CyberusLabs

ELIoT Pro White Paper Series: Part 4

Stay ahead of the hack

HOW BUILT-IN SELF-HEALING TECHNOLOGY WITH PREDICTIVE ANALYTICS, WILL HELP OPTIMISE IOT SUPPLY CHAINS AND KEEP SYSTEMS SAFE, SECURE, AND OPERATIONAL

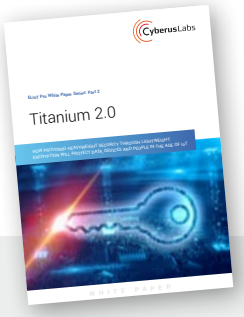
WHITE PAPER

A note on the ELIoT Pro White Paper Series

The ELIoT Pro four-part white paper series details how Cyberus Labs has identified the key issues that need to be addressed in order to develop the industry's first end-to-end cyber security solution for IoT.

Part 1

considers the issues associated with using passwords for Human-to-Machine (H2M) authentication and the move into the post-credentials era.



Part 2

explores Machine-to-Machine (M2M) authentication, including the problems associated with designing cyber security for IoT devices.

Part 3

examines the need to set rules to monitor the behaviour of an IoT device, track its performance and to detect malfunctions.

In this paper, Part 4,

we discuss the importance of Self-Healing and Device Replacement to keep IoT systems fully operational.

Table of Contents

Executive Summary 3

Lack of self-healing ensures infection risk stays high 4

Stakeholders could pay a high price for inaction 6

Perfecting the recipe for better run, safer IoT networks 8

Presenting EP Cortex Self-Healing engine 9

Three layers of cyber security working together as one 12

Compliance and ELIoT Pro's three layers 13

Conclusion 14

More about Cyberus Labs 15

- A note on ELIoT Pro 15
- Role of Horizon 2020 16

Executive Summary

As the growth of IoT networks accelerates, monitoring and maintaining IoT devices and ensuring optimised performance levels is becoming a major element of IoT cyber security management.

Problems with IoT system management and security have already proved costly for several industries with Device Vendors (DVs) running the risk of losing sales and gaining a poor reputation for customer service, while System Owners (SOs) remain in fear of underperforming devices and the cyber security risks they bring.

Similar to the recent sea-change in data privacy and GDPR, compliance has already begun playing a key role in IoT. Legislation right across the globe is on the way and will ensure both SOs and DVs ultimately realise that it is in their best interests to create robust, safe IoT network and environments.

Technology has already developed many of the key ingredients required to tackle this problem. The use of artificial intelligence, self-healing capabilities, inventory control methodologies, and ecommerce platforms can all play a role delivering a solution that can ease these concerns.

INTRODUCING EP CORTEX

In response to this need, Cyberus Labs have developed an IoT-specific data analytics module known as EP Cortex. An integral part of the world's first end-to-end cyber security solution ELIoT Pro, EP Cortex is home to a predictive analytics capability and IoT device marketplace, alongside other key elements like device profiling and rules management system.

SOs will have access to dashboards that show device performance and display operational limits that the device should not exceed. This ensures the SOs stays fully informed and can detect anomalous or suspect behaviour, ultimately allowing them to buy replacement or additional devices direct from their vendor through the EP Cortex ecommerce portal.

Also containing diagnostics and self-healing properties, EP Cortex deploys data analytics to provide a new level of visibility and management for system owners. It works in tandem with ELIoT Pro's core cyber security elements including H2M password-free user authentication and M2M password-free encryption and machine authentication.

Lack of self-healing ensures IoT system-failure risk stays high

In today's IoT world, the lack of proactive thinking and stakeholder collaboration is resulting in suboptimal devices being left in position even when broken or underperforming, leaving the door open for bad actors and cybercriminals.

Devices are under major pressure and a 2018 study[1] reported that on average, IoT devices are attacked within five minutes of being plugged into the Internet.

IoT networks and the number of devices in each can range from a few hundred to hundreds of thousands. SOs must have real-time insight into the performance and health of each device. Any device that is not performing as expected within predefined parameters has either been hacked or requires repair/replacement.

All parties need to embrace the fact that it's no longer acceptable or even possible to fix a system after a hack or breach has taken place. In this context, monitoring and predicting when a breach or malfunction is approaching and preventing attacks before they happen is essential. In fact, research has shown that 50%[2] of all businesses are unable to detect if their IoT devices suffered a breach.

COMPROMISED DEVICES NOT BEING REPLACED

In many cases, devices are not being replaced on time even if they are presenting anomalous behaviour. If these components or sensors are not doing what they should, this is a problem for SOs. And even in the event of underperforming devices or anomalous behavior, the purchasing systems are not in place to facilitate fast action and replace devices effectively.

Many cyber security solutions on the market allow for real-time viewing of data but a lack of automation means it can still take months before a breach or malfunction is noticed. SOs and DVs need to be aware of the performance of their systems and devices in real-time, to ensure a safe and efficient performance.

[1]https://www.netscout.com/sites/default/files/2019-02/SECR_001_EN-1901%20-%20NETSCOUT%20Threat%20Intelligence%20Report%202H%202018.pdf
[2]https://www.gemalto.com/press/pages/almost-half-of-companies-still-can-t-detect-iot-device-breaches-reveals-gemalto-study.aspx

Cyber criminals prey on inaction and the opportunity arising from it. This lack of self-healing has the potential to do substantial damage to the global IoT network.

In parallel, physical device failure represents another challenge for IoT SOs. And while DVs can predict device failure to a degree, and SOs know and understand their network, the time has come for stakeholders to connect on a continuous, real time basis to keep systems running at an optimum level.

AUTOMATION IS KEY

Manual monitoring alone is simply no longer an option and automation through available technologies is key. Better supply chains and supply chain functionality can ultimately create a more streamlined procurement and replacement process.

It is only by adapting some form of automated, two-way capability where device replacement and data exchange can work in tandem in order to guarantee system continuity, that this problem can be resolved. By ignoring the need to move forward, SOs and DVs are taking major risks as the consequences range from heavy fines to breached networks, and more.

Stakeholders could pay a high price for inaction

This lack of collaborative thinking, resulting in poorly updated and badly equipped IoT networks, is already having and will have in the future, major ramifications for SOs and DVs across all sectors. From safety and security for SOs to compliance and reputational issues for DVs, impacts may well be severe and wide-ranging.

SECTORS FACE INDIVIDUAL CHALLENGES

When smart home devices malfunction, it can have genuinely serious consequences for householders. Nest thermostats found themselves at the centre of such an issue in the winter of 2016[1] when thousands woke up throughout America and Canada in freezing homes as their smart thermostats had drained their own batteries and so were no longer able to function. Without solid management and device-replacement functionality in place, IoT networks are vulnerable, and open to not just malfunction, but intrusion and hacking.

Industrial IoT plays a crucial role in modern factories and production plants with sensors, thermostats, and many other devices in operation right across manufacturing facilities. Their sheer numbers make them vulnerable in security terms, and also illustrate the real threat of downtime. Without identifying the performance of its many sensors and devices across a factory, industrial IoT SOs are taking major risks.

DEVICE VENDORS UNDER THREAT

As the market for IoT devices continues to grow, device vendors are becoming increasingly aware of how damaging suboptimal devices can be. And this manifests itself across a number of key areas...

Loss of business – as the market grows, the opportunity grows for an IoT DV to identify that consumers are concerned and take steps to hard-wire robust IoT cyber security into their units as a matter of purpose. By demonstrating to buyers and SOs that cyber security is an investment, not a cost, DVs can seek to avoid loss of business. It stands to reason that DVs who do not develop or build secure devices and networks, will suffer loss of business to those who do.

[3] https://www.cbc.ca/news/technology/nest-smart-home-problems-1.3410143

Damage to Reputation – recent research, conducted for the Internet Society and Consumers International, found that 65%[4] of consumers are concerned with the way connected devices collect data, and 55% do not trust their connected devices to protect their privacy. From the controversy surrounding international telecoms and accusations of political espionage to the stories of IoT devices eavesdropping on conversations, consumers are wary. And when stories of malfunctioning devices emerge, they will become even more concerned. For DVs who do not respond to these concerns and continue to deliver poorly performing, porous networks, loss of reputation is inevitable. Conversely, smarter DVs can seize the opportunity to grasp a competitive advantage by developing robust systems that monitor networks and devices, assess and predict needs, and enable SOs to maintain networks that will provide security, safety, and more

Compliance – IoT legislation is in its early days and the entire sector is waiting for higher regulatory standards which will be welcomed by many, right across the globe. Already, legislation is before the Senate in the United States and the first steps have been taken to form an EU cyber security agency, ENISA, which will be tasked with creating a framework for cyber security certification for ICT products, to be rolled out across the EU.

Both DVs and SOs who fail to comply by not providing robust, high performing devices and networks will face the wrath of compliance penalties in the form of heavy fines. Investing in the right cyber security solutions and ensuring systems are easily managed, updated, and have the capacity to replace devices easily, will significantly ease this compliance headache.

[4] https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/

Perfecting the recipe for better run, safer IoT networks

Technology does hold many of the ingredients required to solve this problem. System monitoring, predictive analytics and efficient inventory supply management all have the capacity to play a role in a system which increases stakeholder interaction, resulting in better run, safer networks. Individually, they have shown their value in numerous areas.

In the IT world, **self-healing systems** have been around for many years. These systems are designed to proactively monitor and identify a potential deviation from its standard parameters, before validating it with a degree of confidence, and resuming normal operations. Self-healing engines were originally designed to prevent downtime and allow a system to identify suboptimal behaviour before resolving some issue automatically or alerting the right personnel who have the expertise to act.

Mean time between failure (MTBF) is an established metric in engineering and technology sectors. It is a calculation designed to track the predicted elapsed time between inherent failure of a mechanical or electronic system, during what is considered normal system operation. When SOs understand how reliable a hardware product or component is, they can be ready for any potential downtime in advance. It might be in thousands or even tens of thousands of hours between failures and is always designed to give the user as much insight as possible into what level of service or maintenance might be required.

Just-in-time (JIT) is an inventory system that aligns raw-material orders from suppliers directly with production schedules. Originating from the Japanese automotive sector in the 1970s, it is now accepted as a hallmark of efficiency across many industries worldwide.

Recognising the value of each of these technological elements, our team at Cyberus Labs have fused them with other key components to create a robust analytics capability which we call **EP Cortex**, a crucial part of **ELIoT Pro**, the world's first end-to-end cyber security solution for IoT.

Presenting our EP Cortex Self-Healing engine

At Cyberus Labs, we are proud to present our purpose-built EP Cortex technology, home to our unique ELIoT Pro IoT artificial intelligence engine.

Made up of several key components, including monitoring, diagnostics, and self-healing, it is the third layer in ELIoT Pro, our flagship cyber security solution for IoT.

Acting as a type of command centre, EP Cortex allows the system to alert its owners that a dangerous or otherwise anomalous condition has developed so that the system can respond and adjust.

Self-Healing Artificial Intelligence and more specifically our Predictive Analytics and Machine learning engine functionality plays a key role at the heart of our solution. By taking data like Meantime-Between-Failure (MTBF) statistics provided by IoT Device Vendors and combining it with our system's existing surveillance and monitoring data, EP Cortex can accurately predict device failure and facilitate swift replacement.

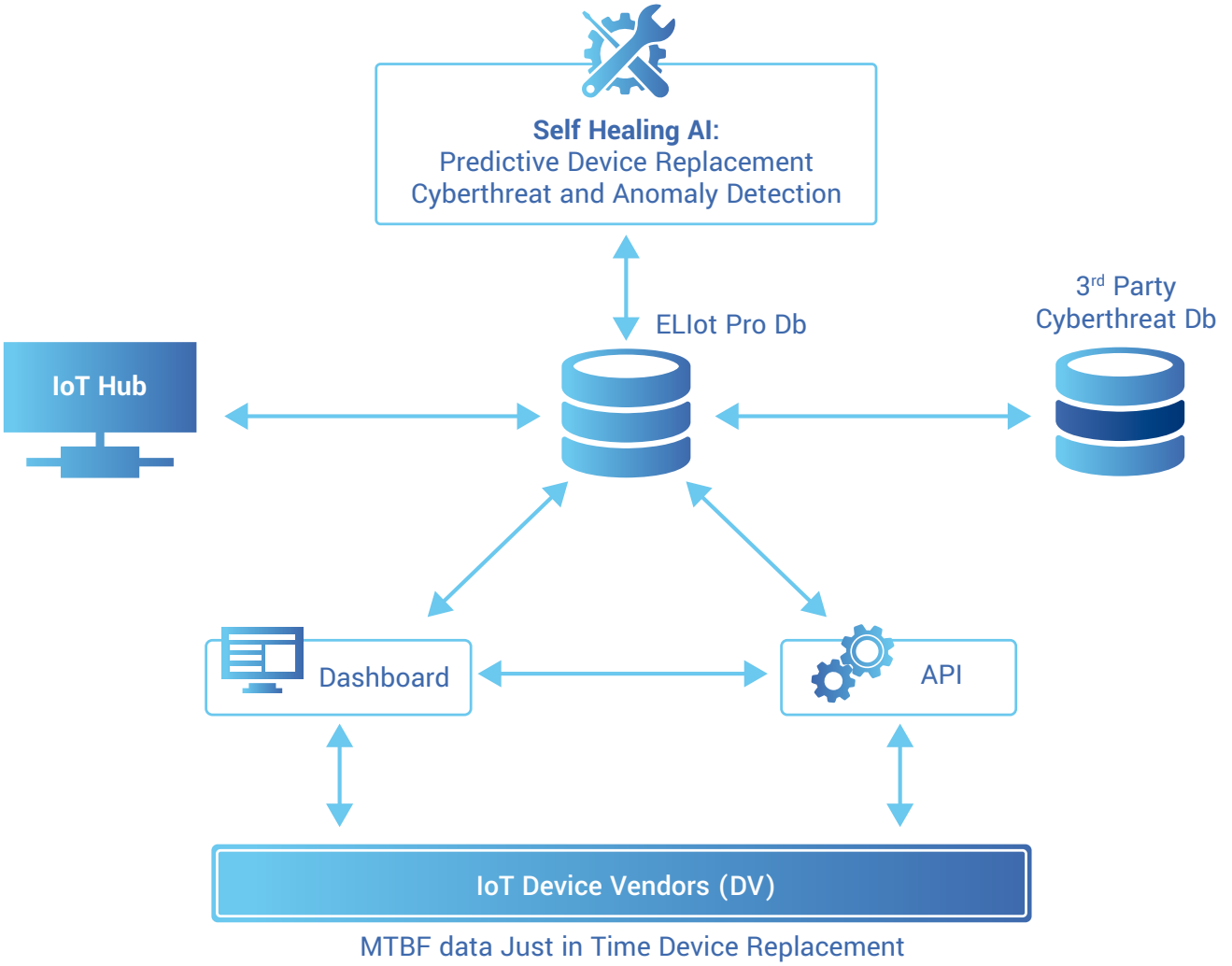
KEY FEATURES

Artificial Intelligence – by learning and monitoring normal system behaviour, EP Cortex establishes the parameters of typical behaviour. Built-in anomaly detection functionality ensures anomalous system behaviours can be identified and classified as a cyber-attack or other type of anomaly like a device malfunction.

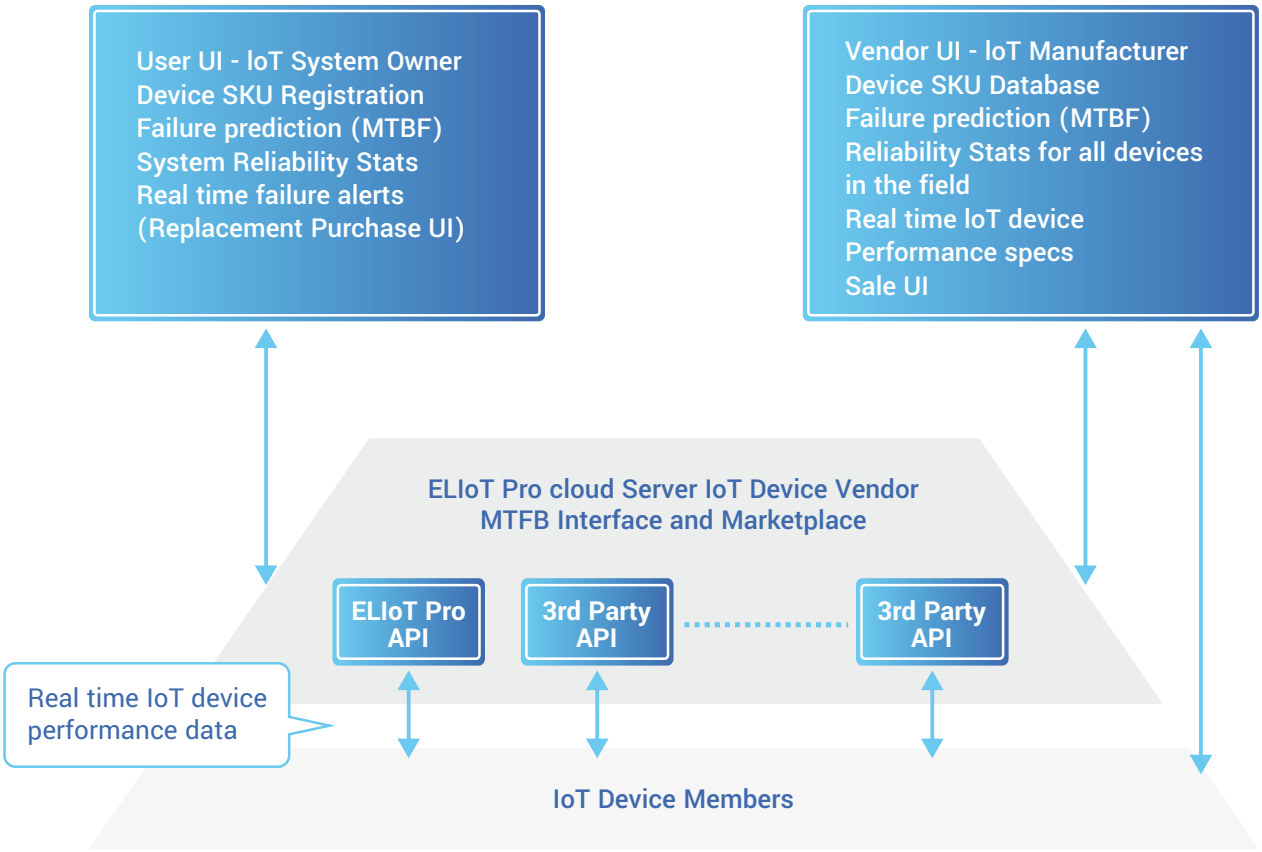
System failures can be predicted by EP Cortex based on MTBF data provided by Device Vendors. And in order to not only rely on MTBF, SOs can supply operations data to refine these numbers and build a more informed overall picture.

API - controlled through a dashboard, our API facilitates real-time interaction between the two most important stakeholders in IoT system development and maintenance – the SO and DV. EP Cortex enables SOs to request MTBF data from DVs to feed data needed by the Self-Healing AI. DVs can now also upload MTBF data to the SO while SOs can share actual in-field IoT component functionality statistics with DVs.

A natural marketplace is also created where replacement IoT devices can be purchased via the API on a Just-In-Time basis. This is a portal through which DVs can also update, fix and monitor their IoT devices in the field, so they can be in compliance with new IoT cyber security laws being currently enacted including the Internet of Things (IOT) Cybersecurity Improvement Act of 2017 (US) and The EU Cyber security Act 2019.



DETAIL FOR ELIoT PRO IoT VENDOR/MTBF INTERFACE



Three layers of cyber security working together as one

ELIoT Pro takes a step-by-step approach to achieving genuine end-to-end security for IoT devices that is firmly built on three mutually dependent pillars. And with each step taken, our level of security intensifies.

1. Beginning with **H2M authentication**, the first layer eliminates the password through the use of one-time transaction codes conveyed via a sonic transmission. Users can simply open an app on their phone and place it near their computer in order to escape the friction and hassle so many of us associate with the login process.

   Read the whitepaper

2. Building on this initial platform and with the wide expanses of the IoT ecosystem firmly in mind, the next layer brings us a level deeper again. By implementing a strong variant of **lightweight encryption**, ELIoT Pro can provide a high level of security to IoT devices with even the most minimal computational ability.

   These two defensive layers work in tandem to provide a new level of protection in our increasingly connected world.

   Read the whitepaper

3. The third and final layer brings IoT cyber security to its deepest level yet. Putting in place a data analytics element we call **EP Cortex** which acts as an IoT immune system, a complete end-to-end solution has now arrived. Through deployment of rules engines, device profiling functionality, predictive analytics, artificial intelligence, and just-in-time device replacement, **EP Cortex** provides a self-healing capability to any IoT system.

Compliance and ELIoT Pro's three layers

Compliance is truly in focus with ELIoT Pro and offers you the peace-of-mind that your IoT systems will be fully compliant with all major IoT regulations now and into the future. And as the latest software updates are available in real-time, you'll have the safest, most efficient systems, avoiding huge fines and damage to reputation.

1

Specific legislation like Internet of Things (IOT) Cybersecurity Improvement Act of 2017 addresses the need to avoid hard code credentials for **'administration, delivery of updates, or communication'**, and our H2M authentication protocols directly comply with this aspect of the standard.

2

Similarly, our Lightweight Encryption M2M capability also addresses the credentials issue, in particular the legislative requirements that **'all components are capable of being updated securely from the vendor'**.

3

Our EP Cortex self-healing functionality directly addresses a key requirement of the legislation, namely that… **'Software or firmware components should be updated or replaced, consistent with other provisions of the contract, in order to fix or remove a vulnerability or defect in the component in a properly authenticated and secure manner'**.

Conclusion

Sub-standard monitoring levels combined with fragmented stakeholder interaction are making IoT networks hard to manage in today's IoT world. At Cyberus Labs, we believe that predictive analytics and insightful use of data, combined with the capability to streamline device replacement between SOs and DVs has a key role to play in helping SOs optimise their IoT networks. And by creating a common platform for SOs and DVs, DVs will have a renewed capacity to improve customer service and sales.

IoT devices break down and in turn will very likely compromise networks. SOs must be able to make informed decisions based on hard data that is derived not just from their own networks but based on larger datasets owned by DVs. And once SOs are armed with this insight, managing their networks by replacing underperforming or broken devices will become easier and more convenient.

CONNECTIVITY, COMPLIANCE, AND MORE

Optimized connectivity, through customized portals, has transformed many supply chains and with EP Cortex, a core element of ELIoT Pro, the world's first end-to-end cyber security solution for IoT, this functionality has now also been created. And this ensures SOs can order and replace IoT devices with ease in real-time.

EP Cortex's Artificial Intelligence is designed to target anomaly detection, identify cyber-attacks and facilitate fast reaction. It will provide SOs with a new level of insight, control, and peace-of-mind over their systems, meeting security, compliance, and operational challenges simultaneously.

Benefitting from predictive analytics and just-in-time device-replacement, this unique collective of self-healing capabilities is key to maintaining a solid level of security for IoT networks today.

More about Cyberus Labs

Based in Poland, with proven Silicon Valley experience, Cyberus Labs is a team of cyber security specialists that fully understand the new cyber threats faced by your business or organisation, whatever your size.

From traditional sectors, which have fully embraced the digital age like banking and e-commerce to the fast-growing world of IoT, your consumers are under threat from hacking attacks in the form of phishing, identity and data theft, and much more. Working closely with the European Union's Horizon 2020 research and innovation programme, we continue to focus on eliminating the risk of stolen passwords or credentials for both your users and devices - with our unique password-free authentication.

A NOTE ON ELIoT PRO

IoT devices and networks currently suffer from a lack of security leaving them vulnerable to a wide range of cyber-attacks. Whether it's rogue nations, thieves or terrorists attacking vulnerable networks, cybercrime is a multi-trillion dollar global threat. When IoT devices are hacked by cybercriminals, it can create devastating financial and reputational damage, and may even endanger human lives.

With ELIoT Pro, the world's first end-to-end cyber security solution for IoT networks developed by Cyberus Labs, you will no longer have to worry about cybercrime, knowing that your IoT users, devices and data are ultra-secure.

- No more passwords or old-fashioned logins means your users' credentials can never be stolen. And by eliminating passwords on your connected devices and machines too, there is nothing for hackers to steal and no way to gain access.
- Your IoT devices have different levels of computing power. And our lightweight encryption requires lower computing power and memory than any encryption system today – making it work on even the simplest IoT devices.
- Whether you prefer cloud-based, on-premise or a hybrid model, it's easy to set up and install with API functionality, an SDK, and a white-label option also available.
- Its AI engine, known as EP Cortex, creates an adaptive, self-healing IoT environment that can anticipate system failures, identify attacks, and automatically react so SOs receive Just in Time device upgrades and replacements to keep IoT systems fully operational. SOs will also be made aware of any breach in progress and provide remedial reaction to safeguard the IoT system.

ROLE OF HORIZON 2020

Horizon 2020 funds high-potential innovation developed by SMEs through the SME instrument. The SME instrument offers Europe's brightest and boldest entrepreneurs the chance to step forward and request funding for breakthrough ideas with the potential to create entirely new markets or revolutionise existing ones.

Contact Cyberus Labs

Cyberus Labs sp. z o.o.
ul. Warszawska 6 pok. 309
40-006 Katowice
Poland

office@cyberuslabs.com

www.cyberuslabs.com

The project ELIoT Pro has received funding from the European Union's Horizon 2020 Research and Innovation programme under Grant Agreement No 822641