Industrial Defender ASM® for Automation Systems Management
INDUSTRIAL DEFENDER ASM FOR AUTOMATION SYSTEMS MANAGEMENT

Industrial Defender ASM® is a management platform designed to address the overlapping requirements of cybersecurity, compliance, and change management for Industrial Control Systems (ICS). A “single pane of glass” that provides asset visibility, tracking, configuration, policy control, and reporting for industrial endpoints from multiple vendors.

APPLICATION FEATURES

Industrial Defender ASM includes an active dashboard (Figure 1) and application feature sets. The Industrial Defender ASM active dashboard provides a tabbed interface for easy access to key information about assets, security, operations, and compliance. These tabs provide visibility to top level asset data, security event trends, operational controls, and system-wide compliance.

INDUSTRIAL DEFENDER ASM BENEFITS

- Gain a consolidated view into your ICS asset base at a single site and across your fleet to monitor trends, manage events and investigate anomalies
- Improve accuracy and efficiency of compliance reporting with automated data collection and archival of artifacts relevant to regulatory requirements
- Reduce cybersecurity risks with automated asset configuration collection, enabling you to perform on-demand vulnerability management
- Increase visibility into systems performance including application and process failures, registry and file changes
- Improve situational awareness and reduce total cost of ownership with multiple application feature sets on a single platform
These work together with built-in feature sets for;

1. Asset Management

Asset management features (Figure 2) provide a fully automated solution to discover, track and report on hundreds and thousands of assets across your ICS footprint.

- Know what is deployed – Automate asset detection, configuration collection, baseline asset inventory creation, and search capabilities.
- See it live! – Asset topology (Figure 3) features a map of deployed ICS assets with single-click access to status, reachability, and health. The map dynamically expands from local, to plant, to fleet-wide views.
- Enable cybersecurity controls and compliance – Use best practices such as the “Top 20 Critical Security Controls,” industry standards such as NIST SP 800-82 or industry guidelines such as NEI 08-09 for Nuclear Power Reactors, and create documentation for NERC-CIP.

2. Configuration & Change Management

Configuration and change management features provide (Figure 4) a robust set of tools and reports that leverage asset management baselines to search, alert, manage, and control asset configurations.

- See changes as they happen – Compare baseline to actual reports to eliminate drift. Group configuration management by type of asset, and automatically report changes, including software release level, patches, ports, services, and firewall rules, regardless of vendor or location, including HMIs on the plant floor and the PLCs, RTUs, and IEDs responsible for operations.
- Take control of change – Normalize and group types of assets, and report changes to individual assets, including software, regardless of vendor or location.
- Reduce manual activities – Manage configuration rules automatically and remotely, including changes to user accounts or firewall rules.
- Improve control system cybersecurity – Use asset baselines to determine which systems to harden, disable unnecessary ports and services, and quickly identify vulnerable assets.
3. Security Event Monitoring

Security event monitoring features (Figure 5) provide actionable intelligence from your control system. These features consolidate, track, triage, and trend events in your ICS base using user-selectable time periods including hourly, daily, weekly, and monthly.

- Improve situational awareness – Track critical events specific to your asset base. Events are user selectable and can be tracked by category, time, port, and priority.
- Consolidate event logs – Enable broad searches and event reporting across multiple devices and device types.
- Use event trend analysis – Track potential vulnerabilities that appear at higher rates in specific categories.
- Detect user access issues – Support ongoing vulnerability assessment and document NERC-CIP requirements, including password failures, user account changes, and unauthorized user access.
- Reduce triage time – Detect anomalies quickly and easily with built-in correlation rules for counts, thresholds, standard deviations, and more.

4. Policy Management

Policy management features (Figure 6) automate the enforcement of compliance across your control systems asset base. As a vendor-agnostic solution, policies can be easily created and applied to multiple asset types, saving time, cost, and reducing duplication of effort. In addition to user-created policies, Industrial Defender ASM includes standard policies for NERC-CIP v3 and v5, Nuclear Energy Institute (NEI) 08-09 cybersecurity standards, and NIST SP 800-82.

- Establish compliance and management – Create security policies and governance standards that cover multiple assets quickly and easily.
- Create sustainable compliance programs – Construct a program for NERC-CIP, NIST SP 800-53, ISO 27000, and CFATS that is easily sustainable.
- Improve visibility to risk – Uncover insufficient policy adherence and potential security and compliance gaps.
- Protect against known malware – Check baseline software patch levels for protection via proactive policy rules.
- Be audit ready – Link policies to applicable regulations as evidence of compliance in case of audit.
5. **Report Management**

Report management features (Figure 7) eliminate the laborious manual task of data collection and report generation, providing a suite of standard reports, including NERC-CIP V3 and V5 reporting packages and a wide range of reports encompassing assets, configuration, firewalls, policy, software and patches, and users. Report subscriptions can be configured for non-privileged users, allowing them to receive reports via many alternative methods, ensuring the delivery of the most current information to those who need it most.

- NERC-CIP V3 and V5 compliant documentation – Cover all key elements of your NERC-CIP audit need, with over 40+ NERC-CIP reports, including asset baseline vs. actual and user access reports.
- Document network controls – Compare changes to ports and services on each asset across your environment, by time interval.
- Validate software revision and license inventory baseline – Control cost and understand patch levels for internal audits.
- Document user access controls – Comply with NERC-CIP and NIST SP 800-82 via password policy.
- Document user account management – Detail asset access controls and failed logins attempts.

6. **Workflow Automation**

Work Automation Suite (Figure 8) is an optional feature set that integrates document management and reporting as part of a structured workflow enabling ICS professionals to streamline and eliminate the manual processes associated with change management.

- Structured Workflow – Enables operators to initiate a change, define assets that will receive the change, upload related test documents, track progress, and automatically report on progress streamlining the entire process.
- Document Management – Provides a central repository for documents related to a change including test documents, configuration files, and approvals, capturing all related information in a single storage container.
- Automated Reporting – Leverages the policy management feature set. Reports run automatically based on completion of the change, a defined time, or at a set interval, ensuring you never lose track of and can easily see the impact of a change on cybersecurity requirements.
OPTIONAL ASM SERVICES, MONITORING CAPABILITIES, AND REPORTING

Vulnerability Monitoring
Leidos Vulnerability Monitoring Service is an optional offering that combines the power of Industrial Defender ASM® asset management with the accuracy and robustness of industry vulnerability and patch databases, such as NIST and Microsoft Technet, delivered as a service. Industrial Defender ASM uses a “scan-less” approach to collect software inventory data from your assets and via our service maintains a current list of the potential Common Vulnerabilities and Exposures (CVEs). It compares the CVEs to the known software inventory, documents vulnerabilities and available patches that exist on individual assets.

Passive Monitoring
Industrial Defender ASM integrates active and passive monitoring into one platform to provide a single view into your SCADA environment. Active monitoring uses agent or remote credential-based data collection and passive monitoring methods collect information via the wire. With Industrial Defender ASM customers have a choice in the monitoring technology to use depending on multiple factors including the device type, area of the operation, and depth of data required. Active methods typically yield a wealth of configuration and security data from endpoints, while Passive methods allow you to look deeper into the PLC environment.

Custom Reporting
Custom Reporting is an optional capability that enables ASM customers to author their own reports using newly created datasets within the ASM database. It leverages Microsoft’s Report Builder 3.0 to run Custom Reporting against a collection of parameterized datasets that are user-defined. Custom Reporting includes sample reports with example usage against existing datasets. Users can copy and modify the sample reports or create new reports from these templates. These same ASM datasets are also available to be accessed via 3rd party business intelligence tools.

BUILT TO INDUSTRY STANDARDS
Industrial Defender ASM is built to support industry standard cybersecurity control models including those developed by the International Society of Automation (ISA-99/IEC-62443) for Industrial Automation and Control System (IACS) Logical Framework.

EASE OF DEPLOYMENT AND ROBUST SERVICE OPTIONS
Industrial Defender ASM is a vendor-agnostic solution that is easily installed in ICS footprints using existing software deployment models. No asset reboot is required. Using efficient and transparent auto discovery features helps to lessen the load of importing assets into the system.

Our qualified deployment team accelerates solution implementation to ensure efficient and optimized operation within the automation environment. A subscription service that provides ongoing product releases, support, and troubleshooting can ensure your team sees continued value and return on your investment.
INDUSTRIAL DEFENDER ASM SOLUTION ARCHITECTURE

The Industrial Defender ASM solution architecture consists of three interconnected components; Automation Systems Manager (ASM), Advanced Services Appliance (ASA), and Network Intrusion Detection System (NIDS).

- ASM can be deployed either as a dedicated 2U appliance or optionally as a Virtual Machine (VM) providing application features sets and the active dashboard.
- ASA, a 1U appliance, resides deep inside the control network, collecting information directly from ICS devices using standard communication protocols like SSH, SFTP, SNMP or through specially designed automation system agents. The ASA correlates the information, stores, and forwards it using a secure communication channel to the ASM for analysis and reporting.
- The NIDS monitors all network traffic within the control network security perimeter, enabling detection of internally generated attacks, as well as any attacks that may have circumvented perimeter defenses. NIDS includes the ability to monitor industry standard protocols used by process control systems such as Modbus TCP, DNP3, Proﬁbus, ODVA Ethernet/IP, and ICCP, and generate alarms that are sent to the ASM for logging and diagnosis.

Industrial Defender ASM is tuned to collect data from over 100+ industrial endpoints – including RTUs, IEDs, and PLCs – and report on baseline deviations, alert on priority security events, and flag policy violations.

WHY INDUSTRIAL DEFENDER ASM?

Industrial Defender ASM addresses the overlapping requirements of cybersecurity, compliance, and change management for Industrial Control Systems (ICS). Over the last decade, Leidos has developed and delivered a single unified platform to secure and manage control environments for critical infrastructure protection. Industrial Defender ASM is the industry standard for maintaining availability and reliability of critical infrastructure amid escalating cyber threats, increasing regulatory burdens, and accelerating ICS management challenges. Over 400 companies in 25 countries rely on Industrial Defender ASM solutions to configure, manage and secure their critical infrastructure while reducing costs, manage risk, and enhance operational excellence.

NEXT STEP:

Is your organization ready to increase visibility, improve situational awareness, enhance compliance and mature your ICS cybersecurity posture? Talk to a cybersecurity expert today.
ABOUT LEIDOS

Leidos is a Fortune 500® information technology, engineering, and science solutions and services leader working to solve the world’s toughest challenges in the defense, intelligence, homeland security, civil, and health markets. The company’s 31,000 employees support vital missions for government and commercial customers. Headquartered in Reston, Virginia, Leidos reported annual revenues of approximately $10.17 billion for the fiscal year ended December 29, 2017.