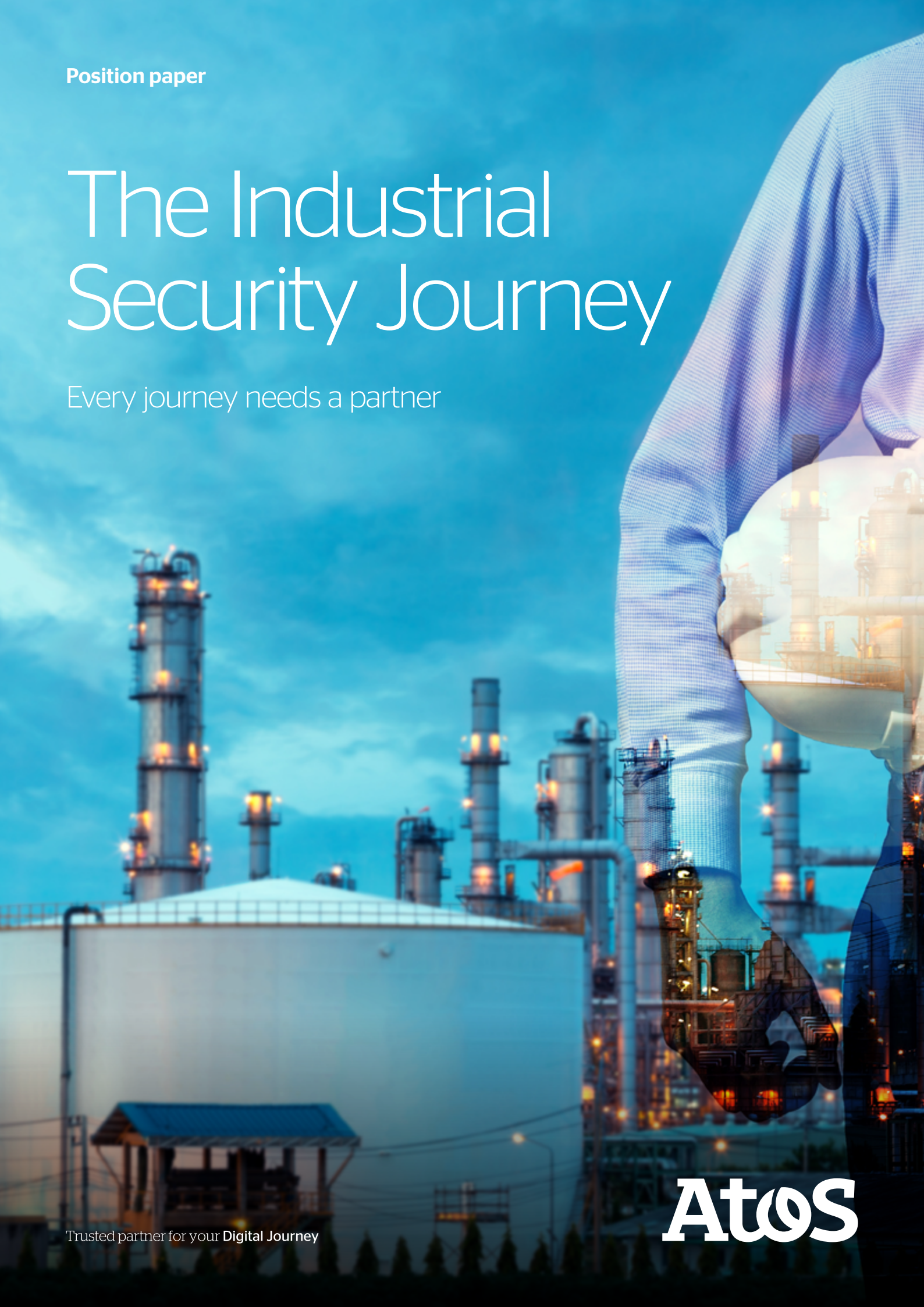
Position paper

The Industrial Security Journey

Every journey needs a partner



Trusted partner for your **Digital Journey**

Atos

To secure environments that are not inherently secured is not always easy and does not start by just adding security controls. It is about prioritizing the most critical processes, systems and potential sources of attacks or vulnerabilities. Security is about identifying, managing and setting up a strategy.

Industry 4.0: new challenges on the path of a smooth digital journey

Industry 4.0 creates value from connected assets throughout the product lifecycle, manufacturing and supply chain. These networks of devices connected to systems monitor, collect, exchange and analyze data to enable industrial companies to make smarter business. The result is operational efficiency, worker safety and environmental sustainability.

Interaction between machines, products, people and processes represent change at every level.

The Internet of Things is not the only technology driver of change in Industry 4.0 - Artificial Intelligence, Robotic Process Automation and Big Data analytics are all expected to contribute towards significant industry change. With Industry 4.0 and the Internet of Things, new business models appear, operational models need to adapt, and the services need to be reinvented.

Gartner predicts that **by 2020, more than 25% of identified attacks in enterprises will involve the IoT.**

If businesses want to ensure that they benefit from Industry 4.0 they must be prepared to overcome some specific challenges:

Security issues

that will arise as more and more devices are connected. Every new connection point is another potential vulnerability, so organizations must ensure that their security systems are suitable while moving towards the Internet of Things.

New connectivity between people, processes and things

organizations can radically improve efficiency and the quality of service. It also becomes key to business innovation and service development. Having technology work together leads to better business outcomes and potential marketplace innovations.

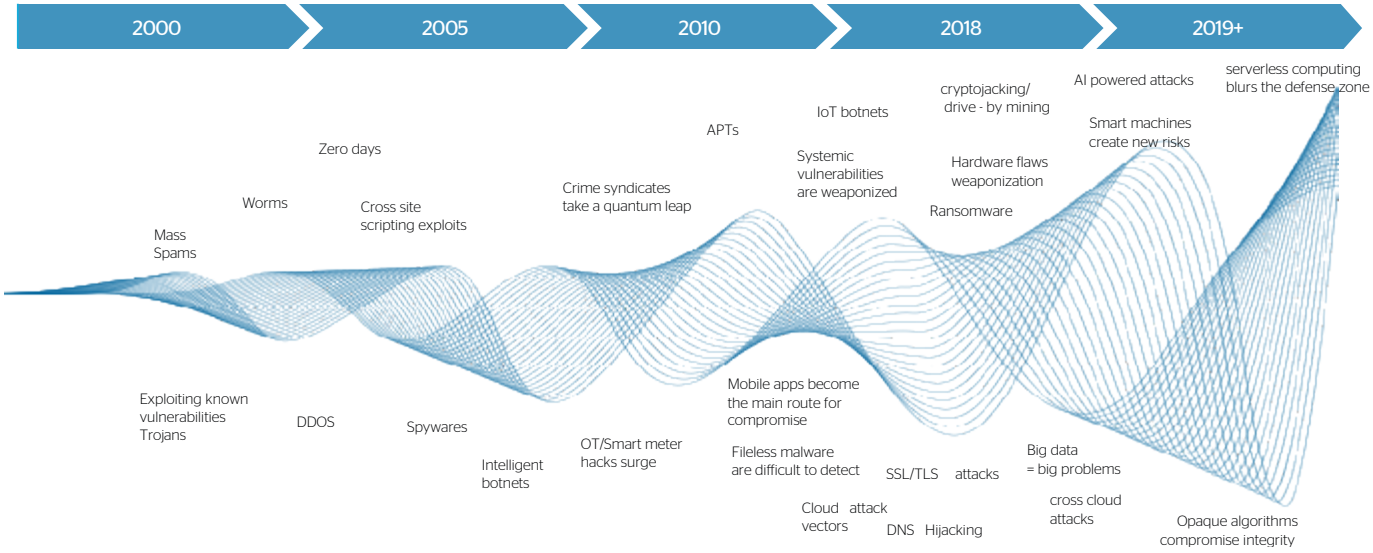
Necessary skills

businesses will need to ensure that their staff have and maintain the necessary skills required to cope with new technologies and evolving ways of working. Without the right development and training, IoT efforts can be tough to implement.

Gartner's latest forecast predicts that **the number of connected things in use will go up to 25 billion by 2021, from 14.2 billion in 2019.**

Better visualize today's cyber threats to prepare your Industry 4.0 cybersecurity strategy

The threat landscape is evolving and getting more complex, while the attack surface is growing with the appearance of new technologies. 2017 was the year of Ransomware, 2018 the year of Cryptojacking and 2019 will be the year of file-less cross platforms attacks. Companies need to adapt their strategies and change their mindset.



Type of attacks

Man-in-the-middle

An attacker breaches, interrupts or spoofs communications between two systems. In an IIoT scenario, an attacker could assume control of a smart actuator and knock an industrial robot out of its designated lane and speed limit – potentially damaging an assembly line or injuring operators.

A criminal attempt to cause storage facilities to explode was made against an unnamed Saudi Arabian petrochemical firm in 2018

Distributed Denial of Service (DDoS):

A denial-of-service attack (DoS attack) attempts to render a machine or network resource unavailable by temporarily or indefinitely disrupting services of a host connected to the Internet. In the case of a distributed denial-of-service attack (DDoS), incoming traffic flooding a target originates from multiple sources, making it difficult to stop the cyber offensive by simply blocking a single source. DoS and DDoS attacks can negatively affect a wide range IIoT applications, causing serious disruptions for utility services and manufacturing facilities.

On October 12, 2016, a massive distributed denial of service (DDoS) attack left much of the internet inaccessible on the U.S. east coast. The attack, which authorities initially feared was the work of a hostile nation-state, was in fact the work of the Mirai IoT botnet. There are two main components to Mirai,- the virus itself and the command and control center (CnC).

Ransomware:

Ransomware is a form of malicious software (or malware) that, takes over your computer and threatens you with harm, usually by denying you access to your data. The attacker demands a ransom from the victim by promising — not always truthfully — to restore access to the data upon payment.

The massive ransomware bill faced by Merck echoes the financial hits taken by other enterprises like Maersk and FedEx. Due to a production shutdown caused by the attack, Merck saw sales reductions of around $240 million.

Incidents of industrial cyberespionage

The growing threat of organized ransomware attacks against industrial companies could trigger development of another, related area of cybercrime: the theft of industrial information systems data to be used afterwards for the preparation and implementation of targeted (including ransomware) attacks. It can also be used to copy, conterfeit or compete.

Italian oil company Saipem was targeted by hackers utilizing a modified version of the Shamoon virus, taking down hundreds of the company's servers and personal computers in the UAE, Saudi Arabia, Scotland, and India.

Top three cybersecurity challenges facing industrial enterprises

1. increasing **amount of automation systems** - the variety of automation tools, number of organizations and individuals with direct or remote access to automation systems, as well as the emergence of communication channels for monitoring and remote control between previously independent objects.

2. **growing interest of cybercriminals** and special services - a decrease in profitability and increase in risks from cyberattacks aimed at traditional victims is pushing criminals to search for new targets, including those within industrial organizations.

3. looking at security from an **end-to-end perspective** as there are so many components involved, from connectivity to devices and connected applications. Security by design and embedded security is a must, involving your information security management teams early on. Gartner uses the term "digital security" to describe a common framework for security requirements across IT, OT, the industrial IoT (IIoT) and physical security environments.

Industrial security framework

The 7 key functional blocks of an end to end IoT system have different forces and contexts

Distributed Devices	Core Platform				Ecosystem	
Devices	Edge	Device Mg	Analytics	aPaaS	Marketplace	Applications
• Extremely heterogeneous environments depending on market • Managed and unmanaged devices • High cost and low cost devices	• Market still defining functionality: aggregation, security, possibly decentralized analytics... • No security standards	• Substantial impact on cost effectiveness of management (patch management, vulnerability management, updates,..) during normal operation phase • Large scale	• Lack of consolidated IoT cyber security platforms (only emerging ones) • Few Atos use cases require large data lakes and those are definitely not Security specific	• Deploy and maintain application-specific functionality on top of basic core • Integration with other systems within Enterprise often required	• Marketplace optional, depending on desire of platform owner to go beyond in-house applications and build 3rd party ecosystem	• Currently most often created by producers of the end devices without security as a priority • For ecosystems with a marketplace created by 3rd parties

Challenges:

Highly specialized/legacy protocols and equipment
Limited visibility into IoT/OT security cyber events
Cyber threat landscape rapidly growing in sophistication
High-level of specialization address gaps in security
Specialized application protocols such as CoAP

There are three important questions regarding the Industrial Security:

WHAT kind of security?
WHERE to implement?
WHICH threats should be addressed?

The main aim for the industrial security is to manage all the isolated landscapes, to find a way to secure everything, even if it is not on common operating systems. You need to set up a vulnerability management strategy on the connected assets to know how to secure, how to protect, and how to improve their integrity. Any connected device can become a weapon for hackers. Having real-time security analytics and a cyber-resilient system are essential when deploying IIoT solutions to protect against any potential attack.

Creating the unprecedent levels of connectivity needed for digitally transformed business demands a special mix of business and technical skill. Atos has the depth of technical expertise, the industry-specific knowledge and the depth of specialist partnerships to support you along your industrial security journey.

Siemens and Atos

have formed a strategic partnership since 2011 with an ambitious joint go-to-market plan and joint innovation and investment program. The program €330 million and aims to enhance Siemens and Atos' digital strategy and develop joint capabilities in Data Analytics, Artificial Intelligence, advanced IoT & connectivity services, cybersecurity and digital service technologies to support the digital transformation of their customers through an end-to-end IoT suite. Since the start of the partnership in 2011 Siemens and Atos have achieved a joint order intake of €2.5 billion and significantly surpassed all expectations.

As a partner in the development of connected products and services, Atos provides solid support from the initial idea to industrial implementation. As business technologists, we will ensure you derive maximum benefit from innovation without compromising security for either the organization, the clients, the partners or the suppliers.

Manufacturing focus

Experienced in both embedded software and business solutions, Atos business technologists' understanding spans both industry and business perspectives.

End-to-end Support

Make us your partner from brainstorming through to industrial deployment and delivery: we are equipped to serve as an end-to-end partner for your connected product and service initiatives.

Innovation

Through the Atos scientific community and company network of Business Technology Innovations Centers, we provide practical pathways to continuous innovation.

Security and compliance

Whether person-to-person or machine-to-machine, customer confidence is built on solid and demonstrable expertise in security.

Atos value proposition

Atos industrial Security Services – end to end approach

In today's more interconnected world, companies need to adopt the right tools to get closer to the market and become more competitive.

Industrial Security is considered a key area for digital transformation. At Atos, we believe that to achieve this digital transformation, it is critical to secure the business value of Industry 4.0 with sustainable security models. We highlight three value propositions among our end to end IoT Security catalog: IoT Security Suite, Secure Remote Access and SOC for Everything.

IoT security suite for an end-to-end secured ecosystem

With Horus products and solutions, Atos delivers trust for the Internet of Everything (IoE) and ensures the security of the IoT on every level through its IoT Security Suite:

- **Embedded Security:** Protect devices and sensors without compromising performances with hardware trust anchors, secure elements, trusted identity and middleware for IoT devices.
- **Identity Lifecycle Management:** Provision and manage devices digital identities securely through a security server for device enrollment with IoT PKI & HSM for key and certificate management.
- **Secure Communication:** Encrypt private data at rest and in transit in IoT ecosystems with an end-to-end data encryption and privacy enforcement for message authenticity.
- **Firmware Update:** Improve integrity of sensitive operations such as device firmware updates of IoT devices to prevent malicious code execution.

Secure Remote Access to bridge the air gap between IT and OT

How we bridged the Air gap on a smartphone:

A QR code scanned with the smartphone – in this way the smartphone connects to IT network and it is possible to see the person who is trying to connect to the OT system. If the person has the access, he receives a code to prove that he or she is properly authorized.

Evidian is the Identity and Access Management (IAM) software suite of the Atos Group. It offers a dedicated Secure Remote Access solution to manage the shop-floor landscape. It is changed from isolated islands to highly complex networks, keep security at the forefront in configurations while maintaining availability and secure remote access credentials to avoid espionage or sabotage.

The Industrial Internet of Things needs trusted secure Identities for Humans, Services and Things. With our Evidian solutions we bring strong authentication for industrial processes and enforce IAM for both IT and OT to interconnect both worlds and ensure integrity.

Atos offers full transparency and control on the access you might wish to provide to your suppliers and partners for remote services. Our solution includes a detailed audit trail with ease of use. We make sure you have the full sovereignty over your data.

Federated Access for the Connected Industrial IoT Ecosystem - the Universal Identity Service Architecture

In a co-innovation project with Siemens AG Atos defined the Universal Identity Service Architecture as a blueprint for the next generation Identity and Access Management infrastructures for the Industrial Internet of Things (IIoT).

The Atos Universal Identity Service Architecture (UISA) provides a framework for delivering secure identity and access management services for the industrial IT use cases in the extended enterprise. UISA defines a set of IAM services, functionalities, standard interfaces and protocols ready to be operated in the cloud or on premise. The IAM End User Services include identity assurance, dynamic risk analysis, risk tagging and risk-based authentication.

In an IIoT environment, several identity name spaces must be integrated and managed for multiple tenants (customers, system vendors, IIoT service partners or external organizations, for example).

The UISA architecture defines a set of open standards and protocols for connectivity, identity management, authorization, authentication and identity federation, such as SCIM, OAuth, OpenID Connect, SAML and multi-factor authentication. The services are accessible via RESTful interfaces. Adapting the UMA standard supports the decentralized user-centric access control necessary for enhancing privacy and confidentiality. In addition, UISA provides ancillary functions such as monitoring, analytics and reporting.

The key design principle is externalization of IAM functionality on all layers of the IIoT architecture. We assume that both the Use Case Apps and the IIoT Services will not operate self-sufficiently but will require an open security layer to interact with each other and new third-party services.

The Evidian IAM suite is providing all key features of the UISA blueprint. New developments like Identity as a Service will complement the Atos offer for the extended enterprise and IoT.

SOC for Everything

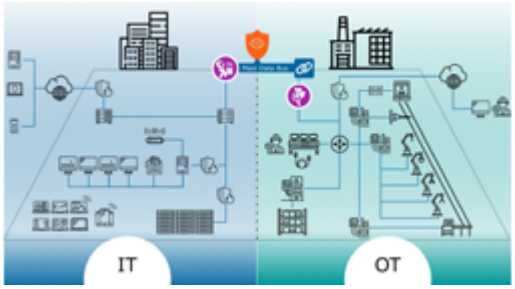
Atos, as a global leader in digital transformation, has developed the concept of prescriptive security solution for customers to predict and remediate to security threats before they occur, the SOC for Everything. Combined with Atos Big Data analytics capabilities and powered by BullSequana S servers the detection and neutralization time is improved significantly compared to existing solutions.

Based on Big Data analytics and Machine Learning technology, the SOC continuously learns from previous threats and orchestrates automated responses in real-time.

With Atos prescriptive next-generation Security Operations Centers, your IT and OT infrastructure will continuously be monitored, indicators from both environments correlated and when relevant, raw events will be merged and analyzed. This will enable organizations to create visibility throughout their full surface and win the race against malware attacks, taking advantage of vulnerable, unpatched or highly proprietary systems, and propagating systemically and laterally into the rest of the Enterprise assets. Atos SOC orchestrates then the necessary actions, in real time, to protect the assets and stop the threats before the organizations critical processes are paralyzed.

360° Security Event and Incident Management for the whole Entreprise

- IT and OT environment
- Best in Class It Security Expertise
- Best in Class OT Security Expertise through partnerships
- 24/7 Security Operation
- Global Presence
- Security Analytics
- Automated Response



"By combining Big Data, security analytics and supercomputing, Atos offers its customers the opportunity to be one step ahead of cyberattacks. The deep data analytics and monitoring in real-time allow a unique and continuous prescriptive security. Our customers can now predict and neutralize threats before they reach their goal."

Pierre Barnabé,
Executive vice-president,
Head of Big Data & Security, Atos.

Charter of Trust

The digital world is changing everything. Artificial intelligence and big data analytics are revolutionizing our decision-making process; billions of devices are being connected by the Internet of Things and interacting on an entirely new level and scale. As much as these are improving our lives and economies, the risk of exposure to malicious cyber-attacks is also growing dramatically. In this case, the security remains the most important key for a digital journey.

At Atos we believe in a collaborative approach of public and private entities to overcome all these new cybersecurity challenges of such digital world. Therefore, Atos is founder member of the Charter of Trust.

The Charter of Trust is a cybersecurity initiative that establishes three primary goals:

- to protect the data of individuals and business
- to prevent harm to people, businesses, and infrastructure
- to establish a reliable basis where confidence in a networked, digital world can take root and grow.

The Charter outlines ten principles to ensure companies and governments are acting to address cybersecurity at the highest levels:

1. Ownership of cyber and IT security
2. Responsibility throughout the digital supply chain
3. Security by default
4. User-centricity
5. Innovation and co-creation
6. Education
7. Certification for critical infrastructure and solutions
8. Transparency and response
9. Regulatory framework
10. Joint initiatives

Charter of Trust

For a secure digital world

Other members are of the Charter of Trust are: AES, Airbus, Allianz, Cisco, Daimler, Dell Technologies, Deutsche Telekom, IBM, MHI, NXP, SGS, Total, TÜV Süd, German Federal Office for Information Security, the CCN National Cryptologic Center of Spain and the Graz University of Technology in Austria.

The digital journey can be compared to a sport. Both demanding determination, performance, reinvention and persistence. We can never complete this alone. Every progressive step is the result of constant challenge and collaboration. Every journey needs a partner.

About Atos

Atos is a global leader in digital transformation with over 110,000 employees in 73 countries and annual revenue of over € 11 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 technology space. Its expertise and services support the development of knowledge, education as well as multicultural and pluralistic approaches to research that contribute to scientific and technological excellence. Across the world, the group enables its customers, employees and collaborators, and members of societies at large to live, work and develop sustainably and confidently in the information technology space.

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

atos.net/en/solutions/cyber-security

Let's start a discussion together

For more information:
Marc.Llanes@atos.net
Farah.Rigal@atos.net
Simon.Ulmer@atos.net

CT_12264_190503_RY_PP_THEINDUSTRIAL