Business challenge

To improve the scope and capabilities of its security processes, Aragonesa de Servicios Telemáticos (AST) needed a more comprehensive management console.

Transformation

To comply with government standards and improve its security tools, AST, along with IBM Business Partner Nologin Consulting S.L., launched a consolidated security management platform. The solution, built with IBM® QRadar® technology, delivers comprehensive analytics and real-time visibility into security status across multiple departments and systems.

Results

Reduces security risks
with proactive monitoring and comprehensive analytics

Boosts productivity
thanks to a consolidated view of systems and events

Supports compliance
with local and national government standards

Aragonesa de Servicios Telemáticos

Proactive monitoring. Productive teams. Powerful security.

AST supports and manages the IT operations for the Administration of the Region of Aragon—the regional government of Aragon, Spain—which comprises several independent public offices that employ more than 56,000 staff. Formed in 2001 by the Government of Aragon, the agency oversees the telecommunications infrastructures and services, computer systems and application development and maintenance for these all government departments.

"Before, we did not have all of this information. Now we know in a moment what is going on, and if we need to react."

—Óscar Torreror Ladrero,
Technology and Systems Director,
Aragonesa de Servicios Telemáticos

Share this

New laws mean new standards

In the realm of IT security, compliance with industry and government standards is non-negotiable, especially for government offices. And AST bears the responsibility for keeping all of these public offices within the Aragon region of Spain up to the necessary IT and security standards.

Previously, AST was already certified at the highest level of the nation's Esquema Nacional de Seguridad (ENS), or national security scheme. This accreditation standard was developed by the Ministry of Finance and Public Administration and the National Cryptologic Center (CCN) of the Spanish government to outline the basic principles and minimum requirements necessary for the adequate protection of information.

However, in early 2018, the Government of Aragon wanted to further protect its data and architecture, signing the Securización y mantenimiento evolutivo de las herramientas de Administración Electrónica—which charged AST with the task of improving IT security through the use of electronic management tools.

"We were subject to the strictest standards of this mandatory rule," explains Óscar Torreror Ladrero, Technology and Systems Director at AST. "We support 56,000 people throughout the Aragon government, and we support infrastructures across diverse areas such as health, justice and education. To meet these new security standards, we needed a broad solution that would let us be more conscious of what was going on with our services, networks and applications—and how we were responding to these."

> ***"QRadar is incredible, giving us a lot of characteristics and capabilities. It lets us see the full state of the security in our infrastructure with a centralized console and custom search tools."***
>
> —María Eugenia Pamplona Falomir, Security Project Manager, Aragonesa de Servicios Telemáticos

In particular, the office needed a tool that could support the management, analysis, retention and correlation of IT infrastructure logs in a non-homogeneous system.

Previously, AST had used a handful of security information and event management (SIEM) tools for monitoring, but none of these solutions were robust enough to cover the full scope of covered systems. Similarly, they lacked the analytics capabilities needed to integrate and correlate security events to achieve compliance.

"We needed to evolve," adds María Eugenia Pamplona Falomir, Security Project Manager for AST. "We decided to change our security model and how we organized our data centers. And as part of this evolution we wanted to put in place a global integration solution that could manage our logs, analyze attacks and improve our incident response."

And to meet the compliance deadline, AST needed to act quickly.

See more, do more

To help navigate this evolution of its security operations in a timely fashion, AST turned to IBM Business Partner Nologin for support. "They did a great job," comments Pamplona. "They gave us the experience and methodology to adapt our security polices and infrastructure with the tracking capabilities we needed."

Working under an IBM Embedded Solution Agreement, Nologin deployed the QRadar offering as part of its SIEM platform, highlighting that the IBM technology could:

- Manage large volumes of data
- Expand through the IBM Security App Exchange and open APIs
- Integrate with other leading security vendors
- Deliver threat intelligence with IBM X-Force® Exchange

With QRadar now in place, AST is tracking, managing and responding to roughly 337 million events each day across multiple Aragon government agencies. And the results of these efforts along with comprehensive analytics data can be readily shared with the national government since the new SIEM platform is integrated with the country's ENS.

"QRadar is incredible, giving us a lot of characteristics and capabilities," adds Pamplona. "It lets us see the full state of the security in our infrastructure with a centralized console and custom search tools. And it's changed how we operate—now our operational teams receive automatic alerts of attacks or configuration problems or problems with compliance."

In addition, AST is using IBM QRadar Vulnerability Manager to proactively identify and respond to potential security risks or compliance gaps within the vast architecture it supports. The network scans provided by the tool also help to provide additional data and context for the firm's security analytics efforts.

Further, Nologin provides ongoing support, managing the platform and regularly enhancing it to improve alert filtering.

Agile and appropriate

With this new solution in place, AST has kept its security costs low while improving visibility into security events.

"This tool has made a lot more work for us, but that's a good thing," explains Torrero. "Before, we did not have all of this information. Now we know in a moment what is going on, and if we need to react."

From a unified console, AST staff can monitor operations and coordinate responses across sites and systems, yielding faster reactions and greater productivity. And the analytics capabilities of the platform encourage proactive monitoring, reducing risk and helping to identify and resolve vulnerabilities before they can be exploited.

In addition, the joint Nologin and IBM solution helps the local government manage compliance with the new national regulation. "We have a security management system that is fully integrated with ENS and meets ISO/IEC 27001 Information Security standards," elaborates Pamplona. "So now, as events occur, we can manage and resolve them in an agile and appropriate manner."

Beyond the functionality delivered, AST is pleased with its choice of working with Nologin and IBM.

"Initially, the Government of Aragon held a meeting that evaluated all of the products on the market," recalls Pamplona. "Nologin with QRadar was the best solution between all the candidates, meeting all the technical criteria—quality, provisioning, resource utilization, the whole infrastructure."

And Torrero adds: "Nologin gave us their experience, their solution, their methodology. It was very important to get a technology expert like them to help us. They did a great job."

> ***"Nologin with QRadar was the best solution between all the candidates, meeting all the technical criteria—quality, provisioning, resource utilization, the whole infrastructure."***
>
> —María Eugenia Pamplona Falomir, Security Project Manager, Aragonesa de Servicios Telemáticos

Solution components

- IBM® QRadar®
- IBM QRadar Vulnerability Manager

Take the Next Step

To learn more about the IBM solutions featured in this story, please contact your IBM representative or IBM Business Partner.

About Nologin Consulting S.L.

Founded in 2000, IBM Business Partner Nologin delivers IT solutions intended to help customers protect, store, manage, organize and maintain their data. The business is headquartered in Zaragoza, Spain, and it maintains additional offices in the US, Mexico and Bolivia, employing more than 80 staff worldwide.

To learn more about its information solutions and what Nologin Consulting S.L. can do for you, please visit: Nologin

58033258USEN-00