Client story

Enhancing vulnerability management for a leading manufacturing organization

Strengthening cyber defenses with risk-based and cyber-aware orchestration

Objectives

- Map attack surface and enable real-time threat monitoring
- Prioritize vulnerabilities based on risk and resources
- Define clear departmental cybersecurity accountability
- Create a collaborative governance framework
- Unify fragmented security policies

Why Unisys?

- Proven experience deploying cybersecurity-focused technology without operational disruption
- AI intelligence, cloud solutions, and cybersecurity integrated into complex environments
- Specialized continuous threat exposure management for complex estates across organizations
- Extensive compliance expertise with data privacy regulations
- Vendor-neutral experts deploying rapid improvements through real-world testing and risk mitigation

Solution

Unisys cybersecurity solutions

- Implemented comprehensive vulnerability management using advanced technology and cybersecurity best practices
- Integrated risk-based security orchestration, automation, and response (SOAR) capabilities with ServiceNow SecOps for rapid threat response
- Deployed real-time dashboards providing stakeholder visibility into vulnerabilities, risks, and security measures
- Created organization-wide attack surface visibility and assigned departmental cybersecurity responsibilities
- Automated vulnerability assignment to departments based on expertise through centralized ServiceNow SecOps
- Developed custom risk assessment algorithms enabling data-driven vulnerability decisions

Results and benefits

- Strengthened security posture with faster threat response — risk-based SOAR and ServiceNow SecOps reduced attack surface while custom algorithms improved threat prioritization and response times
- Unified fragmented cybersecurity through clear accountability — new model created departmental responsibility and compliance with privacy regulations
- Enhanced legacy system vulnerability management — risk acceptance framework enabled better decision-making for complex systems
- Built a cyber-aware organizational culture — continuous training and support from Unisys experts fostered enterprise-wide security awareness
- Improved stakeholder experience and visibility — modernized dashboards transformed user satisfaction and decision-making capabilities

Building a secure ecosystem with proactive vulnerability management

A leading manufacturing organization set out to modernize and streamline its vulnerability management program to better protect sensitive data and mission-critical services. Disparate tools and processes across departments limited visibility into the full attack surface, with upgrades needed for risk-based prioritization.

The enterprise sought a strategic partner to establish an enterprise-wide cybersecurity governance model, clarify roles and responsibilities, and unify processes and dashboards to drive faster data-driven remediation while maintaining uninterrupted operations. The organization engaged Unisys to accelerate this transformation and cultivate a cyber-aware culture anchored in data privacy.

Sealing the deal with specialized technology expertise

The organization chose to work with Unisys because of our extensive track record with highly regulated sectors. We've cultivated a strong reputation as a trusted cybersecurity partner, excelling at helping clients reorganize complex technology environments to strengthen cybersecurity protections.

Unisys' team of vendor-neutral cybersecurity experts implements complex solutions without disrupting mission-critical operations. Our ability to help the enterprise comply with stringent data privacy regulations while building a new vulnerability management solution from the ground up was also essential.

Protecting critical assets with risk-based security orchestration

The foundation of this implementation was Unisys' integration of risk-based SOAR capabilities, which our experts seamlessly integrated with a ServiceNow SecOps module. With this combination, the organization could automatically prioritize vulnerabilities and remediation strategies based on real-time threat intelligence and estimated business impact.

Unisys also created a custom interactive dashboard that allows client stakeholders to gain real-time visibility into these vulnerabilities, risks, and remediation efforts with the click of a single button. Our experts also developed custom algorithms for risk reassessment, helping stakeholders make data-driven decisions and focus on the enterprise's most critical cyber threats.

Deploying a centralized platform to manage vulnerabilities and thwart attacks

One of the most significant challenges in this engagement was addressing the fragmented cybersecurity policies and roles throughout the organization. This fragmentation created several vulnerabilities and prevented technology leadership from understanding the full breadth of attack vectors the enterprise faced.

Unisys catalyzed a major organizational transformation by implementing an enterprise-wide cybersecurity governance and accountability framework. The framework established clear, actionable policies and procedures for vulnerability management across the enterprise and within individual departments.

A critical aspect of this framework was the creation and appointment of cybersecurity governors in each department. These leaders are now responsible for coordinating data privacy efforts across the enterprise and holding their departments accountable for patching vulnerabilities and responding to real-time threats.

Enabling a cyber-aware culture for sustainable success

Unisys recognized that building a cyber-aware culture was essential to creating a sustainable impact on cybersecurity. Unisys led ongoing training sessions for all technology stakeholders to achieve this, equipping teams with the knowledge and skills needed to manage vulnerabilities effectively.

These training programs shifted the enterprise from reactive to proactive, cultivating a cyber-aware culture in which every technology team member is accountable for cybersecurity and ensures the transformation endures well beyond the implementation.

Building sustainable security and strengthening defenses

The organization's partnership with Unisys exceeded stakeholder expectations and delivered measurable benefits. The enterprise significantly strengthened its overall security posture and maintained a refined vulnerability management process, producing faster remediation times and more data-driven threat prioritization.

The new cybersecurity governance model and enhanced accountability for departmental leaders also produced greater transparency and trust in the organization's security posture. Stakeholders prize the custom dashboards' ability to provide data-driven insights and improve decision-making.

The partnership strengthened internal and public confidence in the organization's data privacy safeguards by unifying a fragmented cybersecurity environment into a proactive, accountable program. The modernized technology foundation and enhanced cybersecurity posture position the organization to sustain robust, long-term defenses against an evolving cyber threat landscape.

Learn how Unisys is helping organizations and businesses respond to the growing number of cybersecurity threats and build trust. Visit us online or contact us today.

unisys

unisys.com

© 2026 Unisys Corporation. All rights reserved.

Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.

07/26 6952-12635