CASE STUDY

Maire Group's Path to Proven Anti-Fragility with Picus

In a high-stakes industrial environment where operational continuity is essential and threats evolve constantly, global technology and engineering group MAIRE recognized that cybersecurity maturity requires more than layers of defense. It requires proof.

To meet the demands of a complex IT and OT landscape, MAIRE Group embedded Picus Security's Security Control Validation (SCV) and Attack Path Validation (APV) into its cybersecurity operations. The result was a measurable transformation from traditional security practices to a dynamic model focused on continuous validation, transparency, and business alignment.

Industry:

Industrial Engineering and Technology

Products:

- Security Control Validation (SCV)
- Attack Path Validation (APV)
- Attack Surface Validation (ASV)
- Exposure Validation (EXV)

About MAIRE

MAIRE is a global technology and engineering group providing Integrated E&C Solutions for the downstream market and Sustainable Technology Solutions through three business lines: Sustainable Fertilizers, Low-Carbon Energy Vectors, and Circular Solutions. It operates across 50 countries with more than 10,200 professionals globally.

Challenges and Results:

- **Limited visibility into control effectiveness**
  → Gained continuous, measurable insight into real-world defense performance
- **Undetected misconfigurations creating risk**
  → Found and fixed hidden weaknesses missed by traditional tools
- **Lack of demonstrated cybersecurity maturity for compliance**
  → Aligned with frameworks like MITRE ATT&CK and ISO/IEC 27001
- **Silos slowing response and accountability**
  → Boosted collaboration across security, IT, and business with shared metrics
- **Resource allocation without performance validation**
  → Maximized ROI by optimizing tools and prioritizing high-impact fixes
- **Reactive measures limiting innovation and growth**
  → Built a proactive cybersecurity culture that strengthens over time
- **Overwhelm from theoretical vulnerabilities and risk scores**
  → Used Exposure Validation to focus on exploitable risks and prioritize fixes

Problem:
Confidence Alone Was Not Enough

"In our industrial context, the issue wasn't missing technology. It was the lack of strategic visibility and measurable control over cyber risk," said Andrea Licciardi, Senior Cybersecurity Manager at MAIRE Group.

Even with a mature Cyber Fusion Center and a strong toolset, the team had no consistent way to measure how their defenses would perform under real-world conditions. Pen tests and vulnerability scans provided only point-in-time snapshots. They didn't uncover hidden misconfigurations or deliver the real-time feedback the team needed.

For MAIRE, this came down to two core problems:

- **Some tools and settings seemed fine on paper but failed against real threats.**
- **Without regular feedback, the team missed chances to improve and collaborate more effectively.**

Solution:
Defenses Had To Be Tested and Proven

Instead of expanding their security stack with another control, MAIRE Group chose Picus to continuously validate and strengthen existing defenses. They began with Security Control Validation (SCV), then expanded into Attack Path Validation (APV) to expose hidden risks and critical chokepoints.

SCV allowed testing against a constantly updated threat library. Simulations exposed gaps in controls that appeared properly configured but proved ineffective. With MITRE ATT&CK mappings and tailored remediation guidance, the team could act quickly and confidently.

APV added deeper visibility. By simulating attacker movement, credential compromise, and data exfiltration, MAIRE Group could visualize and prioritize the most dangerous internal attack paths.

> ***"Picus didn't just show us data. It uncovered blind spots and gave us clear, immediate steps to strengthen our defenses," said Licciardi.***

Outcome:
Data-Driven Security Replaced Reactive Defenses

By integrating Picus into their Cyber Risk Operation Center (CROC), MAIRE Group shifted from a reactive posture to a data-driven model of cybersecurity maturity. With real visibility into detection and prevention, they identified misconfigurations that traditional controls could not see and reduced false confidence through continuous validation. The approach aligned with ISO/IEC 27001 and MITRE ATT&CK frameworks while strengthening collaboration across IT, security and operations, ultimately maximizing ROI on existing security investments.

"Each simulation became a deliberate act of growth," said Licciardi. "Instead of simply withstanding threats, we learned from them and got stronger."

This reflects what modern security now demands. As threats grow more complex and regulations tighten, many organizations remain reactive, investing heavily in prevention tools but lacking real-world testing. ***"There is a mindset shift happening,"*** Licciardi explained. ***"Security is no longer a barrier to innovation. It becomes a strategic enabler, unlocking value through trust, adaptability and operational excellence."***

MAIRE Group chose Picus for both performance and partnership. They began with SCV to establish a baseline, then expanded to APV to simulate full adversary attack paths. The results were clear, actionable and tailored but just as important was the experience of working with the team. ***"What truly sets Picus apart is the people behind it,"*** Licciardi said. ***"The team listens, understands our context and turns feedback into innovation. It's a real partnership, not just a vendor relationship."***

> ***"Absolutely, I would recommend Picus,"*** said Licciardi. ***"But more than that, I recommend the mindset it brings. Picus is not just a tool. It's a different way of thinking about cybersecurity."***
>
> He continued: ***"It helps you shift from perception to validation, from reaction to evolution. Every simulation is an opportunity to learn, adapt, and improve."***