role in assessing the SBOM by meticulously distinguishing between open source and proprietary software components. This aids manufacturers in identifying potential vulnerabilities. In response to post-market requirements mandated by the Omnibus Spending Bill, which necessitates manufacturers to monitor new vulnerabilities, Exein Analyzer provides continuous firmware analysis and vulnerability detection throughout the device life cycle. Our solution generates detailed reports, streamlining the resolution process.

To address post-market vulnerabilities and ensure the functionality and security of a device, Exein Runtime is an ideal solution. It seamlessly integrates into pre-existing IoT management systems, offering advanced runtime protection for devices in a matter of days rather than months.

Together, Exein Analyzer and Exein Runtime provide a comprehensive approach, encompassing proactive monitoring and reactive measures, ultimately safeguarding the security and integrity of connected devices.



BOM Viewer

The BOM Viewer gives you a complete overview of the Software Bill of Materials of open source components, including fingerprinting versions and licenses.

Crypto material found

FILENAME	RESOLVE	OCCURRENCES	LICENSE
01 libkeyutils.so.1	libkeyutils.so.1	3	LGPLV2
02 libresolv.so.2	libresolv.so.2	4	GPLV2
03 libc.so.6	libc.so.6	127	GPLV2
04 libm.so.6	libm.so.6	28	GPLV2
05 libgmodule-2.0.so.0	libgmodule-2.0.so.0	2	LGPLV2
06 libglib-2.0.so.0	libglib-2.0.so.0	10	LGPLV2
07 libgobject-2.0.so.0	libgobject-2.0.so.0	6	LGPLV2.1
08 libpthread.so.0	libpthread.so.0	38	GPLV3
09 libcrypt.so.1	libcrypt.so.1	2	GPLV2
10 librt.so.1	librt.so.1	5	GPLV3

01 - 10 results of 47

6. IoMT Incidents

2017

Hacking risk leads to recall of 500,000 pacemakers

The FDA recalled around 500,000 Abbott pacemakers due to cybersecurity concerns, underlining the serious risks in IoMT devices. Hackers could change heartbeats or deplete batteries.

2019

Medtronic issues 'urgent' recall of insulin pump controller vulnerable to hacks

In August 2018, Medtronic recalled insulin pumps, advising warranty-covered users to disable the remote bolus feature. The 2019 recall expanded to all insulin pump with a remote controller due to identified risks of unauthorized signal copying.

2023

Ransomware Attack (Various Years)

Since the global WannaCry ransomware spread in 2017, causing service disruptions and medical device shutdowns, a worrying trend emerged. A recent Ponemon Institute survey revealed a quarter of healthcare organizations saw increased mortality rates after ransomware attacks.

There are many more incidents that are publicly reported.
By way of example, this brief listing quickly illustrates the gravity of such events. Similar scenarios have been occurring for years with a wide range of impacts. Experts say that it is not a matter of "if" but "when" a successful cyber attack will cause widespread damage.

7. Exein Runtime on Healthcare Applications

In a hospital's intricate digital ecosystem, various components seamlessly interconnect to optimize patient care while presenting a complex network susceptible to cyber threats.

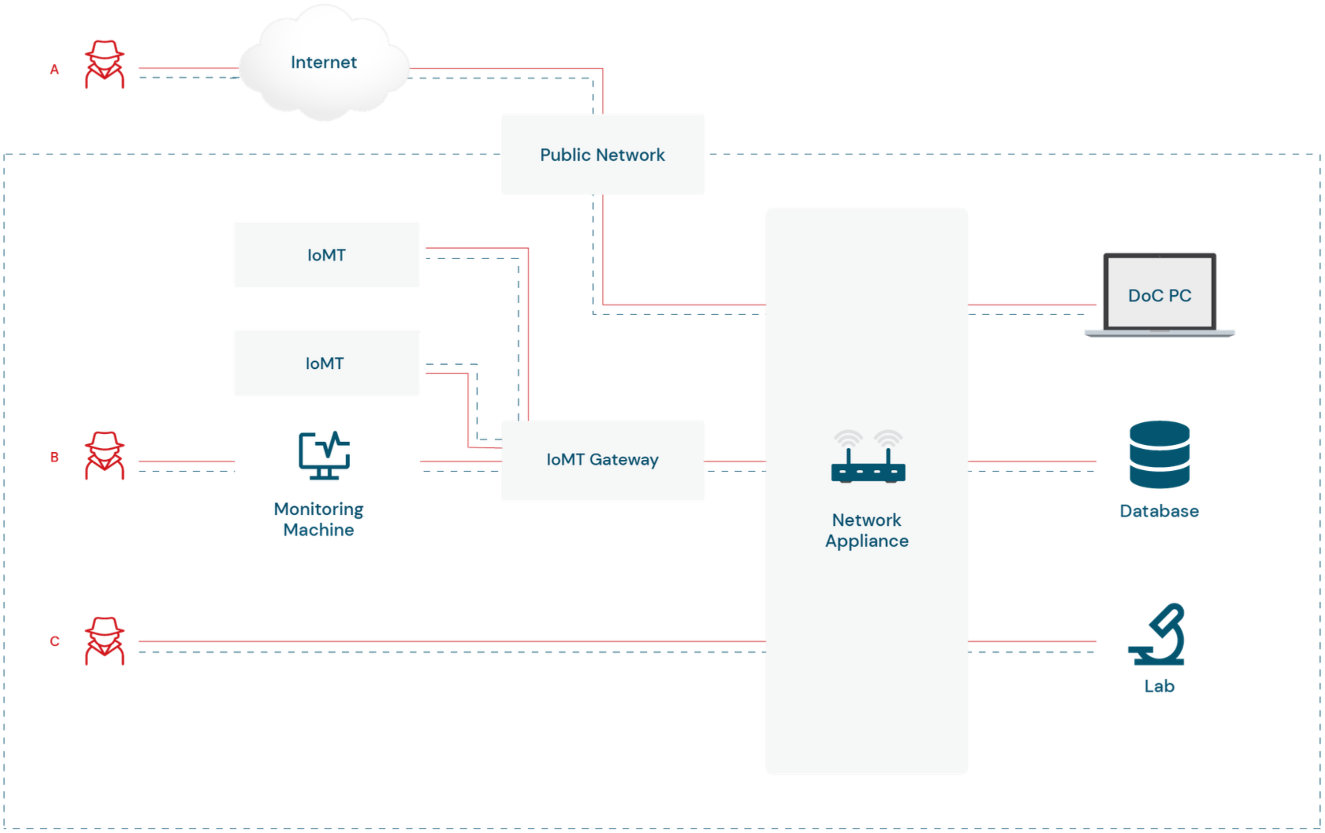
The architecture consists of a dual network structure, with one connected to the public internet and the other secured internally within a private network. Network appliances, including routers and gateways, act as gatekeepers and traffic managers. Within this network, IoMT devices, facilitated by IoMT gateways, play a pivotal role in patient monitoring. These devices, from patient monitors to infusion pumps, relay vital health data.
Doctor's computers, essential for medical operations, link to the private network, potentially storing sensitive patient information. A centralized database securely holds critical data, encompassing patient records and financial information.
We have identified three potential threats targeting a hospital, each with the objective of illicitly obtaining specific information, such as patient or financial data, orchestrated by malicious actors (hackers).

These attacks also involve the manipulation of connected devices, posing a dual risk by potentially disrupting hospital operations and putting the lives of patients at stake.

The first attack (A) occurs remotely over the internet, as a malicious actor exploits vulnerabilities in the hospital's public network, successfully breaching the defenses of the network appliance(gateway or router). This unauthorized intrusion could potentially provide access to the doctor's computer, allowing the attacker to manipulate connected devices and/or gain entry to sensitive hospital information.

Attack B is carried out locally, effectively infiltrating the monitoring machine before advancing to compromise network appliances. Subsequently, it gains entry to the Database, which may house both patient data and the financial information of the hospital.

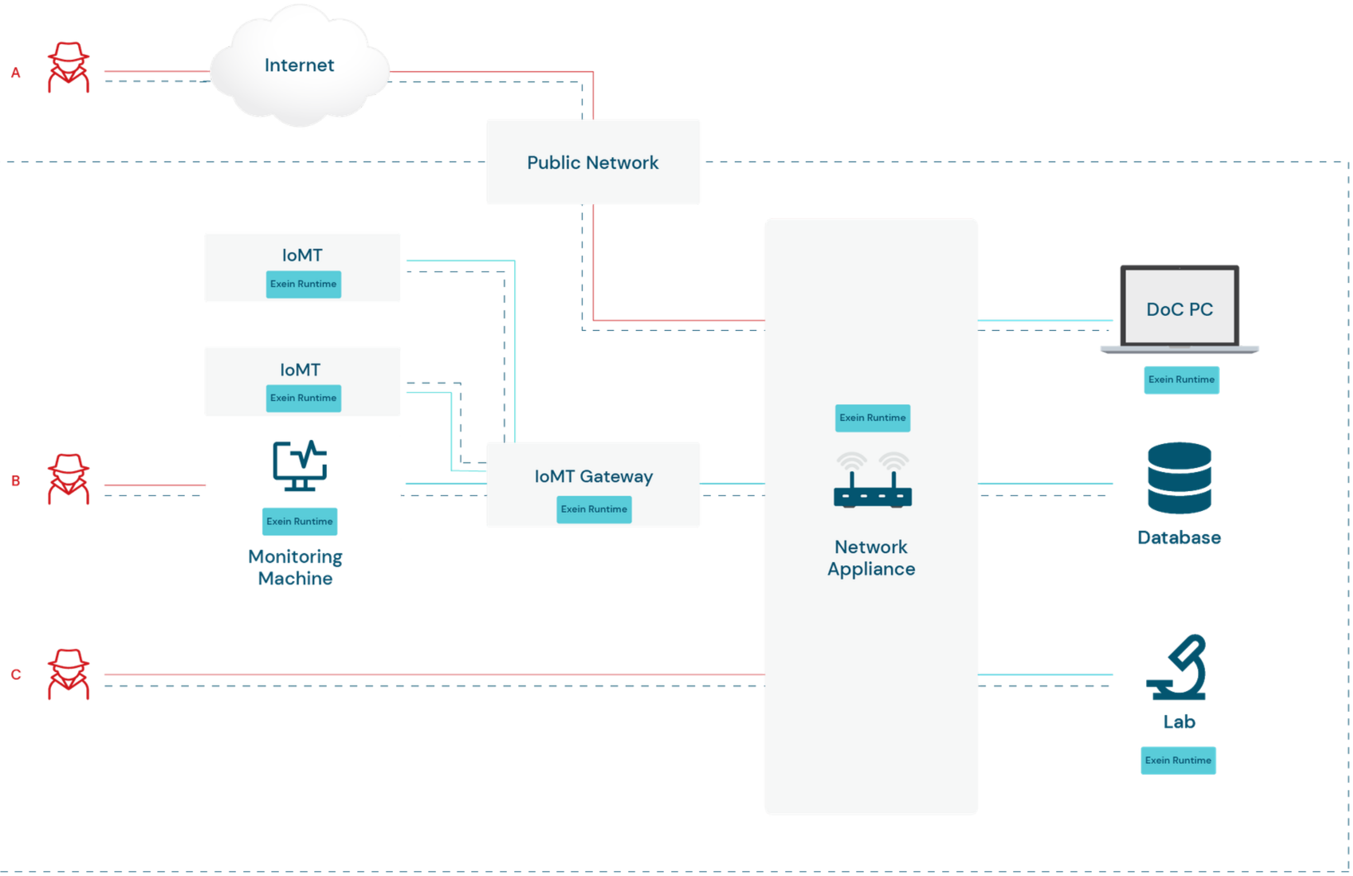
Attack C, also occurring locally, exploits vulnerabilities in the network appliance. Upon successfully breaching the defenses, it gains access to the laboratory.



In all the attack scenarios we've illustrated before, the potential consequences include compromised patient privacy and security, disruption of medical services, potential financial losses, and damage to the hospital's reputation.

To counter these threats, Exein Runtime is strategically deployed on IoMT devices, IoMT Gateways, and all network appliances, as well as internal PCs.

This ensures that the entire infrastructure is protected with a multilayered security approach, providing comprehensive protection at various levels.



8. Exein

Our Enterprise solution brings together several components to enhance attack mitigation effectiveness. With its robust architecture, the solution incorporates the following essential elements:

a. Exein Runtime

Exein Runtime is a real-time threat detection and response solution. It works to detect and address potential cyber threats and autonomously responds to any potential threat minimizing the risk of a successful cyberattack.

Runtime utilizes on-device machine learning to deliver advanced, automated, and up-to-date security measures. It provides granular visibility on the device filesystem, network and process stack allowing for flexible security policies to be adapted and enforced in real-time.

After identifying cybersecurity incidents, Exein Runtime promptly notifies our SIEM Platform, enabling the initiation of appropriate countermeasures.

b. Exein Analyzer

Exein Analyzer offers continuous firmware analysis and vulnerability detection throughout every stage of the device lifecycle, including development, production, and post-production.

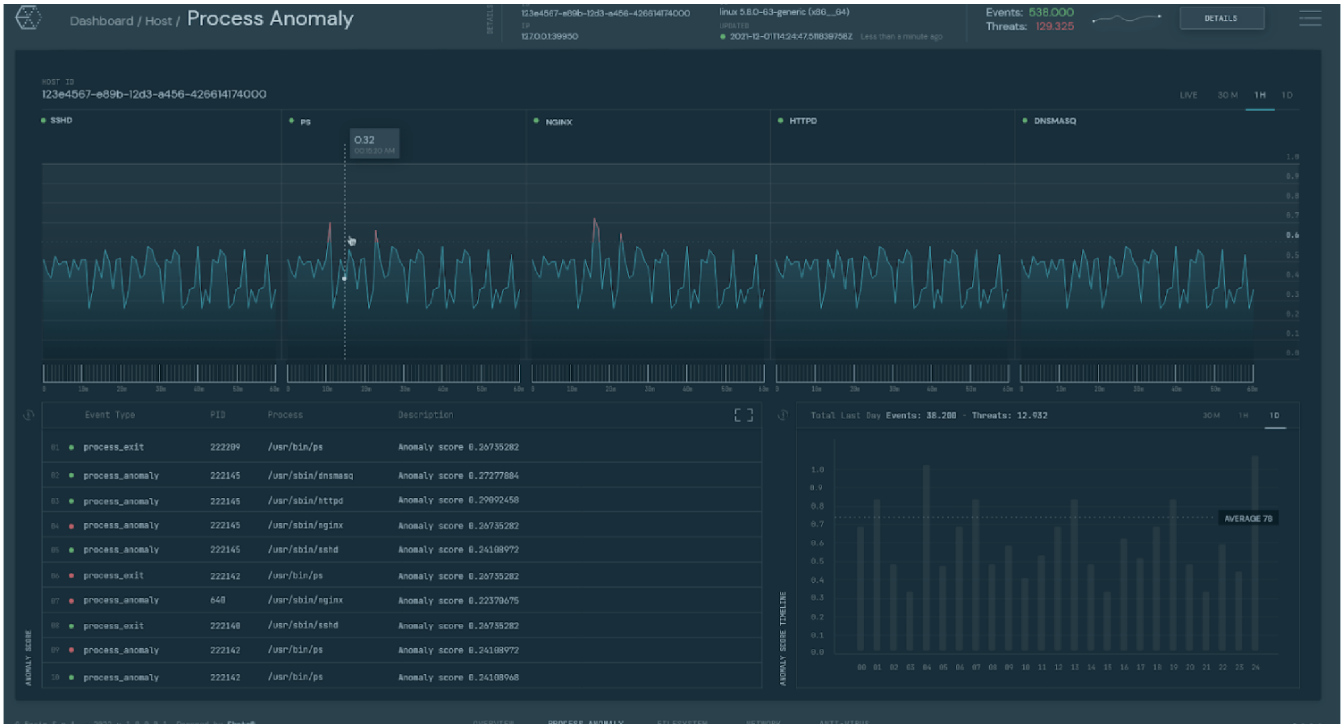
Exein Analyzer is able to identify all potential threats, including weak passwords, common vulnerabilities and exposures caused by third party software, insecure compiler settings, compromised cryptographic certificates and more.
Based on the scan results, Exein Analyzer creates a clean, exportable report overview that summarizes all the key insights found and assigns a priority ranking to each item for a quick and efficient resolution of the vulnerabilities.

c. Exein Platform

Exein Platform functions as an advanced SIEM to manage machines and systems. This comprehensive platform seamlessly integrates processes and a team of highly skilled experts, offering an array of features such as data collection, reporting, analysis, and firmware updates.

Exein Platform has three main tasks:

- **Threat Intelligence**: Performing forensic analysis of security incidents allows the identification and resolution of root causes of breaches, enabling a comprehensive understanding of potential threats.
- **Monitoring**: It tracks and analyzes the activities of each individual device.
- **Asset identification**: Once Exein Runtime is installed on all devices, it is possible to identify the entire fleet of IoT devices in a single solution.



123e4567-e89b-12d3-a456-426614174000
IP 127.0.0.1:39950
linux 5.6.0-63-generic (x86__64)
UPDATED 2021-12-01T14:24:47.5118397582 Less than a minute ago
Events: 538.000
Threats: 129.325

HOST ID
123e4567-e89b-12d3-a456-426614174000

	Event Type	PID	Process	Description
01	● process_exit	222209	/usr/bin/ps	Anomaly score 0.26735282
02	● process_anomaly	222145	/usr/sbin/dnsmasq	Anomaly score 0.27277884
03	● process_anomaly	222145	/usr/sbin/httpd	Anomaly score 0.29892458
04	● process_anomaly	222145	/usr/sbin/nginx	Anomaly score 0.26735282
05	● process_anomaly	222145	/usr/sbin/sshd	Anomaly score 0.24108972
06	● process_exit	222142	/usr/bin/ps	Anomaly score 0.26735282
07	● process_anomaly	648	/usr/sbin/nginx	Anomaly score 0.22370675
08	● process_exit	222140	/usr/sbin/sshd	Anomaly score 0.26735282
09	● process_anomaly	222142	/usr/bin/ps	Anomaly score 0.24108972
10	● process_anomaly	222142	/usr/bin/ps	Anomaly score 0.24108968

Total Last Day Events: 38.288 - Threats: 12.932

Contact Us

Throughout this white paper, we have highlighted the importance of addressing cybersecurity threats in IoT and IoMT devices found in Hospitals.

We recognize that every organization has unique security needs, which is why our solution is customizable to meet those specific requirements.
Our team of experts will work with you to understand your project requirements
and provide a proof of concept (POC) that is entirely free of charge.

During the POC, we will discuss how our technology can help solve your security problems and provide an opportunity to see it in action.

Contact us at hello@exein.io