Cybersecurity Magazine

The future of IoT and OT security

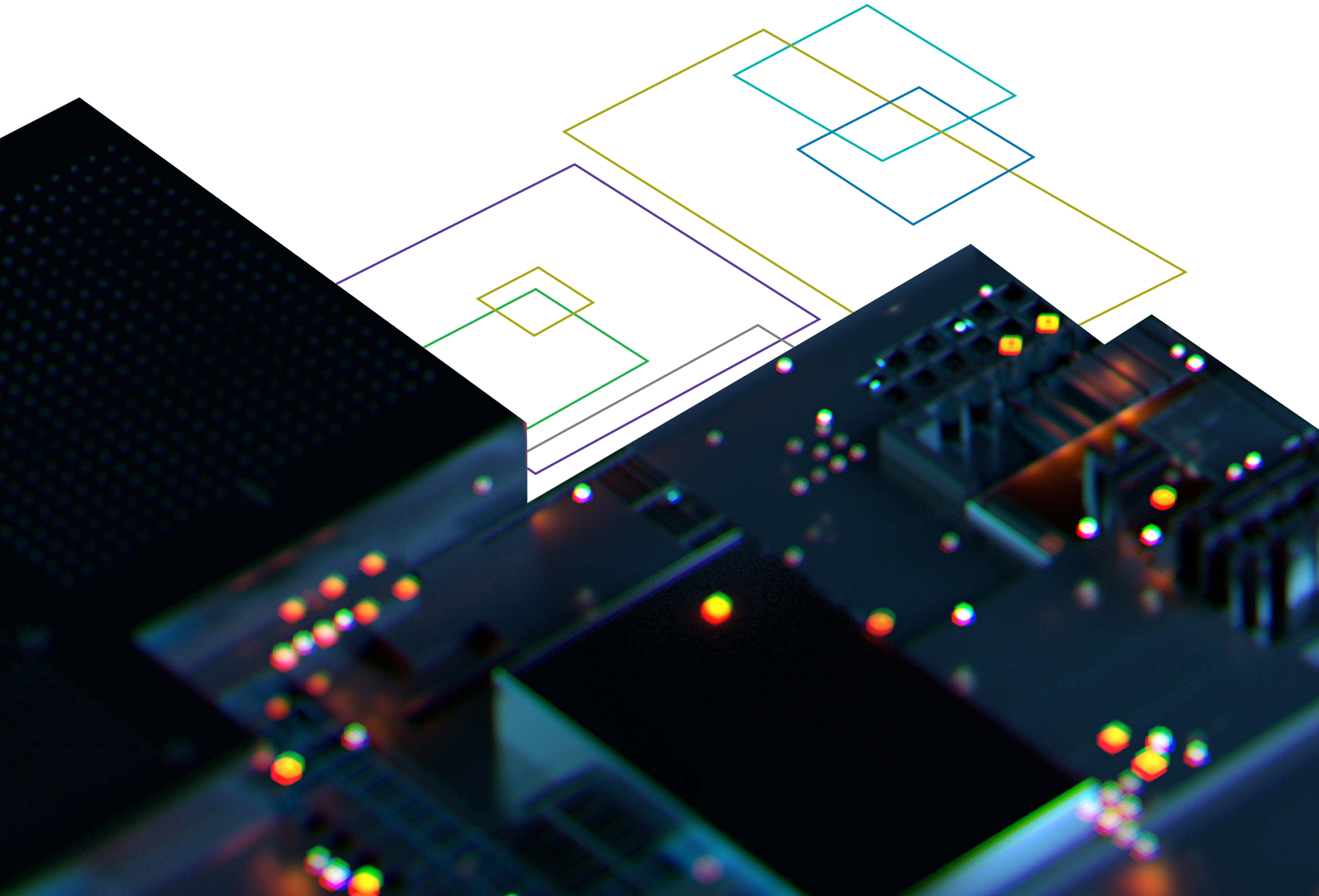
- Privacy and Security for IoT
- Cybersecurity for Industrial Control Systems
- Securing the autonomous vehicle of tomorrow
- True IT/OT/IoT Convergence Through "Middleware"
- OT assessment in time of crisis

Trusted partner for your **Digital Journey**

Atos

Cybersecurity Magazine

Number 1
Q1 2021



Editorial

Dear community,

We are pleased to share with you our first issue of Atos Cybersecurity Magazine, a quarterly publication featuring articles and stories about all aspects of cybersecurity. Our main objective is to create a space to share ideas, bring awareness about the importance of cybersecurity to all and give the right insights to better face digital security challenges.

In this first issue, we are focusing on operation technology (OT) and the Internet of Things (IoT). For that reason, we have gathered a group of members who have shared their stories and written insightful articles from IoT platforms to OT security.

As technology brings operational technologies online, the boundaries between IT and OT are becoming vaguer to identify. Not only the distinction among these environments is blurry, but also the identification of the security risks associated with them. In this context, the concept of IT-OT convergence has become a strong business leader in our customers' daily conversation.

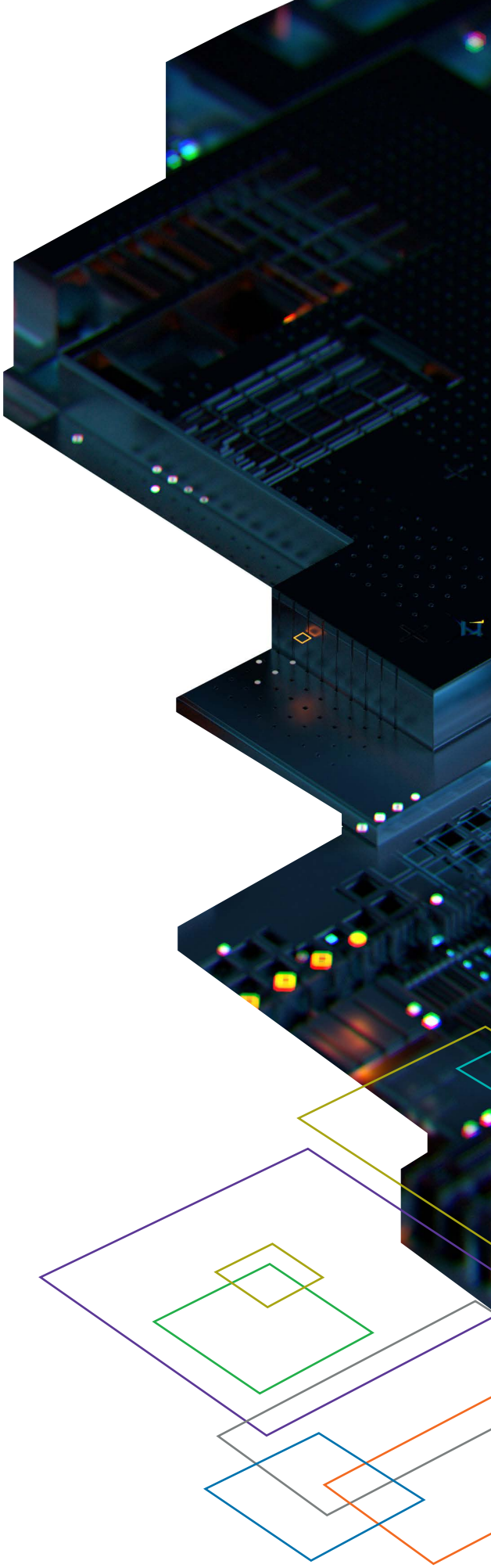
We believe it is fundamental to present the progress Atos has made on security and how our teams are actively participating and contributing to secure these complex environments.

This Cybersecurity Magazine is a joint effort of several cybersecurity teams. We invite you to let us know which topics interest you. We will do our best to improve our next issues with your feedback, as well as to share with you always more valuable information.

Thank you for reading this magazine and looking forward to future cooperation.

Eyal Asila,

Head of Global Cybersecurity Consulting Group, Atos



IoT security with managed detection and response

IoT devices and technologies are being rapidly adopted in the consumer, enterprise and industrial worlds.

Their use cases are growing in number by the day, increasing their possibility of influencing our lives in the years to come. As with every technology, it should be no surprise that there are risks with IoT. However, the **level of concern is much higher in IoT as they have the power to cause physical destruction, harm lives and cause systemic failures.**

Today, **managed detection and response (MDR)** service, with its emphasis on large scale cyber data analytics and fast machine-driven containment, is playing an essential role in securing IoT infrastructure. MDR is the evolution of traditional managed security service with a focus on deep detection and rapid response.

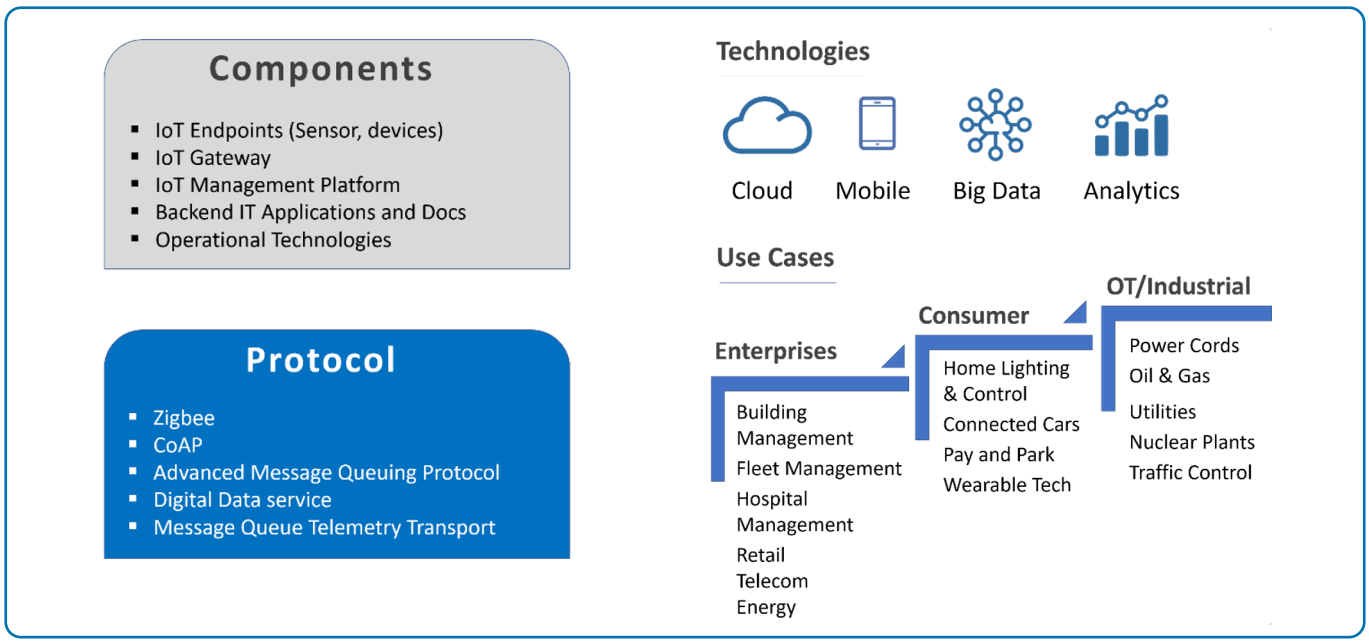
How MDR provides deep detection for IoT infrastructure

IoT technology stack has many new components, including IoT sensors, protocols, gateways, and management platforms. In addition to this, IoT infrastructure also uses traditional web applications and cloud technologies in backend services. **Detecting threats across these components have three challenges:**

1. IoT devices are deployed in thousands at distributed locations and these devices can not be monitored individually with security agents. That means we need to monitor traffic at gateways or network level, which involves large scale data analytics.

2. There are many IoT protocols in the market today including Zigbee, CoAP, Advanced Message Queuing Protocol (AMQP), Digital Data Service (DDS), and Message Queue Telemetry Transport (MQTT). These protocols are either new or derived for IoT from an earlier version used for general purposes. There are limited known rules or signatures to detect threats in these. Hence, we need more of abnormality detection, pattern recognition, outlier and anomaly detection technologies instead of a rule-based monitoring system.

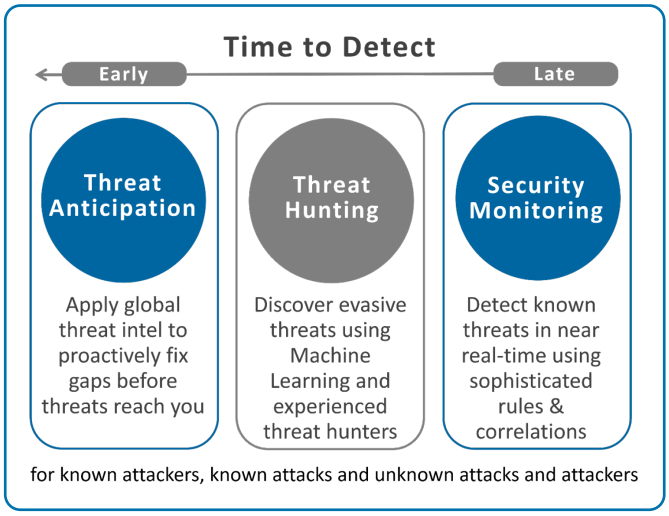
3. IoT management platforms, on the other hand, have web interfaces and are cloud deployed. They are exposed to common web application and cloud infra threats. So, we need a system which can perform detection across a hybrid environment, crossing over from IoT to web platforms.



A typical SIEM, which is mostly a rule-based system for limited protocols, will fail in such a scenario. Traditional security monitoring built around SIEM is no longer sufficient when it comes to IoT. They were good for compliance use cases and visibility into common attacks, but not against today's newer forms of attacks.

MDR technology, such as AIsaac from Atos, has capabilities to address these challenges. It's a big data platform on high-performance computing that provides power for large scale data analytics across diverse data set of IoT infrastructure. And it has built-in machine learning models to detect unknown threats- for those threats where rules cannot be written. The platform supports several native IoT protocols along with cloud and more traditional network protocols.

MDR service complements the AIsaac platform with expert analysts and threat hunters reviewing the data and alerts from the system. This helps in providing 24x7 in-depth coverage for your IoT infrastructure. Detecting potential threats at speed is only one part of cybersecurity. **How you handle these threats and respond to them determines whether they remain a minor incident or become a headline-grabbing breach.**



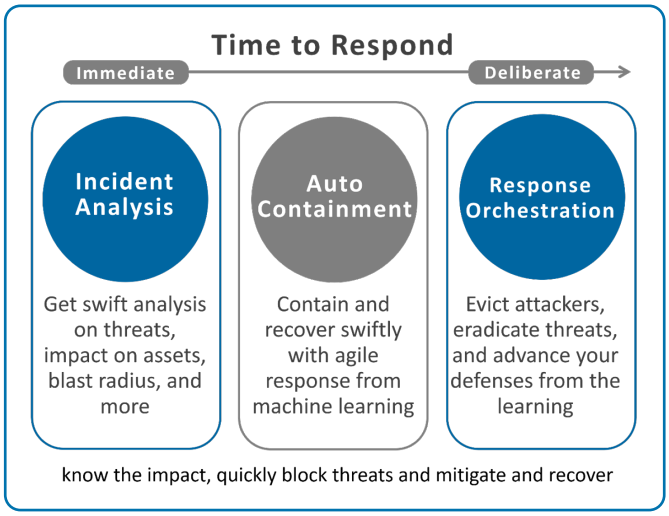
How MDR provides rapid response for IoT infrastructure

MDR platform such as AIsaac offers three critical capabilities for rapid response for your IoT setup:

1. Investigating the threats and quickly assessing the extent of impact: Modern attacks are rarely a one-off event, especially so in IoT where such threats are likely long-drawn-targeted-attacks. Traditional SOC services lack the speed to link past events and create a complete story on the attack campaign. MDR service can uncover the attack campaign quickly and assess the full impact as the platform provides analytics on historical events.

2. Contain threats at machine speed: MDR platform connects to various network elements, security products and gateways to quickly push rules for containment. These can include: quarantining a device, blocking a connection, reconfiguring system parameters, etc.

3. Reduce mitigation time from days to hours: Once the full impact is known, the next stages of incident management needs to be activated- namely eradication and recovery. Today these stages are extremely slow. MDR service brings speed to the incident management process by providing incident playbooks and automating the workflows for execution. Securing the IoT environment requires speed and scale for detection and response. MDR technology and services, combines high-performance computing, machine learning and cyber experts to provide valuable defense for IoT infrastructure.



Rajat Mohanty,
Paladion's CEO

Protecting the Internet of Things: what is at stake for network operators?

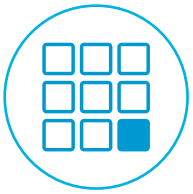
Today, most European tech buyers see IoT as either a tool for transformation or strategy that comes with security issues and concerns.

With this new technological landscape, we are barely beginning to understand the possible repercussions and the security challenges of these millions of connected devices. **End-to-end security is critical as a cyber-attack could bring to a stall a company's activities.**

In terms of security, network operators are the most exposed. When they deploy IoT networks, they need to consider various parameters that can affect data confidentiality. The entire architecture must be secured from the gateways to the user's platform. Network operators are also expected to deliver secure services to IoT business owners while optimizing operating costs. That is why the **biggest challenges to deploy secure, and scalable IoT networks** for their customers are to:

- **Secure the infrastructure** on which the IoT networks are based in compliance with the current standards (4G/5G/ LoRaWAN networks...),
- **Ensure data trust** by verifying the integrity of the payload,
- **Manage the trusted node's lifecycle.**

Poor awareness of security risk



Very large attack surface

Weak security devices

Heterogeneous communication protocols

Higher interconnection

The challenge

A few years ago, Atos had the opportunity to support a major French Telecom company in their security strategy. Under this umbrella, this company envisioned a platform that could allow them to respond to any security concern with a confident **end-to-end approach**. They were also looking for a partner and not only a solution: it was up to the former to analyze security requirements and to ensure that all IoT devices, networks and data would be secured for their customers, as well as maintain and manage security in a continually developing and mutating cybersecurity landscape while delivering insightful analytics.

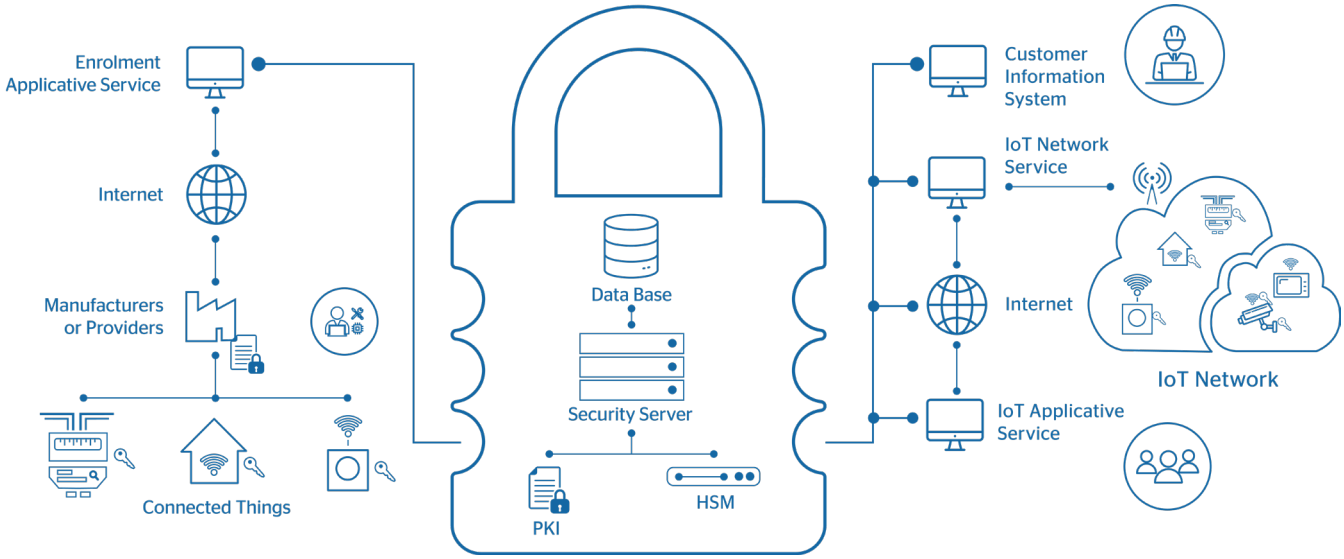
The solution

From initial discussions to implementation, the project took an overall twelve months. As a strategic partner for this new IoT business, we helped the client implement **LoRa technology**, a global standard for secure IoT architecture. Atos showed how the security platform spans the most extensive IoT ecosystems, as it can handle vast quantities of security data generated by millions of IoT devices working at the same time.

By also generating and managing real-time security keys, it eliminates the need for stored keys and, therefore, disarms this critical point of attack.

Atos solution is scalable and allows telecom companies to generate trusted identities for IoT devices as fast as they need to be added due to the use of Public Key Infrastructure (PKI). It is also worth highlighting the automated tooling for full lifecycle management. When so many IoT implementations utilize low-cost and often transient devices, such as shipment-specific sensors in logistics, it is essential that the security solution can **add, monitor and decommission devices** without human intervention.

Enabling security in such complex environments can be challenging. However, the client's data must stay secure. Offering the peace of mind by providing end-to-end security is now a critical asset to become a global IoT network operator.



Jean-Joseph Herpin,
Digital ID - Business & Solutions Manager

Securing the autonomous vehicle of tomorrow

February 17, 2040. My autonomous taxi drops me off at work.

Today, I have an important meeting with a client. I've had my cup of tea and I am heading to the meeting point to take my autonomous taxi. I get in this autonomous vehicle programmed to drop me off in the city center.

I am serene and have full confidence in this intelligent car. I know it will get me safely and faster to my destination using the most optimized route.

It is not only equipped with several sensors but during the course, it is constantly exchanging data with other vehicles and road infrastructure to keep me safe.
I will be reaching my destination soon.

While approaching an intersection, I see that all the traffic lights are green, but my autonomous taxi suddenly stops. The truck coming from the right also stops. What's going on? Why did the vehicles decide to stop? Is it a malfunction, a cyberattack? Luckily, faced with this abnormal situation, my autonomous taxi decided to halt, even though the light was green.

Misbehavior detection, a prerequisite for the deployment of autonomous vehicles

Today's vehicles are increasingly equipped with technologies that allow them to interact with their environment. These intelligent vehicles exchange information with each other and road infrastructure to improve road safety, traffic efficiency and users' comfort.

Communications between vehicles and with the road infrastructure must be secured for the data exchange to be reliable.

A security solution called **Public Key Infrastructure (PKI) already makes it possible to protect these communications by providing digital identities to each entity of the system.** Digital trust, guaranteed by the PKI, ensures the integrity and authenticity of data exchange through cryptographic mechanisms.

But it's not enough. As autonomous vehicles will make decisions based on the data exchange, this **data must be reliable.** Let's imagine that a hacker takes control of a traffic light and changes its color; he will be able to send false information over the network. An autonomous vehicle could also, in case of technical failure, send erroneous messages.

To enable misbehavior detection, a solution must be deployed within each vehicle and road infrastructure, and a central system must be set up.

The future autonomous taxi will be equipped to detect misbehavior. It will receive a message from the traffic light, and it will check it. With the help of its sensors and messages sent vehicles in the vicinity, like the truck, it will be able to detect inconsistency of the data received. It will then make the right decision and determine the suitable local reaction.

The autonomous taxi will send a report to the central entity. The process of misbehavior detection will also be triggered by the truck that similarly witnessed an abnormal situation. Cooperation between the actors of the system will play a key role.

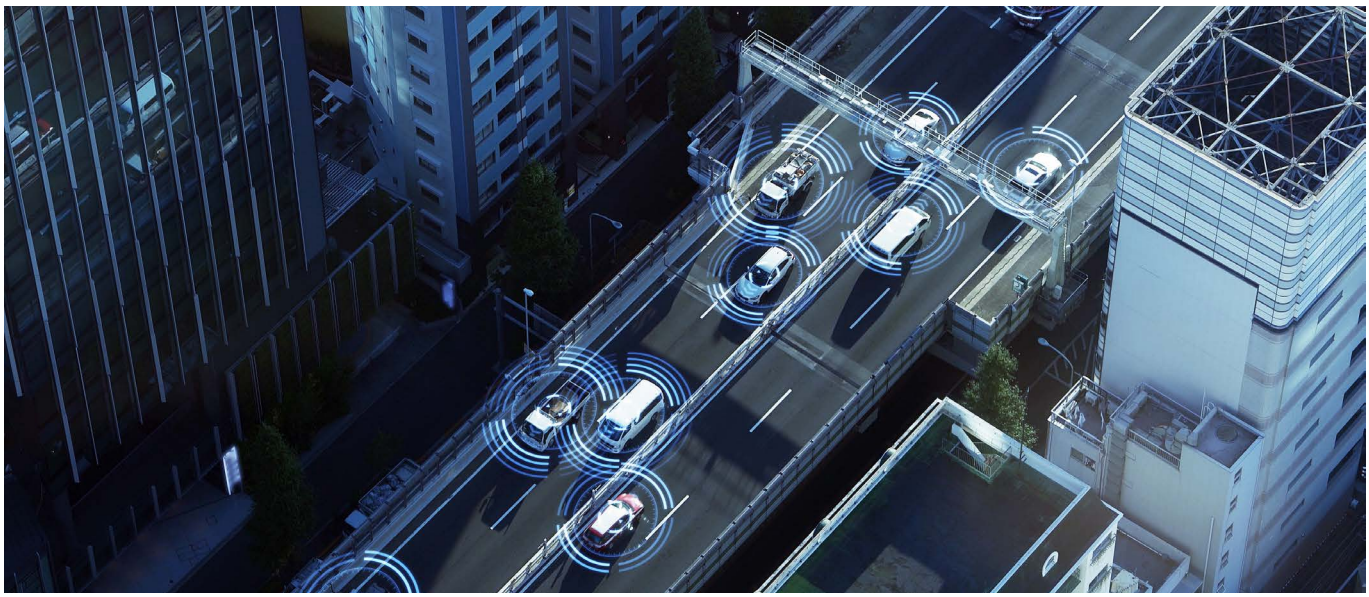
A central entity will be responsible to receive misbehavior reports and to investigate. Its purpose will be to determine whether the traffic light has been compromised or not. If so, a global reaction will be triggered. The possible responses can range from a simple notification to a control center (to request a maintenance intervention) to the exclusion of the entity from the trusted system. Messages sent by this entity would then no longer be considered by the others.

Artificial intelligence takes cybersecurity to the next level

The misbehavior detection solution will benefit from using artificial intelligence such as machine learning. The autonomous vehicle will have to process a large amount of data in a short period of time in order to detect an anomaly. The central system will have to gather a very large number of reports, extract suitable data that will allow to predict the type of misbehavior and establish the more appropriate reaction.

Artificial intelligence enhances digital trust and will be one of the sine qua non conditions for the deployment of autonomous vehicles on our roads.

Hafeda Bakhti,
Digital ID Innovation team leader



Why SOC for Automotive?

Cars have massively evolved in the past decades (centuries already!). Everything started with steam-based machines around the mid-1700s.

In the late 1800s, Karl Benz introduced a significant change in the car industry by building the first car powered by an internal-combustion engine. This triggered the mass production of cars, as everything ran faster right after that.

In 1922, Lancia Lambda was the first car to have a unitary body. In 1935, cars started to include the turn signal to indicate the driver's intentions to others: one of the first interactions with their direct environment. In 1948, a blind man named Ralph Teetor developed the first modern cruise control. In 1963, Porsche released the first 911 -nothing to do with this article, but it's always good to talk about the best car in history! Then, the car industry began focusing on building more and better cars from a mechanical perspective. **But today, we care about technology.**

Technology in cars started to appear in the 1960s with electric windows, anti-lock brakes in 1971, and digital dashboards in 1974. Nothing linked to cybersecurity yet. This realm started to become meaningful with the launch of the first "connected car" in 1996 when some models were able to call the emergency services in case of an accident. **Since then, cars have been aggressively adopting digital technologies aiming to improve the driving experience and maximize productivity.**

Today, a car has hundreds of sensors to capture data like multiple ECUs (engine control units) to control every function with automated responses based on data provided by the sensors. It also has 4G connectivity either for maintenance purposes (e.g. connect back to the car manufacturer, to the emergency services provider or the car fleet owner) and in-car entertainment (e.g. Wi-Fi or Bluetooth connectivity to connect to the car-info system, surf the internet or third-party apps); car digital services, and we keep counting.

Unfortunately, **such a rapid evolution comes at a cost. More specifically, a "security" cost.** We have seen too many times designers and developers underestimating the value of secure software development, providing car technologies with security bugs on top of the intrinsic security risk related to its functions.

From a cybersecurity services provider's perspective, we can effectively think of a car as one of our customers' branch offices. It has plenty of technology communicating from inside and outside the vehicle, moving valuable data around -either business information or information relevant for the car control and safety- among different technical components as well as human beings. At this point, **we can already realize the vast security threat landscape impacting connected cars today. They inherit all the threats from an enterprise IT environment plus all the ones related to a moving vehicle. The most important one being the impact on humans safety which one of the worst associated risks.** We have already seen multiple well-publicized security breaches (e.g. Tesla S, Chrysler Jeep, Nissan Leaf,). As autonomous driving systems increase in number, we expect these attacks to rise in the coming years.

At Atos, we have developed security solutions and services to protect the connected car ecosystem. Some of them include:

- Connected vehicle platform (Worldline's platform for secure communications and fleet services assurance),
- IDnomic secure elements (implemented into existing ECUs to encrypt V2X messages)
- IDnomic C-ITS PKI (IDnomic's Cooperative Intelligent Transport Systems solution providing Public key infrastructure (PKI) technology to secure V2X (vehicle-to-everything) communications).

We also collaborate with an ecosystem of vendors providing specialized security controls either for in-vehicle security, network assurance or back-end protection.

But there is yet a critical component that deserves further development and is getting attention from car manufacturers and fleet operators from a security perspective: a security operations center (SOC) for automotive. A service providing full visibility, detection and response to threats that target their connected cars and associated services. So here we are, running proof of value (PoV) with top vendors like Argus, Upstream, or Cybellum and looking forward to extending our Prescriptive SOC concept into the Connected Cars world.

Despite the COVID-19 situation, the globally connected car market size is expected to reach USD 53.9 billion in 2020 and is projected to reach USD 166.0 billion by 2025, at a CAGR of 25.2% from 2020 to 2025 .... Worth to invest in securing it 😉

Marc Llanes Badia,

Cybersecurity Global Business Development, Atos Senior Expert and member of the Scientific Community.


As autonomous driving systems increase in number, we expect attacks to rise in the coming years

Cybersecurity for Industrial Control Systems

Operational Technology (OT) -also known as industrial control systems (ICS) and supervisory control and data acquisition (SCADA)- **is pivotal** as it allows us to live the 21st-century life we are used to.

The ability to have everything we need (and want) relies on a vast network of industrial facilities, some of them as big as a city and others, as small as a network cabinet. This means that we are surrounded by a world of possibilities and capabilities as vast as we can imagine.

Our society depends on OT for the reliable and stable delivery of essential services, such as energy, water and transportation, as well as other crucial requirements. Therefore, **security becomes essential when talking about the OT realm, especially when there is a possibility of a harmful impact spreading in a very short timeframe.** For a long time, cybersecurity in these environments was not adequately addressed by the manufacturing site management nor by the cybersecurity industry. Today, even after the exponential growth of cyber-attacks, security solutions have not been developed fast.

There is still a big gap that needs to be addressed when it comes to securing such a challenging environment, creating a unique opportunity that requires innovation and familiarity with the OT domain.

Threats, vulnerabilities, and risks

OT environments are by nature exposed to risks and threats as we see more and more industrial organizations emerging from Industry 3.0 to Industry 4.0.

In recent years we have seen an exponential increase of attack on OT, including Stuxnet, Dark Energy, and many others. **The attack agents are abusing the existent vulnerabilities and the lack of know-how and understanding** of what makes this environment so unique. This is also a **primary challenge.**

First, it is important to mention that vulnerabilities unique to ICS are poorly understood, especially when we compare it to the extensive amount of research around IT vulnerabilities. They can be found in the context of:

- management (lack of enterprise risk management (ERM) practices, exercises and/or documentation, RACI matrix, or management engagement),
- operations (lack of network segregation between IT and ICS networks, weak remote access procedures, incident detection, response, and reporting procedure, among others),
- technique (in hardware, software or networks).

Second, we need to understand that OT environments rely on 2 main paradigms: **'Safety comes first' and 'If it is working, do not touch it'**. Therefore, we are talking of environments with (and not only) unpatched systems, obsolete OS, lack of visibility and many other challenges, creating a unique domain to work with.

For most professional operating in this field, many of the tasks rapidly become heavy tasks. These are the primary challenges:

- Lack of professional workforce who understands both OT & IT,
- Lack of communication between OT & IT staff in general and due to the language differences,
- Maturity of security controls,
- Risk avoidance closure which is inherent within the environment.

At Atos, we are aware that to implement cybersecurity controls and measures within this domain, we need to first, **understand the unique nature of the environment**, its vulnerabilities and the possible associated risks. By combining our knowledge with our products and services, we can help our customers to secure their valuable assets and their systems.

The implementation of an industrial security program must provide a **balanced and objective evaluation of risks** in terms of threats and vulnerabilities and its consequences while aligning with the industrial short- and long-term objectives. By working together with our customers, we can help build a more secure and safer industrial environment while enhancing their productivity and operations.

Maria Jose Carvajal,
Consultant Global Cybersecurity Consulting Group

OT assessment in time of crisis: how to proceed?

The pandemic has significantly impacted cybersecurity priorities and budgets. Companies, and especially chief information security officers (CISOs), had to rethink remote working models and their digital security implications.

The pandemic did not stop hackers. Quite the contrary: during the pandemic, the FBI received 400% more cybersecurity complaints daily than before .

During this time, essential operators like manufacturers, hospitals and energy providers had to maintain business continuity as the world depended on them more than ever. **But how to do that when cyber threats strongly targeted their supply chains?**

OT security importance in energy

We recently carried out an operational technology (OT) risk assessment for a leading electricity provider.

Electricity providers need to ensure that their OT equipment (industrial control systems (ICS), programmable logical controllers (PLC), supervisory control and data acquisition (SCADA)...) i**s not be disrupted after a cyberattack**. The client operates along the entire value chain, from power generation and trading to sales. A shutdown of even one day could result in significant damages and costs. Its initial request was then to carry out an all-round analysis of its OT environment:

- OT information security maturity assessment (ISMS) according to relevant standard or framework,
- OT technical security risk assessment,
- OT assets risk overview,
- The physical security of the OT environment

extensive amount of research around IT vulnerabilities.

Cybersecurity consulting in times of crisis

Throughout my career of working with the global cybersecurity consulting team, having spent more than 20 years in information technology and more than 8 years in information security, this was the first time we faced such a unique situation. We had to deliver a report, including analyses and summary of the prioritized measures that should be implemented to increase their maturity posture. **The project was launched in January this year, but soon we were faced with the COVID-19 pandemic challenges**.

Specialized in governance, risk and compliance, I am used to aligning with our customers business strategy on face-to-face meetings. Yet, the COVID-19 obliged us to cancel onsite venues. The documentation was also limited to some extent, as data policies regarding document sharing had been strengthened.

Addressing an OT assessment in times of a pandemic made us rapidly change our strategy, find new ways to resolve the issues, such as data retrieval, and use every possible tool and virtual appliances in our disposition to overcome the challenges.

Project Summary

The project phases and deliverables were the following:

Phase I (2 months)

- Develop a phase-wise RACI matrix based on the project and detailing all processes, activities and deliverables and mapping them according to the roles on the project.
- Scope statement detailing all stakeholders, assumptions, risks, project objectives, requirements, scope, approach, client's obligations, expected deliverables, timelines and milestones.
- Initial discovery questionnaire interviews with all relevant stakeholders to capture first high-level overview of the risk posture.
- Engagement project planning to provide details on each of the phases' different activities, timeframes, tools used and expected outputs.

Phase II (4 months)

- OT network review, retrieving all the required data from their networks and gathering all relevant inputs.
- OT assets inventory and vulnerabilities AS-IS report using one of our partner's OT asset discovery.
- C2M2 interviews to assess their level of maturity and provide future recommendations and improvements.

Phase III (2 months)

- Information security roadmap with short-term and long-term recommendations.
- Executive presentation report to relevant stakeholders.

Historically, OT systems were separate from IT. Now that they are expanding to an extended ecosystem, OT security becomes a priority. We achieved good visibility about the client's assets and could precisely identify anomalies. **This assessment led to greater transparency for the client. Now it can take the right security measures with every parameter in mind to ensure business continuity.**

Nemanja Krivokapic,
Principal Consultant Global Cybersecurity Consulting Group

Atos OT training initiatives: leading the path for knowledge

In the last few years, operation technology (OT) security has become a hot topic in the boardroom.

Due to the complexity of the subject and the continually evolving threats, we have launched different initiatives to expand the stakeholders' knowledge of OT.
As part of our commitment to the Atos community, we seek to maintain an open dialogue and create useful content that can help all of us to expand our knowledge on key topics.

ISACA OT security conference

In September 2020, we presented a virtual conference to ISACA, a global professional association focused on IT governance, on how to integrate OT into cyber threat detection and response. Tom McDonald, Paladion Vice President, US enterprise engagements, and Eyal Asila, Atos Head of global cybersecurity consulting, shared several OT security case studies and gave insights on the best practices to secure OT environments in real-time to all ISACA members.

Key insights from this security conference were especially around the importance of maturity risk assessments in OT, threat detection and response, and the threat landscape. Understanding the current situation of industrial environments and identifying, people, processes, and technologies deployed is the first step that needs to be taken. Through interviews, workshops, IT/OT asset discovery, and vulnerability network scanning, you retrieve the required data to deliver a comprehensive security roadmap.

These sessions are a huge opportunity to raise awareness of the threats targeting OT and the consequences for a company. By emphasizing the importance of implementing security in an OT environment, we hope to help industries better face their unique cybersecurity challenges and reach "cyber maturity".

Atos internal OT learning initiatives

As part of our internal learning initiatives, we also provide 4-weeks training on industrial control systems (ICS) and OT webinars to all Atos employees who would like to familiarize more with this environment and its security. These sessions were aimed at beginners within cybersecurity in the OT.

As cybersecurity leaders, it is our responsibility to ensure that the knowledge we have is shared and acquired by our peers and partners. Our teams are trained to understand the industrial environment better to address these 3 important questions:

- Which threats should be addressed?
- Which security measures should be deployed?
- Where to implement them?

The purpose of each learning initiative is to deliver a maximum of relevant information in the shortest possible time.

At Atos, we believe that to achieve a smooth digital transformation, it is critical to offer sustainable security models to our clients to secure their most valuable assets and environments and that this goal can be reached through training and awareness. Our duties are clear; **now we need to join forces and bring others for acting as a counterweight to the attackers**.

Anna Cantin,
Associate Cybersecurity Consulting Group


“It is our responsibility to ensure that the knowledge we have is shared and acquired by our peers and partners.”

True IT/OT/IoT Convergence Through "Middleware"

In 1998 a group of scientists, engineers and hackers from "L0pht Heavy Industries", a hacker collective based out of Boston, Massachusetts, testified before the U.S. Senate Committee on Governmental Affairs attempting to create public computer security awareness and claimed they could "shut down the whole internet."

Topics included vulnerabilities in computing systems, partnerships with software and hardware companies actively mitigating vulnerabilities, exposing companies deliberately hiding vulnerabilities, and creating awareness of the risk and grave consequences of potential attacks.

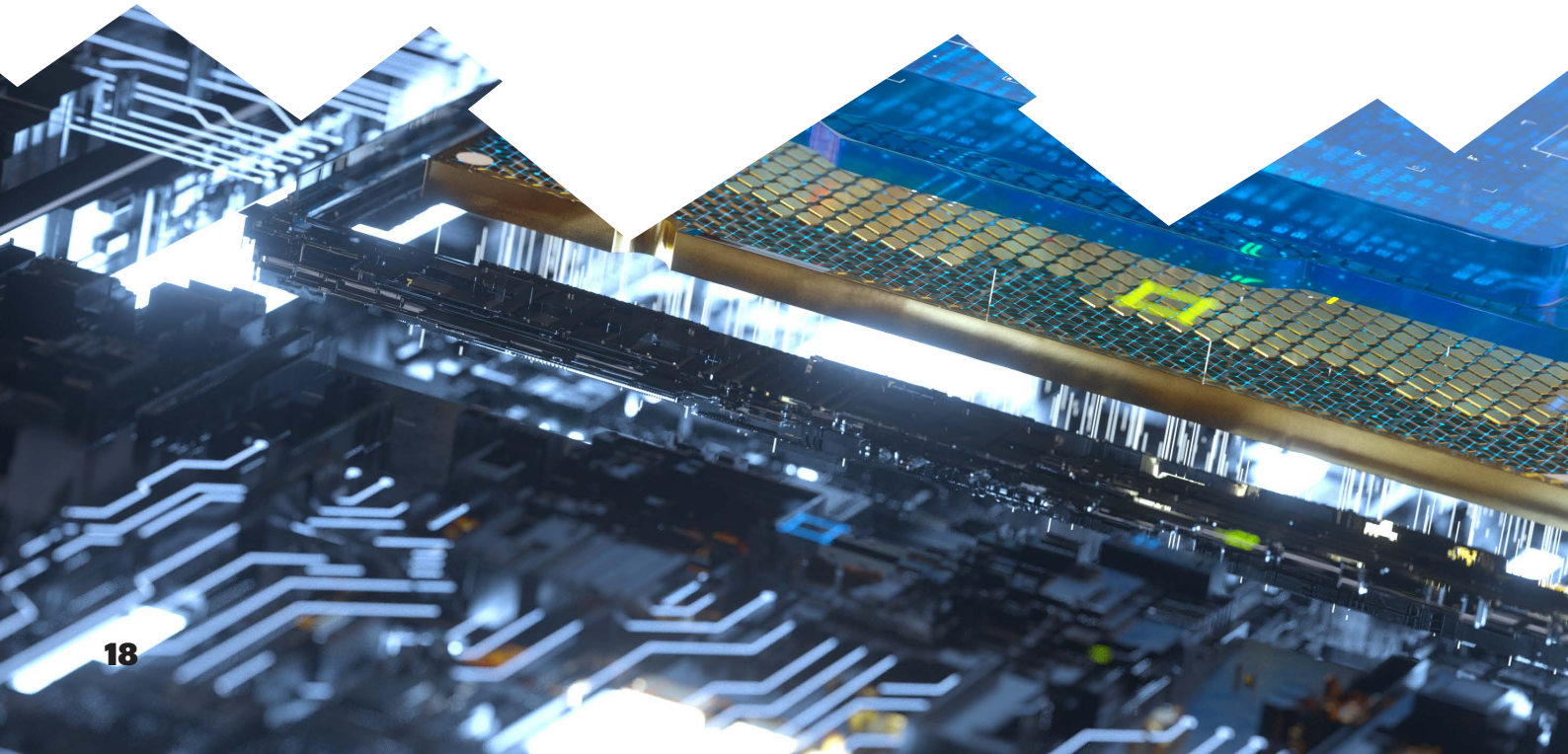
A particularly interesting topic was one spoken of by **Stefan Von Neumann**, an engineer and self-described "user support specialist" who discussed critical infrastructure including energy, water and telecommunications. He outlined the unsecured remote command and control of these essential systems and in almost all cases, the lack of awareness by end clients of the potential to have their critical services compromised, manipulated, denied service, and even have private information spied upon or stolen.

Mr. Von Neumann closed by saying he, "...would personally like to see that the same type of independent review process that should exist for software companies extended to utility companies and internet service providers."

Getting to the root of the OT security issue

Our public awareness of the threat to critical infrastructure systems and the dire consequences that come with an attack or even a mistake has been almost 25 years in the making. So why is the standardization and availability of security technologies for Operational Technology (OT) and Internet of Things (IoT) devices so far behind traditional Information Technology (IT)? Mr. Von Neumann described what the solution was: a standardized framework and review process of security controls in utilities and telecommunications; however, he did not directly identify the root cause of the issue. These security controls and procedures didn't exist and are largely struggling to be equitable to IT even today because **OT/IoT technologies are deployed, operated and maintained by a separate and diverse cadre of personnel with their own "culture" and technical skill sets**.

These OT/IoT specialists have enjoyed luxuries that traditional IT once had in security: segregated networks, physical/wired only transmission, autonomous operation from other business functions, and security through obscurity.



These luxuries have faded away as the threat landscape has grown with the consolidation of employees and facilities, wireless technologies, ready access to information about vulnerabilities, and benefits of system exploitation.

Bridging the gaps

Active and devastating attacks on critical infrastructure, supply chains, and telecommunications have been carried out by nation-states, malicious groups and individuals which has brought organizational management attention to vulnerabilities and threats lurking in their infrastructure. In a hasty attempt to bandage these vulnerabilities, OT/IoT has been flung into the fires of traditional IT management and security operations and therefore has inherited the complications that come with them. I recognize the need for this consolidation of visibility into security incidents and response, however, there is an additional and unaddressed requirement for "**middleware**" in technology, process and people to create **true IT/OT/IoT convergence**.

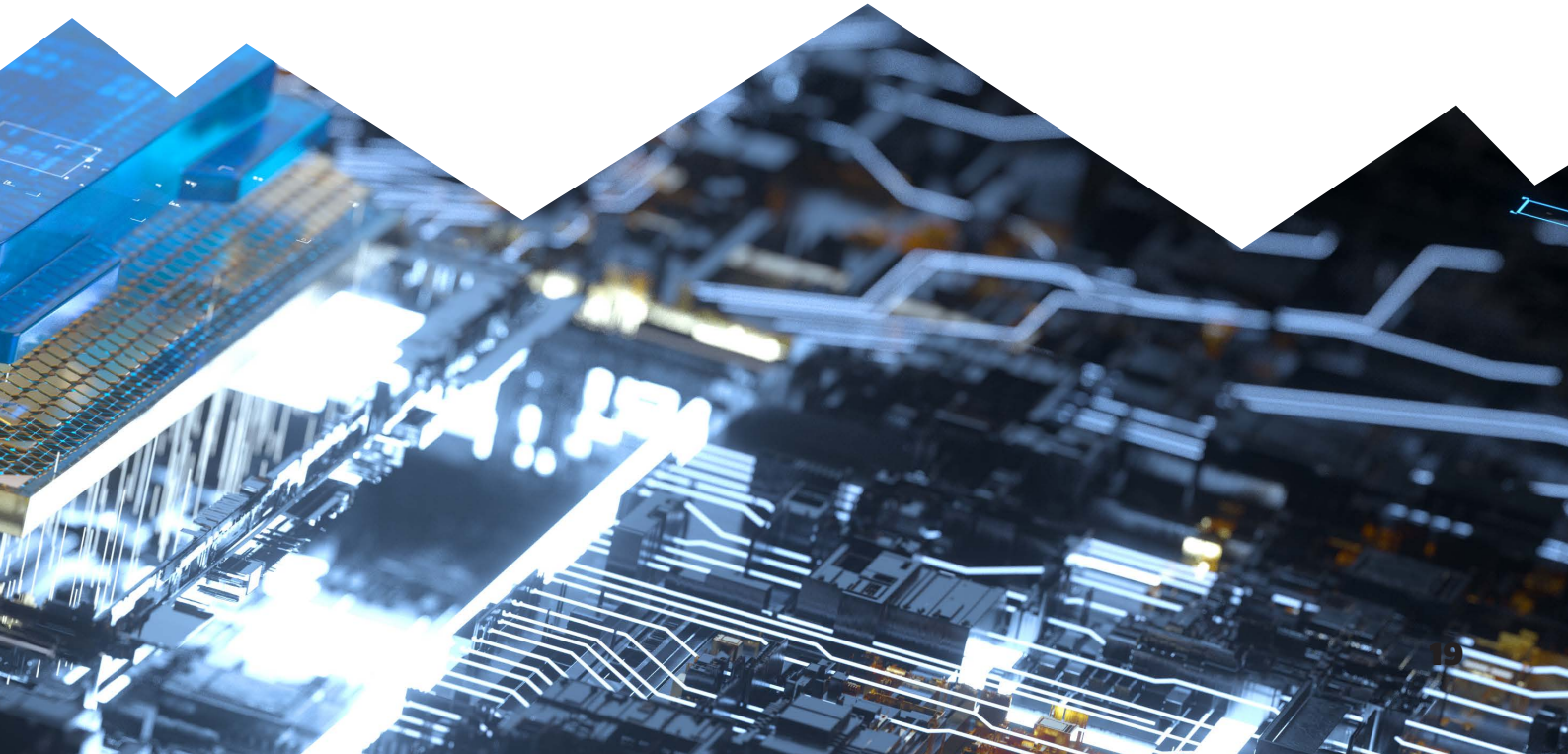
At Atos, I am working with our OT/IoT teams around the globe to bring true, blended security operations management to complex and multifunctional enterprises. Our PSOC for OT/IoT offering focuses on a single point of contact to protect critical infrastructure and supply chains by aligning IT, OT, and IoT security activities to provide near real-time security intelligence and incident response. The Atos Resource and Services group and I are attempting to conceptually prove out our IDnomic for Objects offering as a solution for managing authorization and authentication through certificates issued to safety and preventative maintenance monitoring systems, securing against the unauthorized attack and providing security incident intelligence.

I am focusing my efforts on identifying the gaps between technologies, process, and people and how to bridge these gaps with this missing "middleware" while being inclusive of a range of skill sets, work cultures, and requirements.

As OT and IoT interconnect our lives with critical infrastructure and is technologically intertwined with our activities, business, homes and transportation, **we have a responsibility to ensure privacy and security are carried over to these emerging technologies and respond to the widening threat landscape**. My goal is to develop a secure global infrastructure that includes all technologies. IT security management and organizational management need to embrace the reality of IT/OT/IoT convergence with agility and speed to protect our most valuable and powerful command and control assets. You can join the conversation with Atos and professional security organizations, research something new, train others on OT/IoT technologies, and create tailored awareness around threats, vulnerabilities and potential solutions for IT/OT/IoT Convergence. **Together we can build genuinely secure IT/OT/IoT convergence through the first steps of awareness and evangelism**.

References: IOpht testifies before U.S. Congress

Vieri Tenuta,
Global Cybersecurity Offering Manager



Atos single pane of glass for OT, IoT & IT Security

Atos designs, delivers and manages holistic cybersecurity products and services for our client's environments that have Internet of things (IoT) devices and operational technology (OT) deployed. Our cybersecurity offerings include Atos's IoT security suite, OT security suite, PSOC for OT/IoT (prescriptive security operations center) and Atos cybersecurity professional services.

We provide our clients with three fundamental building blocks for a successful single pane of glass security:

You cannot protect what you cannot see: Visibility is critical. Organizations must have an efficient asset inventory and asset classification.

Guarantee alignment with security policy: Granular compliance management helps to enforce security policies and adapt them to industrial and IoT environments.

Detect and mitigate industrial threats in real-time: Monitoring IT and OT environments helps to bring threat detection for industrial companies and critical infrastructure to the next level. By combining information from different sources, a coordinated attack can be swiftly detected, and the proper countermeasures deployed.

Atos cybersecurity consulting services for IoT/OT augment our client's staff with professional consultants in risk assessment, IoT/OT red teaming and penetration testing, organizational risk and security assessment, vulnerability assessment, security architecture development and deployment, and managed security services.

The **Atos IoT security suite provides** our clients with identity lifecycle management to provision and manage devices and their digital identities. This embedded security protects devices and sensors without compromising performance while maintaining the lightweight design and functionality of IoT devices. **The native suite integrations with IoT platforms, such as MindSphere, enable secure communications and authenticated access for management and operations of IoT.**

The **Atos OT security suite manages security functions in highly complex networks, keeping security at the forefront of your environment while maintaining critical availability of your systems**. Manage your network segmentation authentication authorization for devices to ensure secure and authorized access to your IT/OT converged environments while retaining visibility into the deployment, management and security of OT devices.

- **Atos IDnomic for Objects** is a fully-featured certificate authority and registration authority for management of enterprise IT/IoT/OT public key infrastructure, capable of integration with various standards including IoT and OT lightweight communications protocols to deliver secure certificates to all. IDnomic for Objects interfaces with various IoT/OT management platforms and gives options for on-premises or cloud-based management solutions.
- **Atos IDnomic for Transactions** enables secure messaging, blockchain ledger for secure transactions, and digital signatures to manage secure communications for IoT and OT networks and transactions.
- **Atos Trustway HSM for IoT** is a high transaction-per-second, FIPS 140-2 certified hardware encryption module capable of delivering on-demand, reliable encryption functions to IoT/OT environments including tokenization, message encryption and validation, certificate issuance and key storage.
- **Atos Trustway Proteccio HSM** delivers cryptographic functions for multiple uses while maintaining network segregation and compartmentalization of encryption functions within a physical hardware security module appliance, reducing your security management costs and infrastructure footprint.

Atos PSOC for IoT/OT manages eye-on-glass security operations for IT and OT converged environments and facilitates rapid deployment of security, while connecting securely through your IT infrastructure. Couple these managed security services with inventory and asset management and configuration management for deployed OT, and enjoy an end-to-end, secure management solution for your IT/IoT/OT environments. Atos's first European IoT CERT specialized in IoT Security (following the acquisition of Digital.security) offers in-depth visibility on the IoT threat landscape and advanced IoT vulnerability-lab to assess the security of smart devices.

The Atos IoT/OT cybersecurity product and services enable our clients to assess, deploy and manage highly-available, secure operations no matter what their organization's security maturity is.

> The Atos IoT/OT cybersecurity product and services enable our clients to assess, deploy and manage highly-available, secure operations no matter what their organization's security maturity is.

Acknowledgements

We would like to thank the following authors for their contribution.

Eyal Asila

Head of Global Cybersecurity Consulting Group

Atos

An information security leader with over 22 years of experience, Eyal Asila leads global cybersecurity consulting at Atos. He specializes in OT, HPC, AI and special cybersecurity fields. With this expertise, he has established global information security arrays and has developed unified and standardized technological security systems in several projects. With experience managing complex projects in dynamic, results-driven business environments, Eyal works with management and boards of directors daily and in times of crisis to provide strategic cybersecurity consulting to global enterprises.

Rajat Mohanty

CEO Paladion

Atos

Rajat Mohanty, is the co-founder, chairman of the board of directors and chief executive officer of Paladion Networks. He has been Paladion's chairman & CEO since the inception of the company in July 2000, and was a key member for the joint of forces with Atos. Mr. Mohanty is a regular and sought-after speaker at Indian Institute of Management, Bangalore for start-up companies as a mentor and coach. He is one of the top 10 chief executives who steer the CISO conferences and Security summits in India and Asia. He is one of top business leaders who steer the Industry and University Partnership doing pioneering work in Cybersecurity education with MS Ramaiah University in Bangalore.

Jean-Joseph Herpin

Business & solution manager for Digital ID

Atos

Jean-Joseph Herpin is the business & solution manager for the Digital ID entity of Atos cybersecurity products. Expert of PKI, CMS and digital signature products, he is supporting sales teams at a global level. He has also overseen the development of new IoT security offerings for the telecom and utilities sectors, working closely with the R&D teams to adapt them to the specificities of each market. As perseverant as he is when running marathons, Jean-Joseph takes to heart his mission to support clients in their digital transformation journey.

Hafeda Bakhti

Digital ID Innovation Team Leader, IDnomic

Atos

Hafeda is currently performing the role of innovation team leader at Atos IDnomic, with seven years of experience as an R&D engineer in Paris, France. She mainly works on ITS projects and participates in ITS research projects in partnership with IRT SystemX (French Research Institute). She also was involved in ITS deployment projects such as the national French pilot deployment SCOOP@F, InterCor, and C-Roads. She has managed the deployment of the Atos IDnomic ITS PKI solution in SaaS environment and led the product development following European regulations (C-ITS platform), ETSI standards, or specific functionalities.

Marc Llanes

Global Cybersecurity Business Development Director

Atos

Marc is leading the Cyber Security Global Business Development team at Atos. His base profile is Senior IT and Information Security Consultant with extensive experience in most areas of the business, in international multicultural environments, from architecture or strategy definition, up to systems integration or operations management. He is a member of the Atos Scientific Community and as such he is actively involved in all aspects of Innovation and thought leadership to foresee upcoming technology disruptions and future business challenges. He is also appointed an Atos Senior Expert in Cyber Security, leading the IoT Security domain.

Maria Jose Carvajal

Associate Cybersecurity Consulting Group

Atos

Maria Jose is an Associate Consultant at Atos. Her focus is providing cybersecurity solutions and strengthening Atos's client's security posture across various enterprises from several countries around the world. She has participated in shaping the strategy, design, and implementation of a variety of cybersecurity programs, helping companies secure their ecosystem and build cyber capabilities that go beyond compliance to enable business transformation and innovation. She also has taken a leading role in the Cybersecurity Magazine, coordinating all efforts to bring this magazine to life.

Nemanja Krivokapic

Principal Cybersecurity Consulting Group

Atos

Nemanja is a CyS Global Principal Consultant, experienced Cybersecurity Practitioner with 20 years of professional experience, committed, proactive and creative mind in an Ever-changing cybersecurity landscape. His focuses are InfoSec Governance and Strategy, GRC, Management Consulting, and Project transformation programs. He has successfully managed several engagements and he is one of the key contributors to the overall Global practice initiatives. He is PMP, CISM & Data protection certified and he is currently finalizing a master's in information security.

Anna Cantin

Associate Consultant

Atos

Anna is an associate consultant at Atos. Her focus is on helping implement strategies, communication and processes in a global and growing team, using her creativity and commitment. In an ever changing environment, she helps adapting the consulting needs to the new challenges. She has also participated in several innovative cybersecurity projects focusing on HPC and OT, strengthening the security of Atos's clients and participating on their business transformation.

Vieri Tenuta

Global Cybersecurity Offerings Manager - IT/OT Convergence & IoT

Atos

Vieri Tenuta is an experienced cybersecurity expert, technology strategist, and systems engineer. As a Global Off erings Manager with Atos, his focus is on developing holistic and secure IoT and OT systems off erings that utilize Atos Cybersecurity products and partnerships on an international scale. In addition to his job functions, Vieri works with school districts and youth organizations to provide STEAM educational opportunities through student advocacy, volunteerism and community building.

Chris Moret

Senior Vice-President Cybersecurity Services

Atos

Christophe Moret, engineer from Ecole Polytechnique and Supélec, has joined the Atos Group in 2013, after 17 years in Hewlett-Packard, where he was leading the security outsourcing business for EMEA. After being in charge of security for Atos Global Managed Services, where he has created a global offering for security management, and implemented a network of Security Operation Centers around the globe, Christophe joined the newly created Atos Big Data & Security service line, as leader for the cybersecurity Global Business Line, in charge of all cybersecurity products and services business inherited from Bull and Atos service lines. Before joining HP then Atos, Christophe started his career in Bull, kick starting the Unix Business, then joined GIPSI and finally Chorus Systems, and has been teaching at Ecole Polytechnique.

Closing words

The Covid-19 pandemic will, no doubt, result in intensified attacks on industrial infrastructure as the new way of working increased remote connections to OT environments, making the air gap a thing of the past in this #NewNormal.

Therefore, organizations must select security partners who can measure their security posture across all critical environments. A security partner, like Atos, which can protect their environments worldwide bringing a single pane of glass to their security operations. A security partner, like Atos, who has been committed for decades to protecting clients. A security partner, like Atos, who is agile enough to adapt and innovate their security services to integrate new technological trends at the core of their operations.

Chris Moret,

Senior Vice-President Cybersecurity Services

Editorial board

If you wish to send feedback, please tweet using **#AtosCybersecurityMag** or contact us: https://atos.net/en/contact-us-cybersecurity

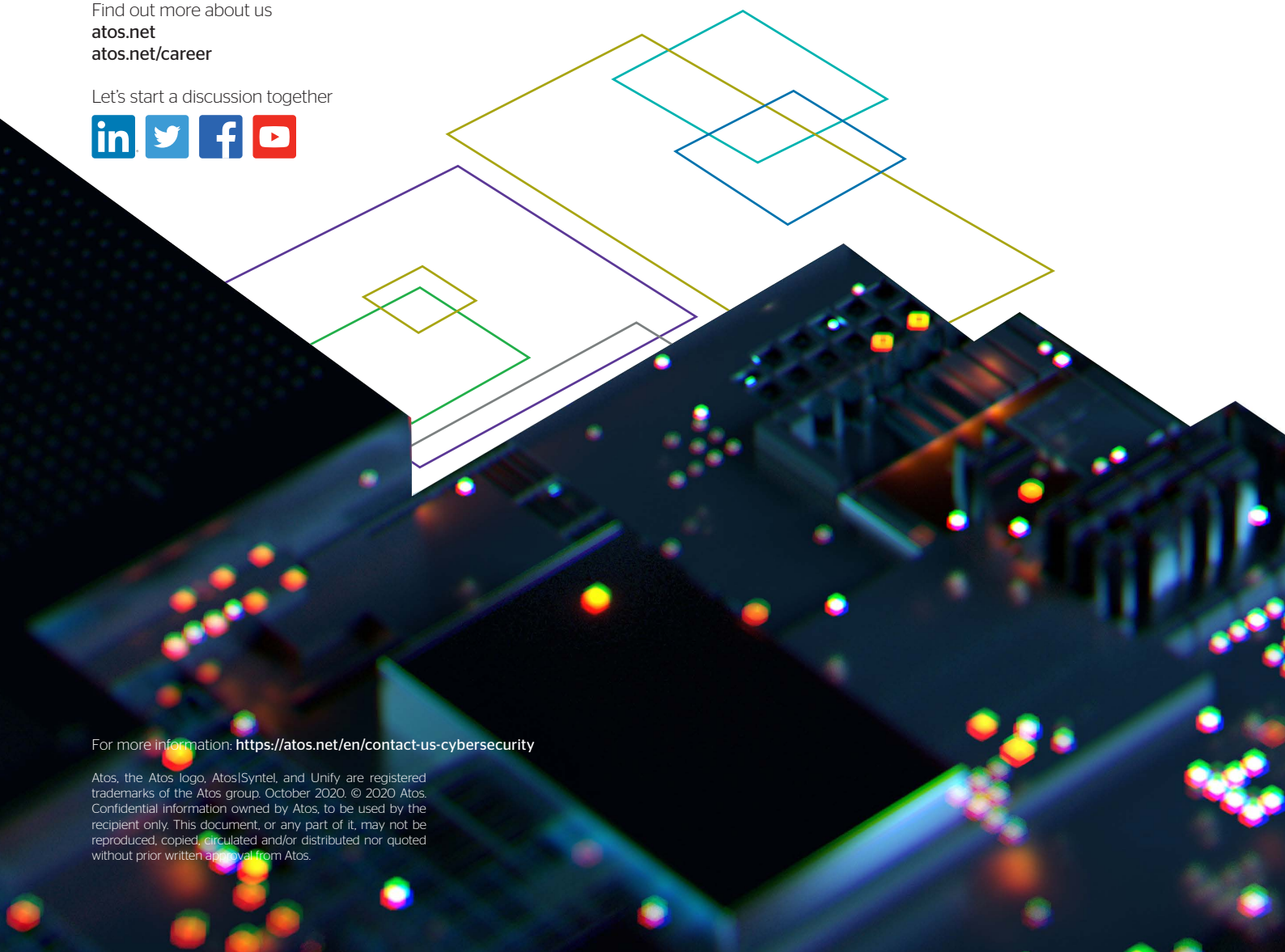
About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together



For more information: **https://atos.net/en/contact-us-cybersecurity**