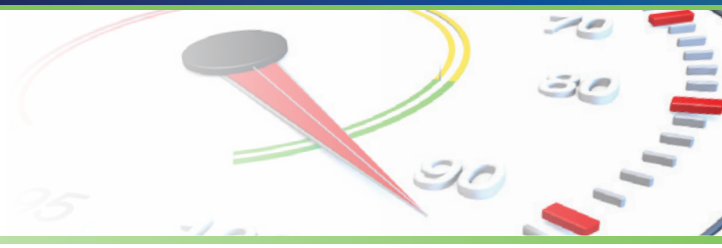
Telos

Xacta.io™

Security data at the speed and scale you need for threat-informed risk management.



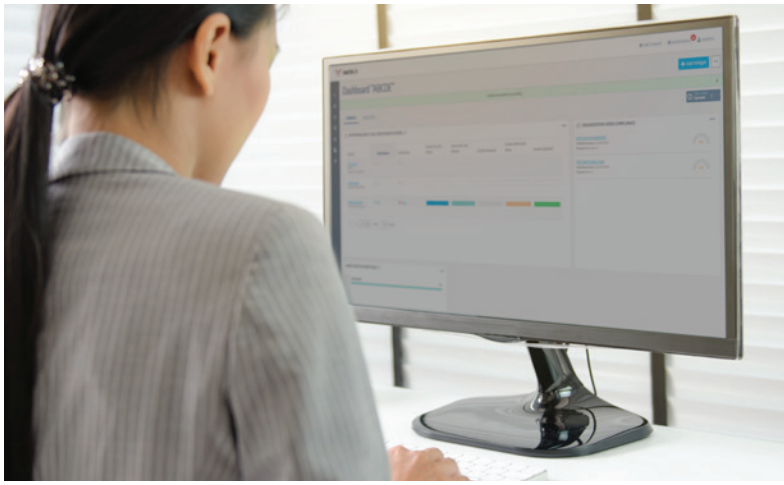
- Aggregate and analyze asset and vulnerability data at scale – in the cloud, on-premises, and in hybrid environments
- Correlate results from multiple security scans into a single view and map them to the relevant controls
- Reduce the time needed to analyze and confirm findings across hundreds of thousands of assets
- Utilize trending reports for greater understanding of how findings have changed over time
- Increase analysts' effectiveness in understanding extensive security results
- Standardize your security approach and methodology by using centralized repositories of mappings to controls

Maintaining your organization's cyber risk and compliance posture is difficult, given the number and diversity of security tools you use. It's hard to keep track of the results from vulnerability scanners and other security systems, much less analyze the results and map them to the right controls. Without a complete, high-level view, you can't be confident that your organization is protected against threats and vulnerabilities.

Now there's a solution for taking control of your ever-changing cybersecurity landscape. **Xacta.io** correlates results from multiple security products across your organization into a single view, and maps them to the relevant controls for security and risk management, such as NIST 800-53, NIST CSF, FedRAMP, COBIT 5, ISO, and others. You can then use these results to create reports for analysis and to understand trending security issues in their environment.

xacta.io™

Data | Analytics | Action



Xacta.io gives you:

- Robust dashboard capability — giving you a holistic view of your organization's asset compliance posture
- Fast, automated processes for validating controls with scan results using our Predictive Mapping™ algorithm
- Control crosswalking for major regulations to minimize audit fatigue
- Actionable reporting metrics for thoughtful, prioritized decisions
- Multi-level reporting with comprehensive, historical trending capabilities
- Greater confidence in test results and reports
- A more consistent methodology for evaluating your security posture
- Direct support for assessment boundaries

Xacta.io is 100% SCAP compliant and accepts configuration and vulnerability data captured from a long list of security tools that assess hosts, application servers, databases, and source code. Configuration and vulnerability data that can't be automatically captured can be easily collected using Xacta 360.

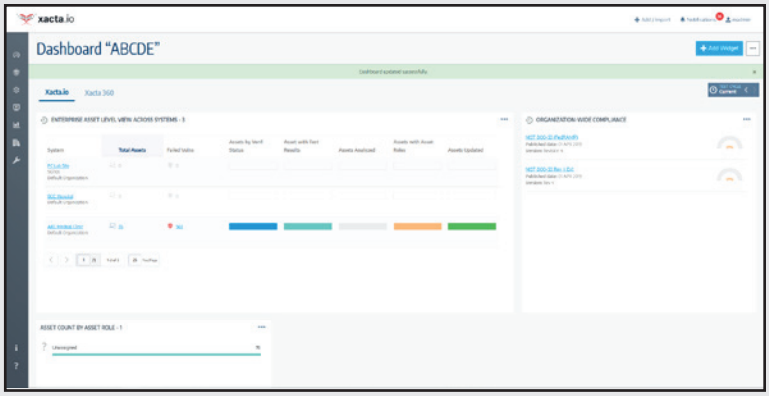
With capabilities unmatched in the industry, Xacta.io gives analysts an unprecedented understanding of their asset vulnerability landscape.

Xacta.io Gives You Greater Confidence in Your Organization's Risk and Compliance Posture.

Only Xacta.io gives you the powerful capabilities you need to:

Identify the assets you need to monitor. Xacta.io organizes your IT asset data into actionable information for compliance, risk, and vulnerability management. It captures and reports on a rich collection of demographic information regarding each device — asset inventory, physical location and ownership information, operating system configuration data, and hardware and software inventory — so you can organize your IT asset data into actionable information.

Xacta.io: Visualized insights for threat-informed risk management.



Xacta.io's dashboard and in-depth reporting capabilities keep you fully informed in real time about your cyber risk and compliance posture.

Xacta.io offers an intuitive dashboard that allows you to make greater use of your asset-related data for real-time threat awareness and fully informed risk management. Its advanced visualization capabilities provide scorecards, regulatory reporting, ad-hoc reporting, analytics, and decision support. It also offers new visualization and reporting capabilities for Xacta 360.

Get real-time information on the status of controls while minimizing performance hits to your IT environment. Agent-based monitoring is precise but also puts a strain on network resources. Agentless monitoring minimizes that strain but doesn't give you as much direct control over monitoring. Xacta.io provides the optimal balance between precise monitoring and network resources, ensuring you always have situation awareness of potential risks and threats. It leverages the third-party agents your current security products use, complemented by the ability to schedule automatic scan file imports from network locations or S3 buckets.

Xacta.io uses a risk-based approach to prioritize control assessments so you can continuously monitor mission-critical systems while also monitoring less-critical systems on an ongoing but less-frequent basis. You can specify a given check-in period for a group of systems, giving you the flexibility you need to be notified about system compliance changes as you see fit. This helps you meet the demands of continuous monitoring requirements in the real world by giving your most vital systems priority.

Automatically map vulnerabilities to the controls you use and the standards you must comply with. Xacta.io's Predictive Mapping and cross walk capabilities save you hours of laborious manual mapping by automatically mapping thousands of system vulnerabilities to the corresponding controls you have in place and the standards in which those controls apply. This powerful capability assures near-real-time compliance with the leading standards for cybersecurity and risk management.

Take action with tools and intelligence for remediating vulnerabilities. Xacta.io imports data from industry-leading scanners, firewalls, and other security tools and from cloud security services to identify trends, make comparisons, and report on findings. Its flexible API architecture enables easy integration with other third-party tools. Xacta.io allows you to quickly analyze thousands of assets in the time it takes to analyze two or three assets through the use of Cascading Analytics and creation of analysis rules.

Predictive Mapping: The Key to Continuous Compliance.

There are many tools that can tell you if your IT environment has vulnerabilities that can be exploited. But it's just as important to know which security controls are affected by these weaknesses and which assets are governed by those controls.

Xacta.io offers a remarkable capability that's unmatched in providing this level of visibility into your cybersecurity environment. It's called Predictive Mapping, and it bridges the gaps between system vulnerabilities and their related controls.

With Predictive Mapping, Xacta.io gives security testers and assessors the power to look across multiple security feeds and understand how they influence a variety of controls and requirements for a particular product or system. It dynamically maps the content from various vulnerability schemas to the relevant controls in a relationship model. It automatically detects and plots the points of intersection among vulnerabilities, controls, and assets. And, the model grows as new sources of information such as third-party scans are added.

Never before have IT security professionals enjoyed this level of visibility and understanding into how assets, vulnerabilities, and controls relate to one another.

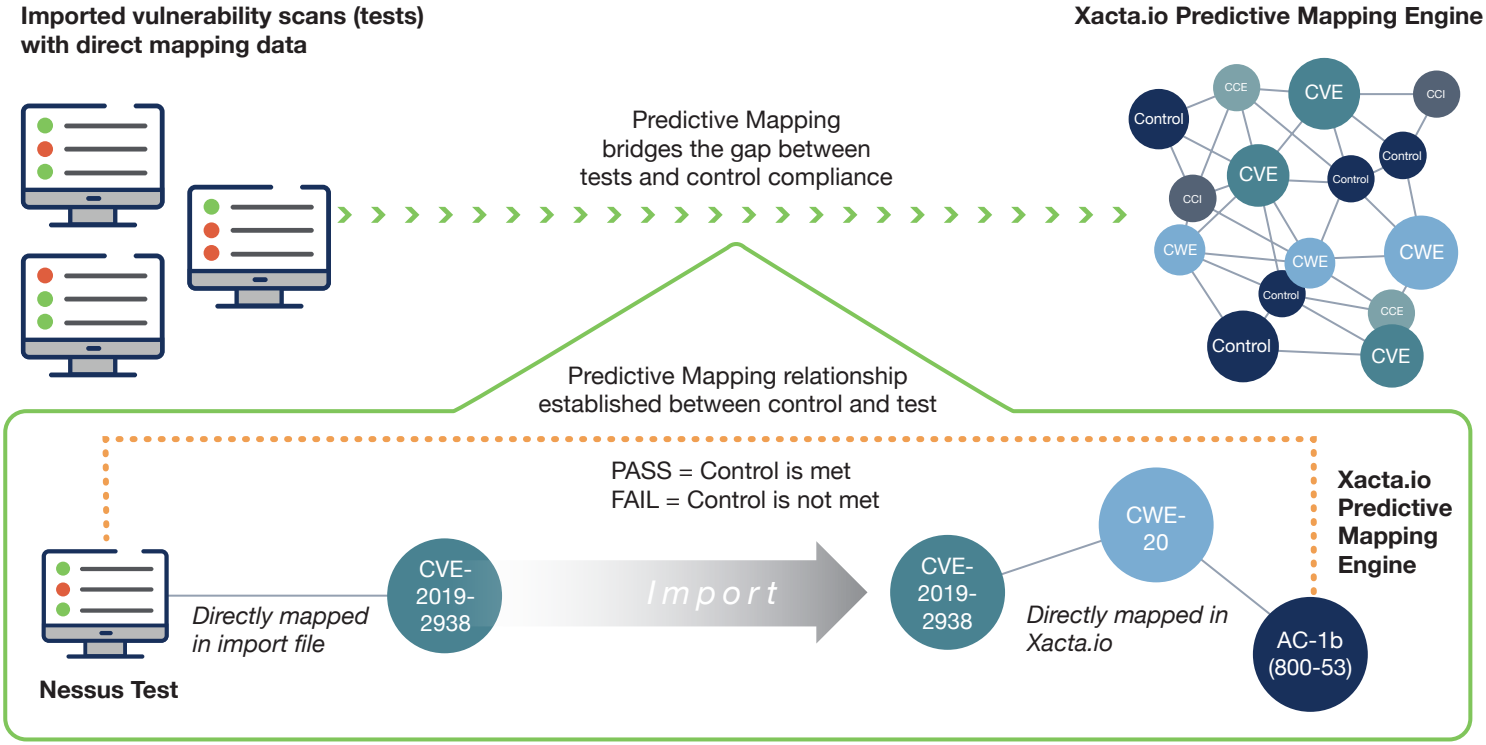
Controls Crosswalk: Effortless Compliance Across Multiple Regulations

Compliance with multiple cybersecurity regulations is the reality for most organizations today. Many of these regulations have similar (if not identical) controls that overlap, resulting in a significant amount of redundant work when it comes to validating them.

Xacta.io has a customizable control mapping library that includes pre-mapped controls between the top regulations and frameworks used in the industry, including NIST SP 800-53, CNSS 1253, NIST CSF, FedRAMP, ISO 27002, and others. Additional mappings can be added by administrators, and the default mappings list grows with each new release of Xacta.io.

Once a test result is automatically mapped to a control via Predictive Mapping, the crosswalk library does the rest of the work. Similar controls that are also mapped to the predictively mapped control will receive the same validation result – met or not met.

The controls crosswalk capability is also useful when scanners return results directly mapped to controls that may not apply to your organization. Through control crosswalking, those results can be applied to the controls that are applicable to your organization.



Predictive Mapping is like a family tree or social network that makes and maintains the connection among IA controls, vulnerabilities, and IT assets.

Cascading Analytics: Analyze Many Assets with Less Effort.

Cascading Analytics is a unique capability that enables analysts to process large numbers of assets along with their associated vulnerabilities. Cascading Analytics is revolutionary in its approach to increasing productivity while decreasing analysis efforts on the part of the user.

Xacta.io's Predictive Mapping engine makes Cascading Analytics possible. Predictive Mapping builds a network relationship among content, assets, and tests, and learns and propagates this information. This means Xacta.io can capture the analysis performed on an asset and adaptively cascade the analysis to all other related assets and tests. This process of analyzing and cascading can be repeated across your environment until all assets are analyzed.

Cascading Analytics will even recognize that tests from different third-party scanners refer to the same vulnerability and apply the analysis accurately based on Predictive Mapping. Analysts will no longer have to analyze all assets in the list. Analyze just a few assets and let Cascading Analytics apply that analysis to the rest.

Xacta.io: A Powerful Tool for Your Continuous Monitoring Requirements.

"Automation supports collecting more data more frequently and from a larger and more diverse pool of technologies, people, processes, and environments." So says NIST SP 800-137, Information Security Continuous Monitoring, the federal government's policy document for continuous compliance monitoring.

The ability to collect and map control data from so many different sources is one of the many capabilities that make Xacta.io a powerful tool for meeting federal mandates for continuous compliance monitoring. Xacta.io maps scan results from multiple sources on the fly to the corresponding security controls you need to meet. You can then use these results in reporting and remediation as part of your continuous monitoring strategy.

Fitting smoothly into your existing security tool environment, Xacta.io can be the core of your continuous monitoring initiative.

XACTA®

Take control of your risk and compliance posture with continuous monitoring and security risk assessment.

Xacta.io is a key component of the Xacta suite for enterprise security risk assessment. Xacta automatically detects changes to the IT environment so you always have situation awareness of potential risks and threats.

Xacta enables organizations to track the security state of a wide range of information systems on an ongoing basis and maintain the correct security posture for the systems over time. Its elements work together to provide CISOs and other senior leaders with a dynamic view into the current status of security controls.

Contact Telos to learn more about Xacta.io.

We look forward to hearing more about your security challenges and sharing more information with you about the capabilities of Xacta.io and the Xacta suite. For government organizations, we offer these solutions under a variety of contract vehicles suited to your agency and requirements. Please contact us to begin a conversation about how we can help you manage your complete cybersecurity posture.

Telos®

Contact us for more information.

info@telos.com | 800.70.TELOS (800.708.3567)

www.telos.com | twitter.com/telosnews

facebook.com/teloscorporation

linkedin.com/company/telos-corporation