IonIA™

leidos

Protecting any environment from cyber threats and maintaining information assurance (IA) begins with effective cyber hygiene. More than 80% of known cyber threats can be mitigated by implementing and enforcing basic cybersecurity best practices. However, the need to have specialized staff to perform risk analysis and execute required manual remediation actions makes it difficult for organizations to attain this level of basic cyber hygiene. In response to the burdens of manual procedures, industry has developed a range of applications to automate many of the manual steps. The best of these applications can reach 95% of the goal for proper cyber hygiene.

Using IonIA™, Leidos can effectively and efficiently protect an enterprise against the 80% known threat. Our proven vulnerability assessment and remediation methodology integrates and applies the right people, process, and automated tools and delivers the ability to reach greater than 99% of the cyber hygiene goal by minimizing the known exploitable attack surface of servers and client systems to less than 1%—providing a strong bulwark against cyber threats.

OUR CAPABILITIES

IonIA is a set of scripts that runs on top of SharePoint and Microsoft SQL that integrates with existing enterprise management support tools. Data is pulled from these disparate sources, analyzed, and then displayed in a number of reports. IonIA employs various tools to audit the infrastructure and assess its vulnerability aperture, security control and compliance status, and foundational components of an organization's system security plan to maintain minimal residual risk.

IonIA achieves vulnerability management and remediation through continuous monitoring involving four key components: vulnerability identification and prioritization, vulnerability assessment, remediation planning, and remediation. IonIA integrates seamlessly to complement an organization's cybersecurity compliance and risk reporting by providing automated post-scan analytics that result in actionable vulnerability remediation intelligence for cybersecurity and operations personnel. Using prioritization and automation, IonIA lowers costs by reducing the amount of time cyber analysts need to spend on more mundane collection and identification tasks.

IonIA continually improves IT security through better IA situational awareness and prioritized remediation efforts. It integrates with existing tools to continuously prioritize remediation that in turn reduces the overall IT infrastructure attack surface and the manpower needed for incident response overtime.

OUR APPROACH

Leidos integrates IonIA and associated toolsets with existing enterprise and agency continuous diagnostics and mitigation (CDM) tools to create an end-to-end detection, identification, analysis, remediation, and reporting architecture and implementation.

Using IonIA processes and procedures, Leidos defines, maintains, and repetitively monitors and reports Federal Information Security Modernization act (FISMA) compliance attributes, security patch enforcement, and secure baseline enforcement at every security layer through rhythmic vulnerability assessment scanning and stringent security-focused configuration management control.

PROVEN SUCCESS

Leidos developed IonIA for a U.S. federal agency's program to handle the problematic combination of ever increasing notifications, the need to manage a large geographically dispersed and complex IT infrastructure, and the necessity to protect data critical to the agency's mission.

Using IonIA, Leidos enforced the agency's security model to provide 100% security to the network at all times. With more than 44,000 workstations and 3,000 servers distributed over 1,500 sites, the model was designed to scale easily and was tailored to meet the needs across these sites.

Leidos created a Vulnerability Management Support Analyst Group, which focused on remote remediation of vulnerable systems. It was able to save more than 3,400 labor hours on 1,266 highly vulnerable systems. During one 6-month period, the group remediated nearly 2,740 high density vulnerable systems, almost doubling the number or systems remediated during the previous 6 months.

Leidos' consolidated security policy provided consistent application of security methods, practices, and approaches across the enterprise to reduce risk.

FEATURES AND BENEFITS

Integrates with existing continuous diagnostics and mitigation (CDM) tools

- Provides transparent, at-a-glance enterprise IA situational awareness
- Optimizes existing tools and improves enterprise-level security visibility
- Minimizes need to stand up a new system or retrain operations personnel

Prioritizes vulnerabilities and increases automated remediation

- Enables skilled cyber analysts to focus on high-value tasks
- Reduces demand for difficult to staff skills, avoiding staffing gaps or need for costly hiring tactics
- Reduces the manpower needed for incident response
- Improves job satisfaction, which increases retention for better mission continuity

Prioritizes IA remediation efforts

- Reduces overall attack surface of the IT infrastructure

Automates compliance reporting

- Saves time and resources

WHY PARTNER WITH LEIDOS?

In addition to understanding effective cyber hygiene, Leidos has developed a Risk and Privacy Management Acceleration Playbook (RAPMAP) to capture required documentation and complete activities in order to support system Authorization to Operate. While compliance alone does not ensure network security, it is a foundational element of all successful security programs. Combining RAPMAP with IonIA positions Leidos as a comprehensive partner in compliance and risk management.

NEXT STEPS

A majority of cyber threats can be stopped by implementing and enforcing basic cybersecurity best practices — many of which can be accomplished easily and at low cost. Leveraging IonIA, Leidos can effectively and efficiently protect organizations against known threats. Contact our experts to learn more about Leidos' comprehensive support for your cybersecurity journey.

FOR MORE INFORMATION

leidos.com/cyber | leidos.com/contact

Export eTrace record 20372 | 19-0051 | Leidos Creative

leidos