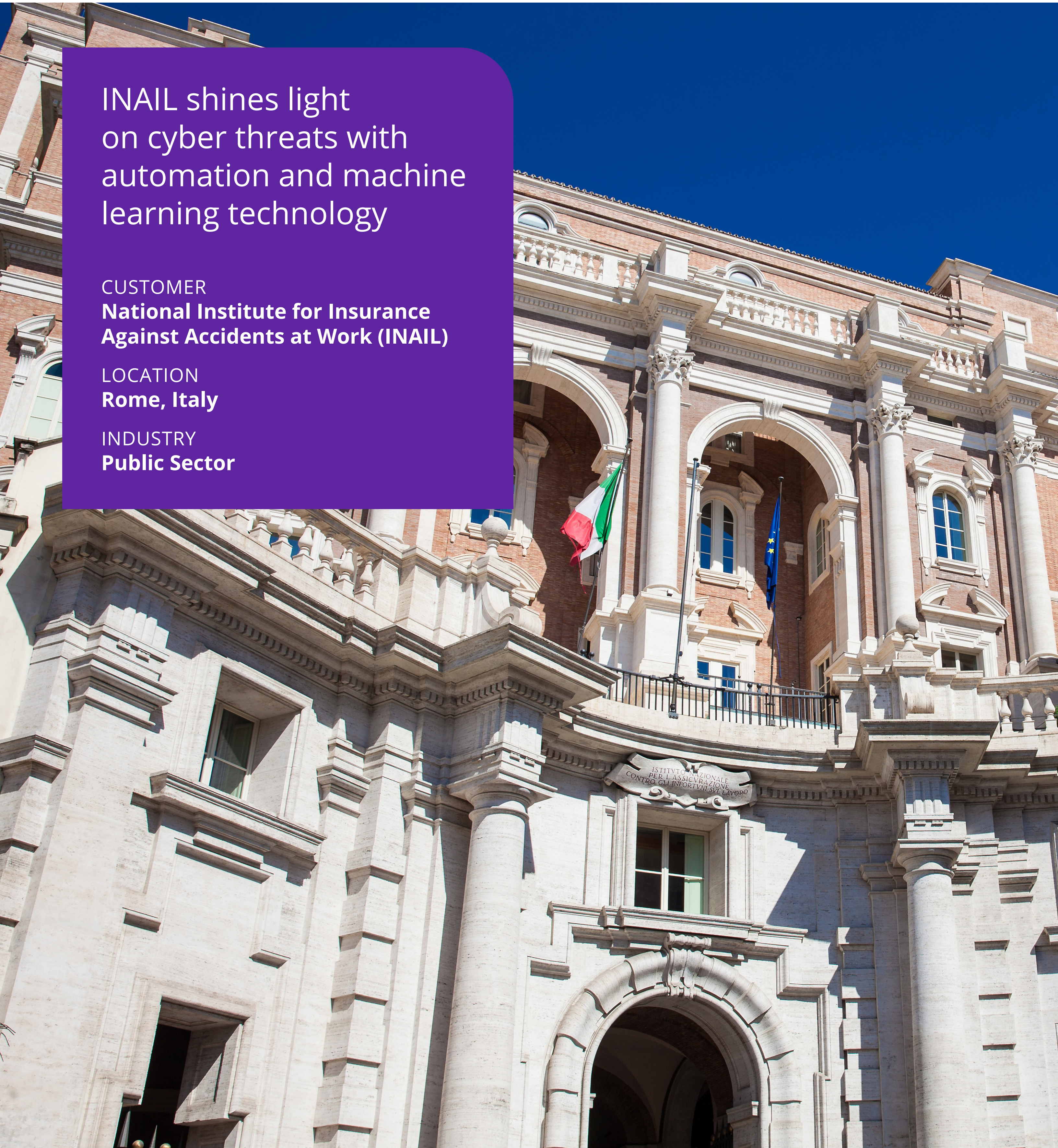
INAIL shines light on cyber threats with automation and machine learning technology

CUSTOMER
National Institute for Insurance Against Accidents at Work (INAIL)

LOCATION
Rome, Italy

INDUSTRY
Public Sector



In the face of growing attacks, INAIL wanted up-to-date threat intelligence with automated analysis and machine learning capabilities.

Challenge

- Defend the enterprise from increasing cyber attacks
- Improve real-time threat intelligence and detection
- Streamline processes with automation and advanced analytics

Solution

- Deployment of a combination of open-source and security tools for security analysis, employing machine learning technology to automate processes
- Automation of exchange of security information with other national security organizations
- Ongoing cloud and IT infrastructure services

Results

- Improved effectiveness and timeliness of identifying and acting on threats
- Increased ability to share threat data through automation and integration
- Avoided costs related to malware infection and work disruption

INAIL shines light on cyber threats with automation and machine learning technology

Cyber security is essential at Italy's national agency responsible for workplace health and safety. Like other public sector organizations, the Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro (Institute for Insurance Against Accidents at Work), known as INAIL, manages a treasure trove of personal information, making it a prime target for cyber criminals.

> "Our goal is to continuously and proactively improve our security practices and technology to deal with ongoing threats. We rely on DXC to support our efforts and introduce INAIL to the best solutions for defeating cyber criminals."
>
> — **Vittorio Baiocco**
> IT Security manager,
> INAIL

Addressing phishing and malware attacks

In the face of growing phishing attacks and highly sophisticated malware, INAIL is at the forefront of preventing data breaches. One of the few public administrators to be certified ISO 27001, a leading international standard for managing information security, INAIL decided to go further to make sure the organization is getting up-to-date threat intelligence and is equipped with automated analysis and machine learning capabilities.

"Our goal is to continuously and proactively improve our security practices and technology to deal with ongoing threats," says Vittorio Baiocco, IT Security manager, INAIL. "We rely on DXC to support our efforts and introduce INAIL to the best solutions for defeating cyber criminals."

Under a longstanding working relationship, DXC runs INAIL's security operations center (SOC) and provides most of the group's security services as well as a wide range of services across the Enterprise Technology Stack, including cloud and IT outsourcing services.

"DXC's support of INAIL in the security arena builds upon the critical service and innovation they provide in supporting our data center and managing applications in the cloud," Baiocco says.

Improved threat intelligence

INAIL first focused on threat intelligence. A key to successful threat intelligence is efficient acquisition, sharing and management of indicators of compromise (IOCs).

To help INAIL incorporate the latest IOCs into its security program, open-source intelligence sources are combined with leading security software to collect information on cyber threats and integrate the data into INAIL's security workflow. This workflow optimizes lists of efficient and reliable IOCs and redistributes them to all security tools.

Two versions of the solution have been released: an external integration layer for technical users, and an easy-to-use malware analysis solution provided to INAIL's 11,000 nontechnical users, allowing them to perform self-service analysis of suspicious email attachments.

Automated security analysis

The project also included a search engine that can detect potential attackers on the dark web. By searching for emails, domains and users in various security intelligence engines, the solution provides real-time, automated identification of security threats and incidents.

Using a machine learning model, INAIL performs predictive reputation analysis based on extraction of unique characteristics of domains and URLs.

AI and machine learning technologies are then deployed to carry out automated security analysis on millions of specific URLs and domains scored as potential security threats. The exchange of security information to and from other national security organizations and institutions is automated.

DXC used open source tools to build two classifier systems that can identify, for example, if a domain is engaging in phishing. Information on IOCs is aggregated by generating configuration lists so the data can be processed by software such as MineMeld, which compiles threat indicators from multiple sources and aggregates the data into a consistent format.

Using a machine learning model, INAIL performs predictive reputation analysis based on extraction of unique characteristics of domains and URLs. AI and machine learning technologies are then deployed to carry out automated security analysis on millions of specific URLs and domains scored as potential security threats.

Advanced protection

By improving the effectiveness and timeliness of threat detection and responses, INAIL is reducing the potential for harmful security events.

The automation and strong integration of data is helping to protect INAIL against new threats and empowers the group to share security information with other agencies more easily.

The robust security platform is also helping INAIL avoid service interruptions. The security environment put in place was particularly beneficial when COVID-19 disrupted business operations.

At the time, business email campaigns and ransomware attacks increased significantly to take advantage of the health crisis. However, INAIL did not experience any service interruptions related to COVID-19.

Looking ahead, INAIL is focused on new security initiatives, including digital identity capabilities.

Learn more at
dxc.com/public-sector

Get the insights that matter.
dxc.com/optin