EXEIN

Securing Smart Homes

How to Protect Against Evolving Cyberthreats

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 | Q3 2023

www.exein.io

Table of Contents

1. IoT is Everywhere

Can you say, without thinking about it too much, how many Internet-connected objects have you used today? Probably not, and don't try to count them: we are almost certain you might overlook more than one.

You went for a run, did you bring your smartwatch with you? and before leaving, have you commanded your smart home to turn off all the lights and appliances?

And if you've been drinking coffee, is it possible that the machine you used was also connected to the Internet?

The areas of application for the Internet of Things are potentially endless: from smart thermostats, smoke detectors, lightbulbs, appliances, entertainment systems to cameras and speakers.

The only limit in short seems to be imagination: any object, as long as it is connected to the Network and communicates something to someone, can fall under this definition.

Even the cat's bowl, as long as it is equipped with a sensor that communicates, for example, if the cat has finished its ration of food.

2. Smart Homes

A smart home is an intelligent environment equipped with interconnected devices that can be controlled remotely or automatically. These devices enhance convenience and efficiency by automating tasks, such as lighting, security, and climate control, often via smartphone apps or voice commands.

Manufacturers of IoT appliances for smart homes hold the key to shaping this transformative industry. While user-centric features and seamless functionality are indeed paramount, a critical consideration that must not be overlooked is the security of these devices.

Prioritizing performance and user-friendliness over ensuring robust protection against cyber attacks may cause vulnerabilities in devices that malicious individuals can exploit, potentially gaining access to entire home networks.

This happens because as devices are introduced into networks, they collectively form an expanding attack surface, providing cybercriminals with multiple entry points to compromise user data and privacy. To address these pressing concerns, device manufacturers must prioritize robust cybersecurity measures throughout the entire development process.

3. IoT Communication in Smart Homes

To identify potential threats, it's vital to note that devices continuously communicate with each other and the environment. IoT devices use various protocols, with a common communication pattern:

1 Device-to-Device Communication

IoT devices within a smart home can communicate with each other using protocols like Zigbee, Z-Wave, Bluetooth, or even proprietary wireless protocols designed for short-range communication.
Example: a motion sensor might communicate with a smart light bulb using Zigbee to trigger the light to turn on when motion is detected.

2 Local Network Communication

Many IoT devices connect to the home's local Wi-Fi network, allowing them to communicate with each other and potentially with a central hub or gateway. This local communication enables devices to work together within the same network.
Example: a smart doorbell might communicate with an indoor monitor or a mobile app over the local Wi-Fi network.

3 Cloud Connectivity

IoT devices often connect to cloud services provided by manufacturers. This cloud connection allows for remote access, data storage, software updates, and additional services.

Cloud connectivity enables users to control and monitor their devices remotely, often through smartphone apps or web interfaces.

4 User Interaction

Users can interact with their IoT devices through cloud-connected mobile apps. These apps provide a convenient interface to control and monitor devices remotely.

5 Data Collection and Analysis

Data collected by IoT devices, such as temperature readings, motion detection, or energy usage, can be transmitted to the cloud for storage and analysis. Cloud services can provide insights and trends based on the data collected from multiple devices.

6 Automation and Remote Control

Users can create automation routines that trigger specific actions based on device interactions or time-based events. These routines can be configured and managed through cloud services.

Overall devices communicate with each other locally using protocols like Zigbee or Bluetooth, connect to the local network for broader interactions, and leverage cloud connectivity to provide remote access and advanced features.

Security measures at each stage of communication are vital to ensure the privacy and integrity of the data being exchanged and to prevent unauthorized access.

4. The Threat is Real

2016

Mirai DDoS Attack on Dyn

The attack overloaded Dyn's servers with a massive amount of traffic, disrupting its ability to translate domain names into IP addresses. This resulted in widespread internet outages affecting numerous websites and online services like Twitter, Reddit, and Netflix.

2016

DDoS Attack Paralyzes IoT-Based Heating Systems in Finnish Properties

IoT-based heating systems in Finnish properties, offering remote internet control, fell victim to a crippling DDoS attack. Hackers flooded these devices with excessive traffic, rendering them temporarily inoperative and causing heating disruptions for residents during winter.

2019

Ring Security Cameras Compromised

Reports emerged of unauthorized access to Ring security cameras, manufactured by Amazon. Hackers were able to breach user accounts and gain unauthorized access to the cameras, allowing them to watch and communicate with people inside their homes.

2020

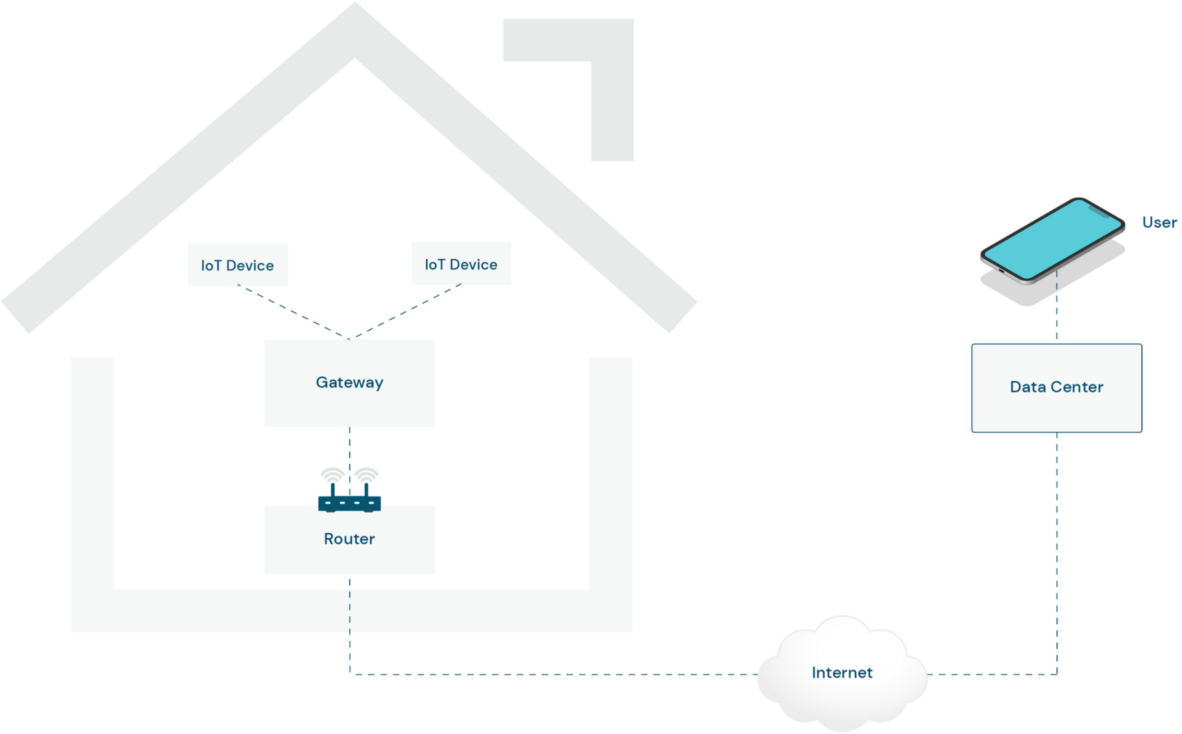
Massive IoT Data Breach

Cybersecurity researchers discovered a significant data breach involving an exposed database that contained over 2 billion records of data from various Internet of Things (IoT) devices and smart home systems.

There are many more incidents that are publicly reported.
By way of example, this brief listing of cyber crimes and cyber attacks quickly illustrates the gravity of such events.

Similar attacks 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 against a utility will cause widespread damage.

5. Exein Runtime on Smart Home Appliances



In examining the architecture of a conventional connected home, a prevalent scenario emerges where homeowners can seamlessly interact with their smart devices, even when they are away from their residence.

This interconnected ecosystem relies on the synergy between various IoT devices, which communicate among themselves and establish connections with a central router and gateway. What distinguishes this setup is the bilateral nature of the connection: not only can users control and monitor their smart devices remotely, but these devices can also transmit essential data back to the user.

This reciprocal communication empowers homeowners with unprecedented convenience and real-time insights into their home environment.

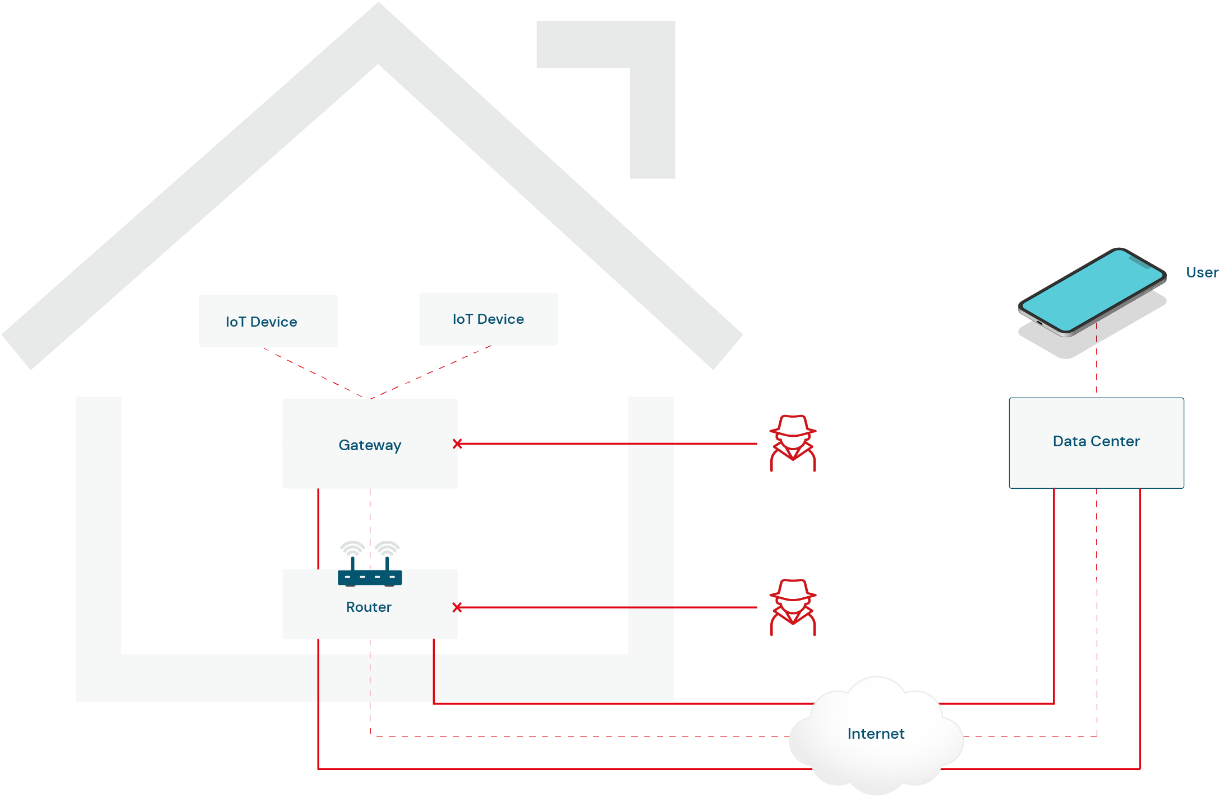
For instance, picture a scenario where a homeowner, while at work, adjusts the lighting in their living room using a smartphone app. Smart lights instantly respond, creating the desired ambiance even before the homeowner arrives home.

We identified two potential attack scenarios within the context of a smart home architecture:

First, an attack directed at the router involves exploiting vulnerabilities in its firmware or software, granting the attacker unauthorized access to the home network. Once inside, the attacker intercepts and manipulates data traffic between IoT devices and the data center, potentially compromising user privacy and gaining control over the connected devices.

Similarly, targeting the gateway offers another avenue for intrusion. An attacker exploiting vulnerabilities in the gateway's security could potentially compromise the centralized control point of the smart home ecosystem. This breach would enables the attacker to manipulate the communication between IoT devices and the gateway, taking control of these devices and compromising the integrity of the data transmitted.

In both scenarios, the repercussions extend beyond device control to the unauthorized access and manipulation of sensitive data.

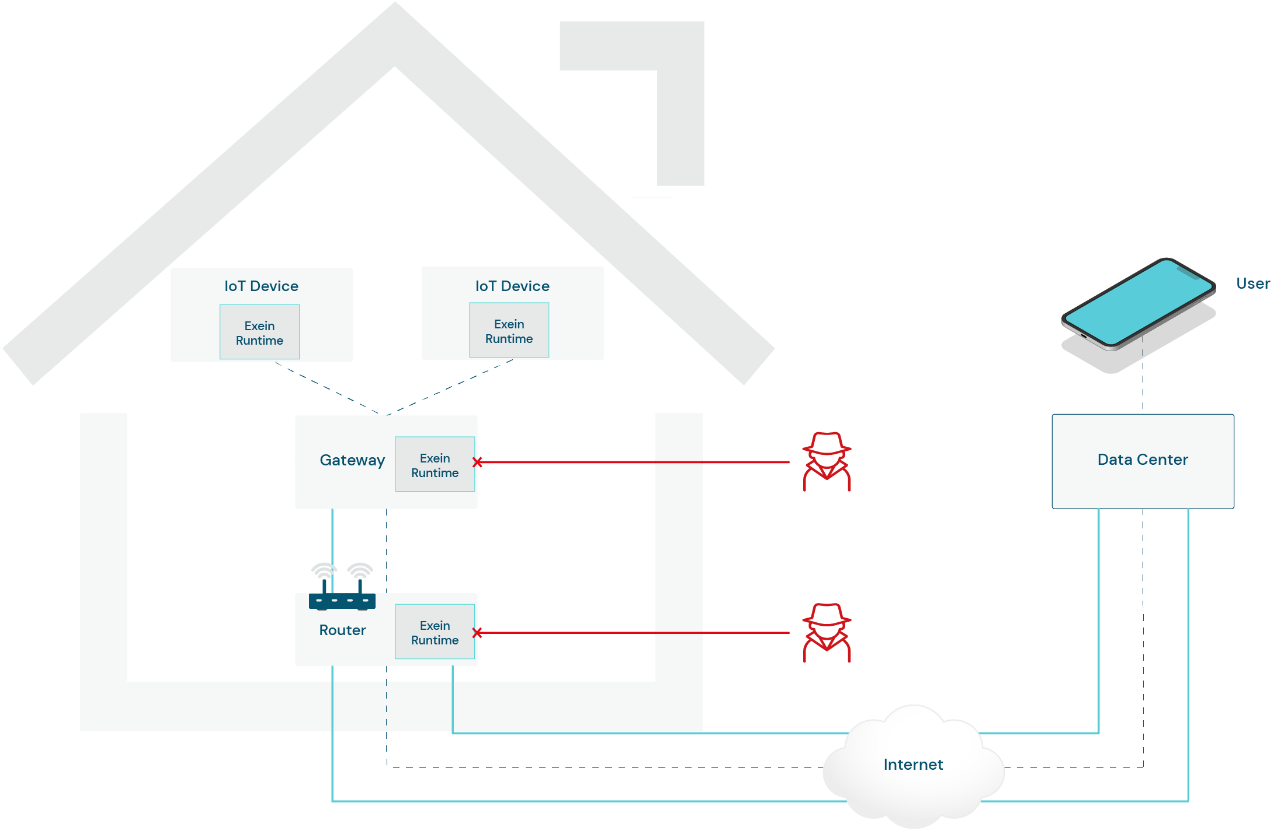


To counter these threats, **Exein Runtime is strategically deployed on the Router, Gateway and IoT devices**, providing comprehensive protection at various levels.

Our advanced security solution harnesses on-device machine learning for proactive, high-performance, and up-to-date security, specifically designed for IoT and edge computing.

It actively monitors filesystem activity, enforces access rules, and continuously evolves to stay ahead of emerging threats.

Moreover, its seamless integration with existing embedded devices enhances security within smart home environments, ensuring the safety of connected devices and the integrity of the data they manage.



6. 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.

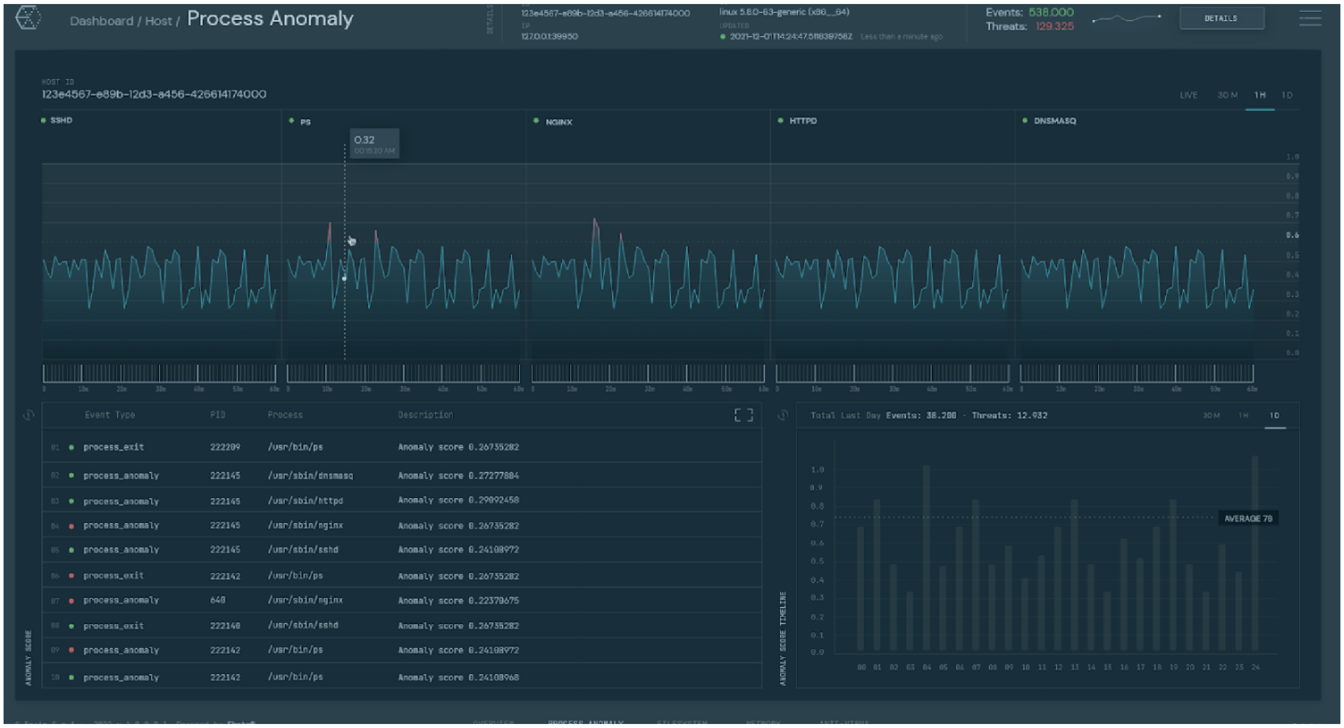
Exein Analyzer is able to identify all potential threats, including weak passwords, common vulnerabilities and exposures caused by third party software, insecure compiler settings, compromised cryptographic certificates and more.
Based on the scan results, Exein Analyzer creates a clean, exportable report 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
UPDATED 2021-12-01T14:24:47.5118397582 Less than a minute ago

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: 38.280 - Threats: 12.932

7. The EU Cyber Resilience Act

The EU's Cyber Resilience Act (CRA) mandates robust cybersecurity measures across digital systems. It guides OEMs to prioritize security throughout the product lifecycle, ensuring compliance with stringent EU standards.

Security Requirements

Secure Product Design

Security should be prioritized throughout a product's lifecycle, making it resilient against cyber threats.

Risk Assessment

Understanding and mitigating potential risks through comprehensive assessments is essential.

Cybersecurity Documentation

Maintaining records of cybersecurity aspects, including vulnerabilities and updates, is key.

Third-Party Component Integration

Integrating third-party components requires caution and thorough verification.

Risk Assesment Management

Product Vulnerability Management

Proactive handling of product vulnerabilities, including reporting and prompt issue resolution, is crucial.

Conformity Assurance

Pre-launch assessments ensure product compliance with cybersecurity standards, evidenced by an EU declaration of conformity and CE marking.

Product Compliance Monitoring

Continuous compliance monitoring and adapting to regulatory changes are vital throughout the product's lifecycle

Documentation Maintenance

Technical documentation and the EU declaration of conformity should be accessible for authority inspection.

Compliance and Collaboration

Compliance Maintenance

OEMs should ensure that products continuously meet security standards, adapting to regulatory changes and product design alterations.

Reporting and Corrective Actions

Prompt corrective actions, including potential product recall, are necessary for non-compliant products.

User Information and Instructions

Providing clear instructions for secure product use can enhance cybersecurity.

Authority Collaboration

Active collaboration with authorities is necessary for effective incident management and cybersecurity risk mitigation.

Exein: Simplifying Compliance

Exein Runtime aligns with the EU's Cyber Resilience Act, providing device security, risk mitigation, and network compliance. Its features comprise network anomaly detection, file system access blocking, and AI-powered real-time threat response.

Additionally, Exein Analyzer offers detailed security overviews without the need for firmware source code access or agent installations. It integrates effortlessly with asset identification tools for comprehensive IoT ecosystem scans. Exein enables OEMs to effectively navigate the complexities of cybersecurity compliance, adhering to the robust standards of the EU Cyber Resilience Act.

Exein: Leader of IoT Security

At Exein, we are dedicated to empowering organizations around the world to build secure IoT devices.

Our purpose-built technology, developed by our team of cybersecurity and embedded systems experts, ensures that every device is protected from cyber threats in real-time.

We have a proven track record of success, with over 20,000 developers worldwide adopting our solutions to make more than 600,000 devices secure every day.

Our technology is trusted by the world's largest corporations in mission-critical environments, from aerospace to automotive, industrial IoT, telco, and defense.

80M

IoT devices protected at runtime on the field

100K

security scans performed on weekly basis

20K

developers worldwide adopting our solutions

600K

devices secure everyday

Contact Us

Throughout this white paper, we have highlighted the importance of addressing cybersecurity threats in IoT devices found in Smart Homes.

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