

Partner with Siemens & Black Duck
to Lead in Cybersecurity

X-DLM

CROSS DOMAIN LIFECYCLE MANAGEMENT

Reduce Cyber Risk.
Earn Customer Trust.
Accelerate Growth.

Electro Source's X-DLM™ operationalizes Black Duck's security intelligence within Siemens Polarion — transforming vulnerability findings into automated cybersecurity workflows that are traceable, governed, and audit-ready across your products' entire lifecycle.



Cybersecurity is no longer a cost center.
It is a profit driver.



Digital-trust leaders are 1.6x more likely than the global average to see revenue and EBIT growth rates of at least 10 percent.



Opportunity + Trust = Growth.” (from their “Building Digital Trust” framework) — emphasising that digital trust enables more innovation and growth, not just risk-mitigation.”

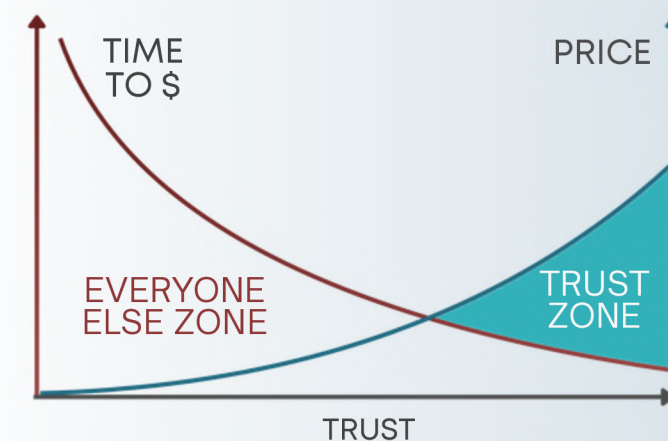


Strong cyber governance protects brand equity, enhances financial performance, and increases shareholder confidence — positioning mature security programs as a competitive advantage.

Built with the world's most trusted names in industrial software and security intelligence so you can earn customer trust, meet next-generation cybersecurity regulations, and do so cost-effectively.



THE IMPACT OF EARNED TRUST



Partnering with Siemens and Black Duck directly impacts your brand’s reputation and helps you gain trust, resulting in shorter enterprise sales cycles, rapid growth, and increased profitability. Organizations that embed best-in-class cybersecurity into their workflows outperform competitors.

TIME-TO-MARKET IMPACT

Being late to market reduces total revenue and profitability. X-DLM™ improves software design velocity by 10 - 20% while maintaining audit-readiness, and reduces late-cycle surprises through the fully-automated collaboration via LiveDocs.





The World's Most Trusted Industrial Brand Leader

Powering the most critical systems for 175 years - delivering engineering integrity, reliability, and ingenuity at global scale.



Siemens is chosen not just for its technology, but for the confidence that its systems operate with integrity in the most demanding environments.



Siemens Polarion

Application Lifecycle Management

Polarion serves as the system of record for lifecycle governance, providing end-to-end traceability from requirements through implementation, testing, issues, risks, and approvals.



Collaboration

User Dashboards, Comments, Approvals, E-Signatures



Traceability

Forensic Analysis of Who, What, Where, When, Why



Reuse

Reuse, Branch and Merge data for parallel Projects



Highest-Accuracy Intelligence Trusted by Global Security Analysts

Powered by the most comprehensive open source Knowledge Base, 317,000+ vulnerabilities, 10M+ projects, alerts 3 weeks ahead of the NVD.

Security Intelligence Only Black Duck Can Deliver



Highest Accuracy, Broadest Coverage

Detects what others miss - binaries, firmware, AI-generated code, and C/C++ without a package manager.



Malware Detection in the Supply Chain

Identifies malicious code embedded in open source components - not just known CVEs, threats other tools don't see.



Best-in-class License Compliance

3,000+ license types tracked. Flags obligations that block distribution, violate OEM agreements, or trigger IP liability before becoming a lawsuit.

Black Duck has the world's most complete repository since 2002, with 63,000+ exclusive advisories, 3.2 petabytes of intelligence. Every BDSA includes exploit evidence & direct mapping to affected components - X-DLM routes each alert automatically into a governed Polarion triage workflow.

CORE CAPABILITIES

- SCA across source, binaries, firmware & containers
- SBOM generation, import & export (SPDX / CycloneDX)
- Vulnerability identification with prioritized remediation
- License risk detection with automated policy enforcement
- Supplier risk assessment & audit-ready evidence

FEATURE

- Full visibility into every layer of your software
- Compliance-ready documentation
- Know what to fix first - no noise, no guesswork
- Stay compliant without slowing down development
- Third-party risk you can see, manage, and prove

BENEFIT

- Reduce the risk of a breach, recall, or liability
- Protect revenue in regulated markets
- Build faster with less cost and less incidents
- Keep IP clean for fundraising, M&A & enterprise sales
- Own your supply chain risk before it owns you

BLACK DUCK Security Intelligence

Most Comprehensive KnowledgeBase
Accurate results mean faster decisions and fewer resources wasted on false alarms.

BDSA Early Warning Intelligence
You see threats before they become headlines.

Exclusive Binary & Snippet Scanning
No code enters your product unexamined — including AI-generated.

Malware Detection
Know if your software has been weaponized, not just whether it's vulnerable.

SBOM Generation & Management
Meet compliance mandates & move faster than competitors who aren't ready.

License Risk & IP Compliance
Protect deal value and avoid legal exposure at every stage.

Software Composition Analysis (SCA)
Have complete visibility into what's actually in your software.

Operational Risk — Component Obsolescence
Eliminate obsolete dependencies before they become incidents.

X-DLM

Black Duck SCA - Siemens Polarion Integration

Hierarchical S/W IP view across all products

Customized Dashboards

Bespoke Remediation Workflows

PLAN SPECIFY DESIGN CODE BUILD TEST RELEASE

SIEMENS Polarion ALM



Cyber Security



Industry Solutions



Software Products



Enterprise Reuse



Regulatory Compliance



Artificial Intelligence

From Regulatory Obligation to Automated Operational Control

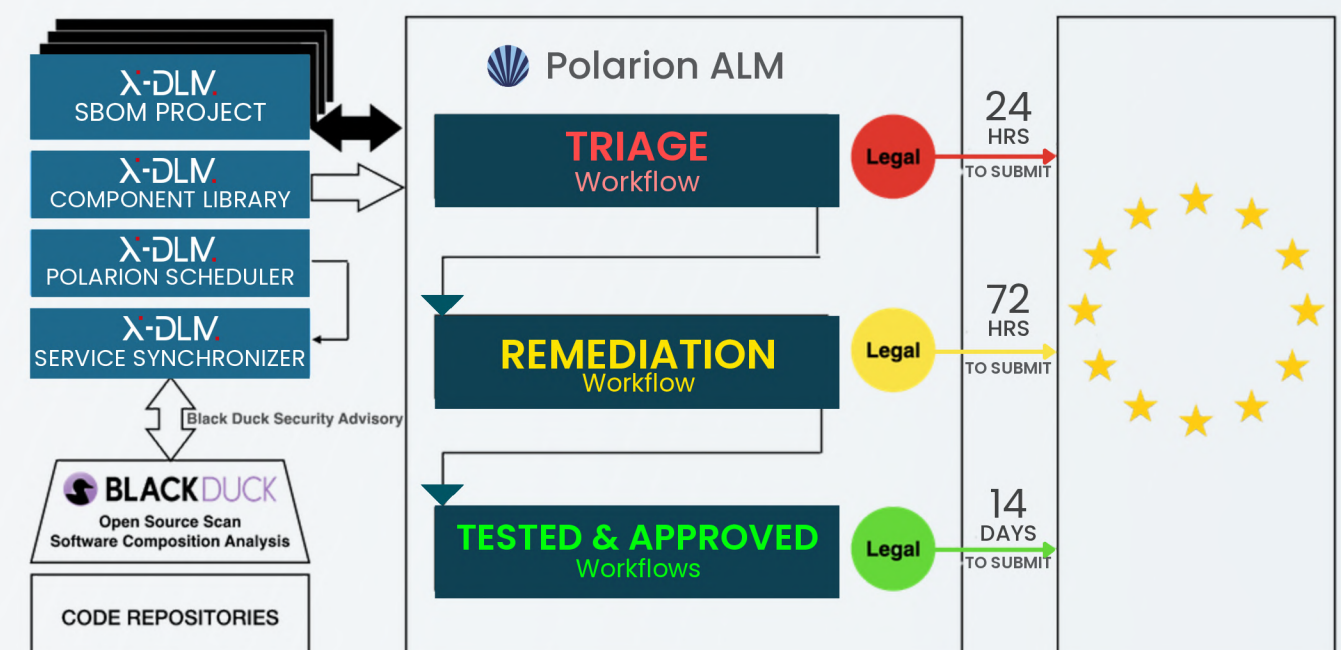


EU Cyber Resilience Act (CRA)

For All Industries

The EU CRA requires products with digital elements to implement secure development, continuous vulnerability management, strict incident timelines (24h/72h), and up to 10 years of audit-ready evidence.

X-DLM™ Bespoke EU CRA Workflow



ISO/SAE 21434 & UNECE R155/R156 (WP.29)

Automotive cybersecurity

ISO/SAE 21434 and UNECE R155/R156 (W.29) mandate systematic cybersecurity risk management for vehicles, covering development, production, operation, and post-sale monitoring.



IEC 62304

Medical Device Software Regulations

IEC 62304 and FDA 21 CFR 820 requires medical device software teams to maintain controlled development processes, risk management, change control, and long-term traceability.

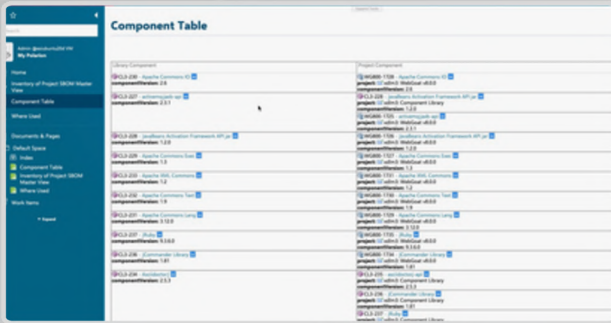


IEC 62443

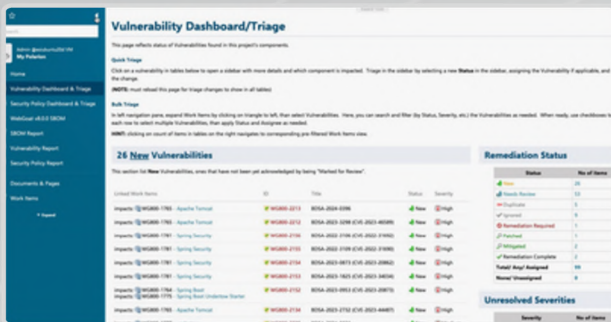
Industrial Automation and Control Systems Security

IIEC 62443 defines security requirements for industrial control systems across suppliers, integrators, and operators.

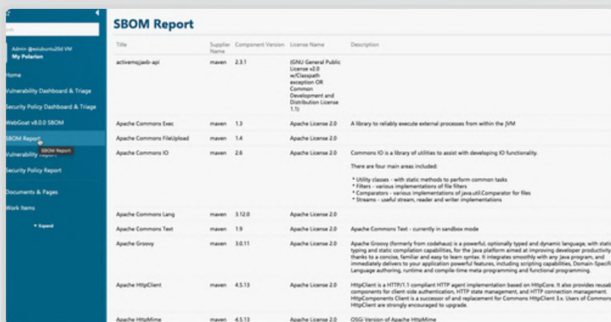
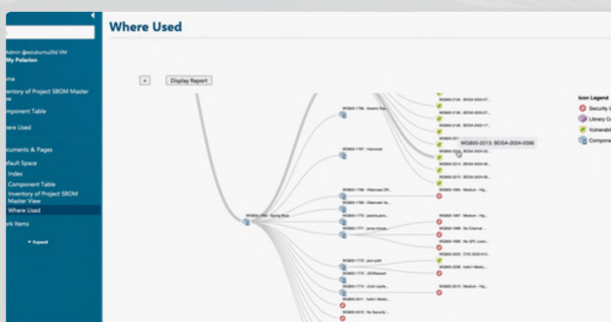
Shift from disconnected security tasks to governed, end-to-end engineering workflows.



Name	Version	Component Type
Apache Commons IO	2.11.0	Library
Apache Commons Lang	3.12.0	Library
Apache Commons Text	1.10.0	Library
Apache Commons Validator	1.0.0	Library
Apache Commons Workflow	1.0.0	Library
Apache Commons X	1.0.0	Library



ID	Title	Severity	Remediation Status
WSN-2024-0001	Apache Commons IO	High	Not Started
WSN-2024-0002	Apache Commons Lang	Medium	In Progress
WSN-2024-0003	Apache Commons Text	Low	Completed
WSN-2024-0004	Apache Commons Validator	Medium	Not Started
WSN-2024-0005	Apache Commons Workflow	High	In Progress
WSN-2024-0006	Apache Commons X	Low	Completed



Name	Version	Component Type
Apache Commons IO	2.11.0	Library
Apache Commons Lang	3.12.0	Library
Apache Commons Text	1.10.0	Library
Apache Commons Validator	1.0.0	Library
Apache Commons Workflow	1.0.0	Library
Apache Commons X	1.0.0	Library

Continuous Closed-Loop Cybersecurity Workflow

X-DLM™ delivers a unified, closed-loop governance framework that turns security findings into traceable, auditable, regulator-ready outcomes—continuously, not as one-off reports, isolated tools or manual handoffs.

Lifecycle Coverage Across Product States

X-DLM™ supports cybersecurity governance across all stages of the product lifecycle:

IP REUSE: Previously approved components and security decisions are reused with full traceability.

NEXT-GENERATION DEVELOPMENT: Continuous vulnerability monitoring and governed remediation workflows are enforced during active development.

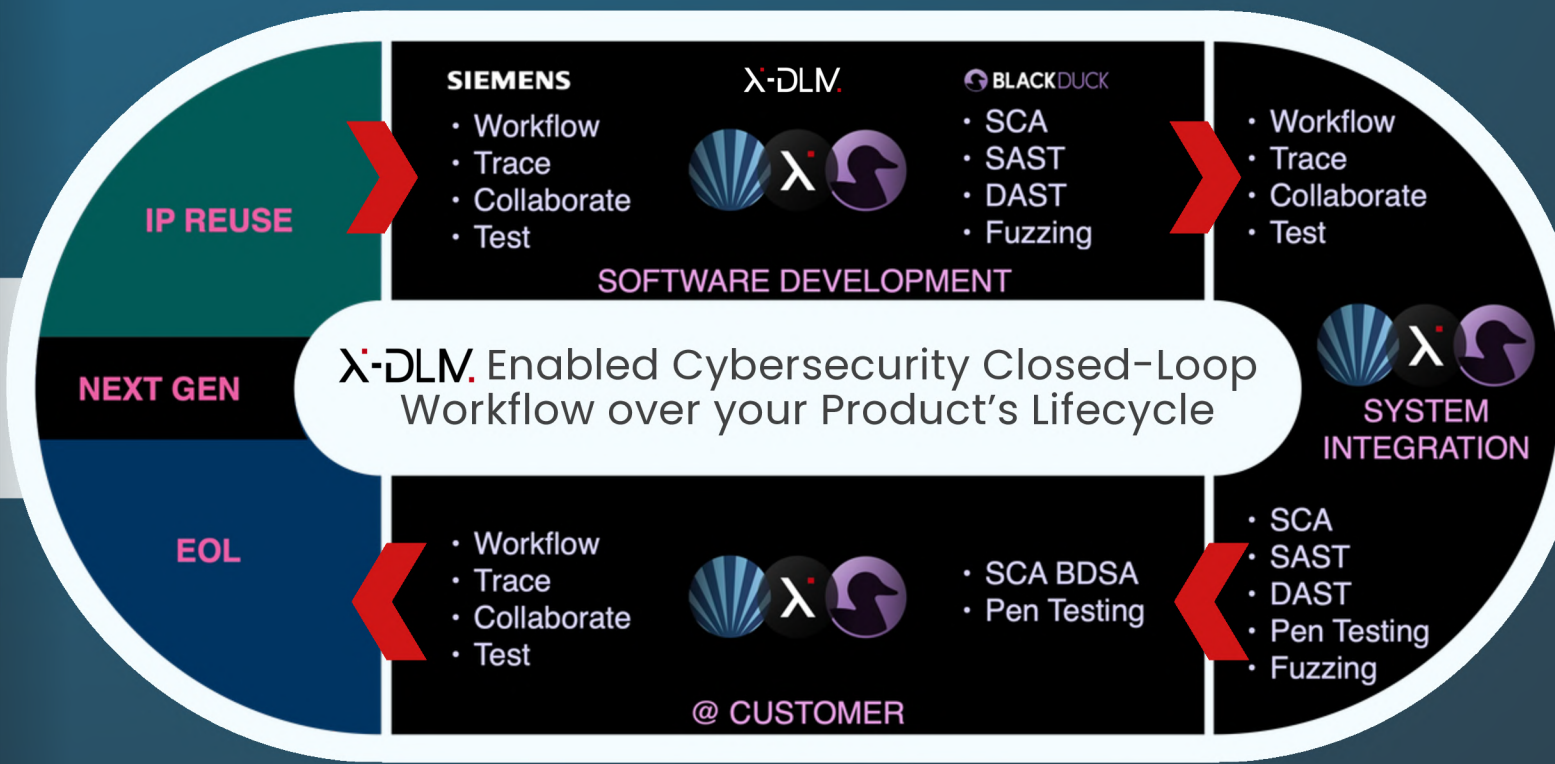
OPERATIONAL PRODUCT: Ongoing vulnerability handling, approvals, and compliance reporting are maintained post-release.

END-OF-LIFE (EOL): Residual risks, decisions, and evidence remain accessible to support audits and regulatory obligations.

Integrated Security Intelligence and Lifecycle Control

The workflow begins with vulnerability detection through Black Duck SCA and security testing. Findings are automatically ingested and synchronized into Polarion through X-DLM, where they are assessed, prioritized, and assigned ownership within governed workflows.

When combined with **Polarion LiveDocs**, collaboration creates a unified system where documentation, traceability, security scans, and approvals **automatically maintain themselves.**



POLARION Application Lifecycle Management serves as the system of record for requirements, risks, approvals, tests, and compliance workflows to ensure traceability across the lifecycle.



Cross-Domain Lifecycle Management acts as the orchestration and governance layer, synchronizing data between systems, enforcing timing and workflow controls, and capturing audit-grade evidence automatically.



Black Duck SCA continuously identifies open-source components, vulnerabilities, license risks, and compliance gaps across source code, binaries, firmware, and containers, generating accurate SBOMs and trusted security intelligence.



X-DLM™ eliminates manual compliance work, automates vulnerability-to-requirement linkage, increases engineering velocity, and gives customers instant audit-readiness.

Business Impact at Scale

Turning cybersecurity compliance into measurable business value.



Cybersecurity compliance is no longer a defensive obligation; it is a visible signal of operational maturity. By demonstrating governed security decisions and lifecycle transparency, organizations turn compliance into a measurable competitive advantage.

When governed correctly, it becomes a growth accelerator—reducing friction, increasing trust, and improving execution across the organization. X-DLM™ directly supports revenue, delivery velocity, and expansion.

Turn Your Cybersecurity Story into a Sales Differentiator



Win More Deals Faster with Built-In Trust



Turn Compliance from a Cost Center into a Growth Engine



Anchor on Market Leaders Trusted by Regulators and Enterprises



Replace Manual Effort with Governed Automated Execution



Differentiate in the Market with 100% Traceable Proof

NEXT STEPS

1

ASSESS

your current cybersecurity workflows

2

BOOK

an X-DLM walkthrough

3

SCALE

confidently across products & markets



Electro Source Inc, partners with Siemens and Black Duck to deliver an integrated cybersecurity and lifecycle governance solution for regulated software and embedded systems. Together, we enable organizations to operationalize cybersecurity compliance, reduce cyber risk, and achieve audit-ready outcomes—cost-effectively and at enterprise scale.

ELECTRO SOURCE CA

230 Galaxy Boulevard
Toronto, Ontario M9W 5R8
Phone:: +1 (416) 675-4490

ELECTRO SOURCE USA

266 Elmwood Ave, Unit 781
Buffalo, NY 14222-2202
Phone: +1 (716) 885-5902

X-DLM

©2026 Electro Source Inc. All rights reserved.
Electro Source, the Electro Source logo, X-DLM, and related product and service names are trademarks or registered trademarks of Electro Source Inc. Siemens, Polarion, and the Siemens logo are trademarks or registered trademarks of Siemens AG. Black Duck and the Black Duck logo are trademarks or registered trademarks of Black Duck Software, Inc. All other trademarks are the property of their respective owners.

Connect with
Electro Source Inc

