Built Secure. Stays Secure.

Delta Product Security Services and Solutions Brochure

DAA – Delta Application Allowlisting Solution

Delta Application Allowlisting (DAA) is an endpoint protection solution designed specifically for critical assets and OT environments. It integrates multi-layered defense, behavioral learning, and non-disruptive update capabilities to enable dynamic and precise trust management. DAA effectively prevents ransomware, malware, and lateral movement attacks, safeguarding equipment and industrial sites without interrupting operations.

CONTACT US
www.deltaww.com
security.sales@deltaww.com

Precise Trust Management

Block unknown, run only trusted.

- Only trusted applications are permitted to execute
- Applications must be verified by signature, hash, or pre-authorized whitelist
- Blocks unauthorized, unsigned, or disguised malware
- Prevents fileless attacks, DLL injection, and lateral movement

Patented Intelligent Update Mechanism

Trusted updates, no downtime.

- Automated update design without disrupting operations
- Supports tolerant mode and trusted updater lists
- Automatically recognizes legitimate application update processes without downtime
- Ensures continuous protection and uninterrupted business operation

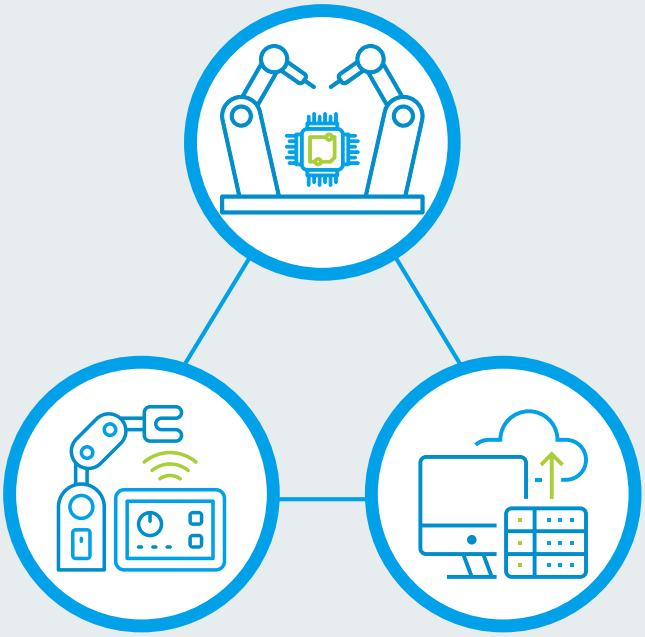
Legacy & Closed-System Support

Legacy and IoT device protection.

- Supports Windows XP / 7 / 10 / 11 / IoT and all server editions
- Deploys protection strategies without hardware upgrades
- Enhances security for devices unable to install antivirus software

Applicable Scenarios

- Legacy factory machines that cannot be upgraded
- Air-gapped environments requiring proactive defense
- Critical infrastructure/ public utilities subject to OT security audits
- 24/7 operational systems intolerant to reboot maintenance



Build device behavior profiles for early anomaly warning

Smart detection of abnormal behavior.

- Long-term learning to establish baseline models
- Detects command-line abuse, abnormal system calls, and parameter anomalies
- Provides real-time alerts and event tracing

Centralized Visual Management Platform

Unified management with full visibility.

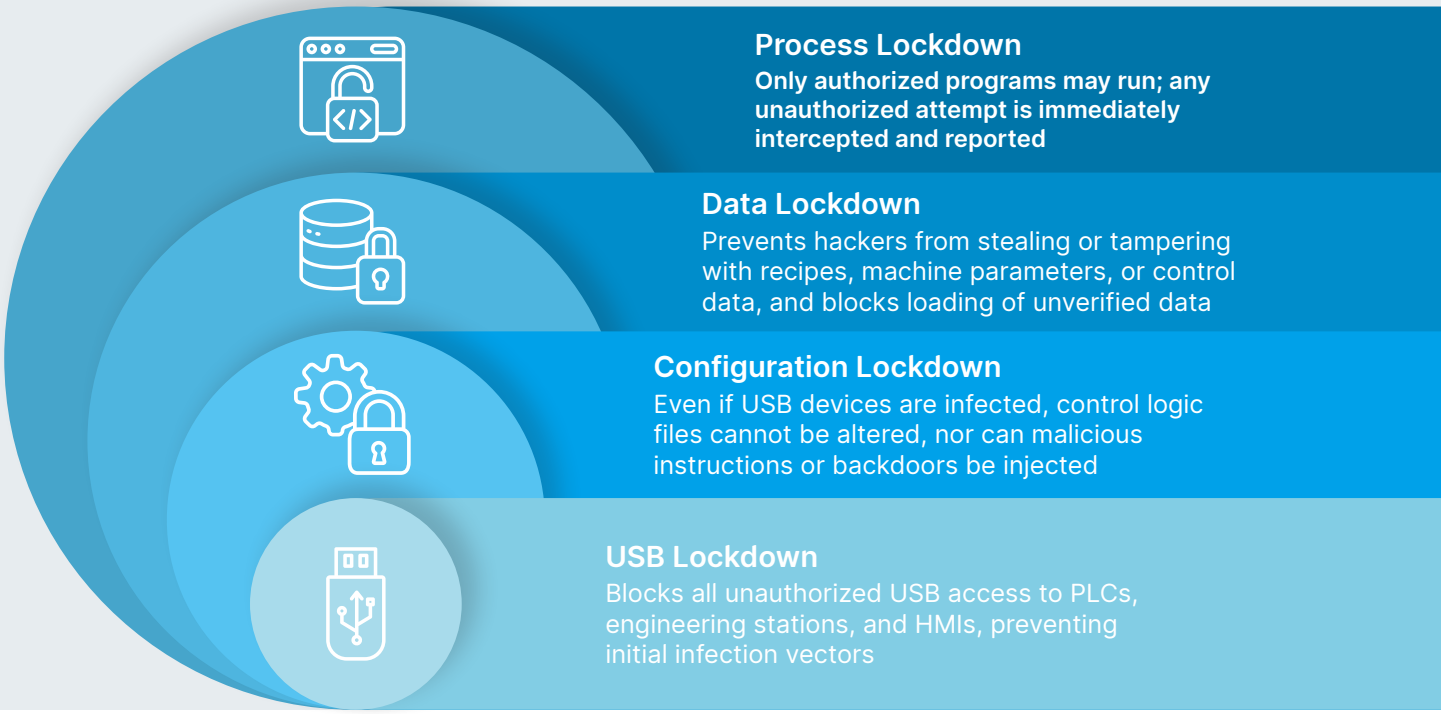
- Supports offline deployment and compliance audits
- Supports air-gapped and localized environments
- Provides dashboards, version control, and event logs

Audit & Compliance Support

Compliance with international cybersecurity regulations and standards:

- EU Cyber Resilience Act (EU CRA)
- SEMI E187 (Semiconductor Equipment Cybersecurity Standard)
- IEC 62443 (Industrial Control Systems Security)

Multi-Layer Lockdown Protection Architecture



Process Lockdown
Only authorized programs may run; any unauthorized attempt is immediately intercepted and reported

Data Lockdown
Prevents hackers from stealing or tampering with recipes, machine parameters, or control data, and blocks loading of unverified data

Configuration Lockdown
Even if USB devices are infected, control logic files cannot be altered, nor can malicious instructions or backdoors be injected

USB Lockdown
Blocks all unauthorized USB access to PLCs, engineering stations, and HMIs, preventing initial infection vectors

Minimum System Requirements

Support List

Windows	Windows XP, Windows 7, Windows 10, Windows 10 IoT,Windows 11
Windows Server	Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022

Minimum performance requirements

Processor
1 GHz or Faster

Memory
4 GB or Greater

Storage
200 MB Available

DAFA – Delta Automated Software and Firmware Analysis Solution

A Full Lifecycle Compliance Platform for Software & Firmware Security

DAFA is a comprehensive platform that integrates firmware component analysis, SBOM management, automated vulnerability monitoring, and compliance tracking. It helps manufacturers manage supply chain risks during product development, ensuring open-source license compliance and product cybersecurity governance.

CONTACT US
www.deltaww.com
security.sales@deltaww.com

A complete SBOM solution designed for product manufacturers

- Binary file analysis for SBOM generation
- Automated licensing and compliance reports
- Supports multiple SBOM international standards
- Continuous monitoring and real-time notifications
- Vulnerability analysis and prioritized remediation
- DevSecOps integration into secure workflows

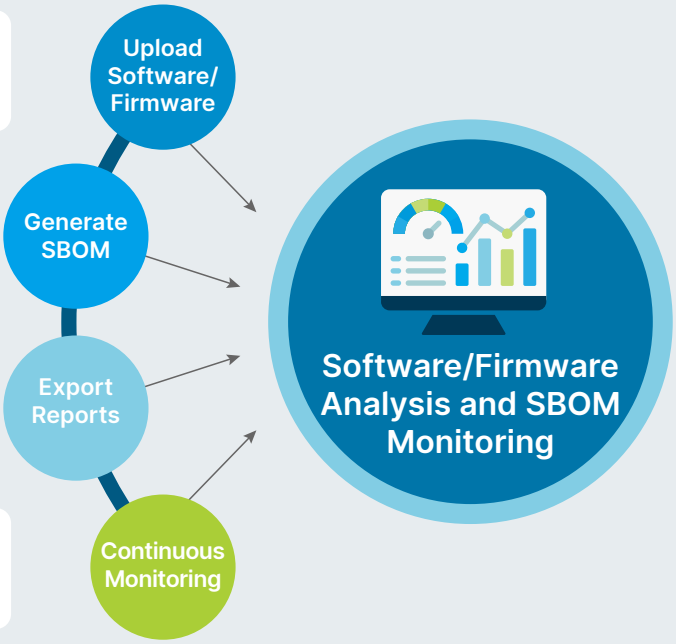
Four Steps to Complete Software & Firmware Analysis and SBOM Monitoring

Automatically unpack, reconstruct architecture, and analyze component and license information

Support SBOM generation and analyze security vulnerabilities and license compliance

Export in SPDX, CycloneDX, and other formats for auditing or third-party verification

Track new vulnerabilities in real time to safeguard supply chain security throughout the lifecycle



Automated SBOM Creation and Analysis

No Source Code? No Problem.

- Supports SBOM generation from compiled binary firmware without source code
- Automatically analyzes component versions, license types, and software architecture
- Compatible with mainstream standards such as CycloneDX and SPDX
- One-click export of complete SBOMs for third-party integration and regulatory submission

Multi-source Integration and Precise Matching

Turning SBOMs into Trusted Asset Maps

- Combines manual SBOMs, scanning tools, and third-party component data
- Builds enriched SBOMs by integrating vulnerability and license information
- Proprietary matching technology improves CVE mapping accuracy and version recognition
- Automatically includes VEX descriptions to assess real-world vulnerability impact

Vulnerability Management and Continuous Monitoring

From Passive Reporting to Proactive Defense

- Periodically scans firmware and reports the latest vulnerabilities
- Automatically categorizes severity and prioritizes real risks
- Centralized dashboard integrating alerts, remediation advice, and version history
- Reduces manual workload and enhances security response efficiency

Comprehensive SBOM Solution for Product Manufacturers

Comprehensive binary file analysis: Build a compliant SBOM without source code

Supply chain risk visibility: Instantly identify vulnerabilities, licensing, and component changes

Fastest compliance path: Easily meet EU CRA, open-source licensing, and self-attestation requirements

Support for firmware management models: Seamless adoption, suitable for OEM/ODM

Open Source Licensing and Compliance Management

Simplify Compliance, Prevent Legal Risks

- Automatically tracks open-source license changes
- One-click generation of compliance reports and audit logs
- Supports declaration generation for EU CRA and other international regulations
- Delivers complete report formats for supplier self-certification or external audits

Automated Scanning

Firmware & Software Security Posture

- Automated analysis of firmware, no manual triggers needed
- Always up-to-date SBOMs and vulnerability information
- Ensures synchronized information and continuously strengthened security posture
- Supports version comparison and anomaly detection alerts

Integrate with Existing Security Processes

Automated Security Workflow – Easier CI/CD Integration

- Natively integrates into DevOps workflows and common CI/CD tools
- Embeds security checks into the development pipeline for simultaneous delivery and security
- Streamlines processes, reducing collaboration costs between security and development teams

Product Security Compliance Services

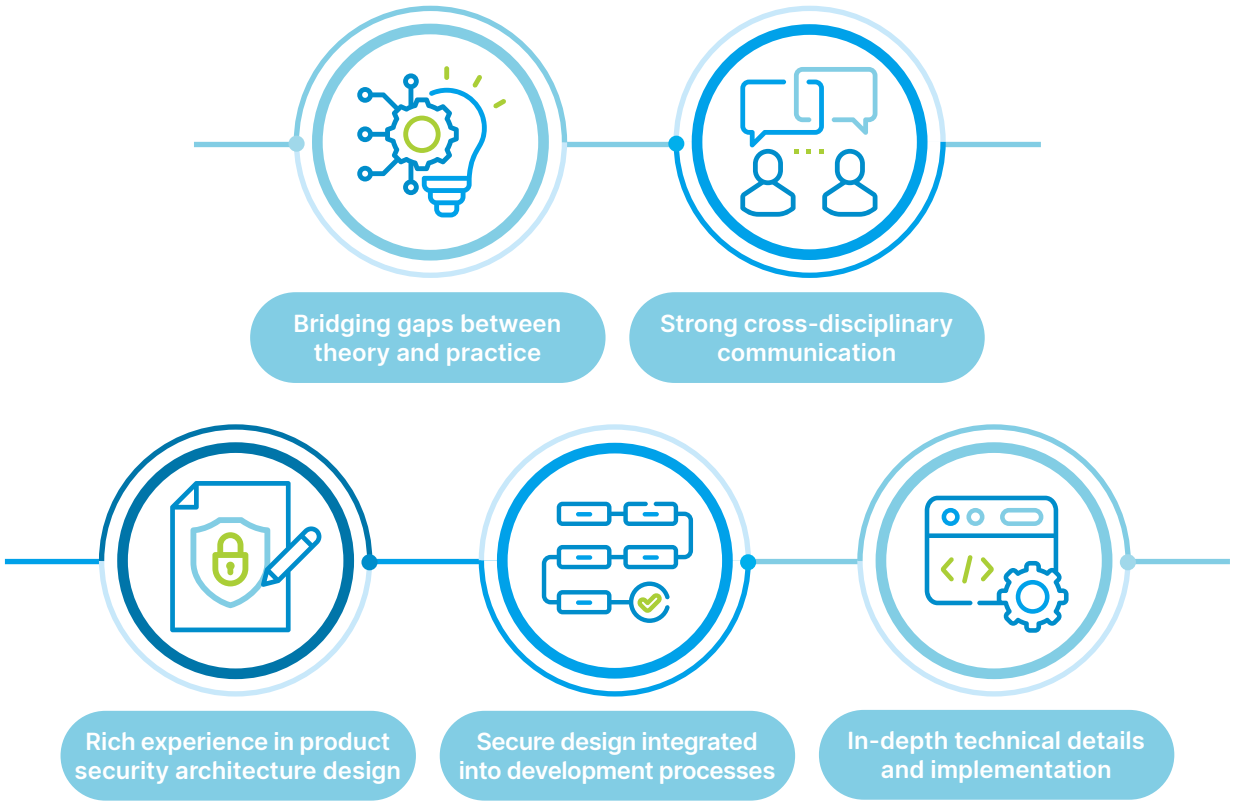
Comprehensive cybersecurity compliance aligned with international standards

Our compliance consulting team combines deep expertise in cybersecurity standards (ISA/IEC 62443, EU CRA, RED-DA, TISAX) with extensive experience in industrial control, automotive, semiconductor, and manufacturing sectors. Beyond reviews and interpretation, we deliver practical, tailored solutions that guide enterprises through auditing, implementation, and continuous operations.

CONTACT US
www.deltaww.com
security.sales@deltaww.com

Product Security Service Platform

Supporting key compliance standards to create holistic protection



IEC 62443 (IACS Cybersecurity Standard)

IEC 62443 is a series of industrial cybersecurity standards developed by the International Electrotechnical Commission (IEC), specifically designed to address the security requirements of Industrial Automation and Control Systems (IACS). Its primary goal is to help enterprises build security defense frameworks against cyberattacks and insider threats, ensuring the stability and reliability of industrial operations.

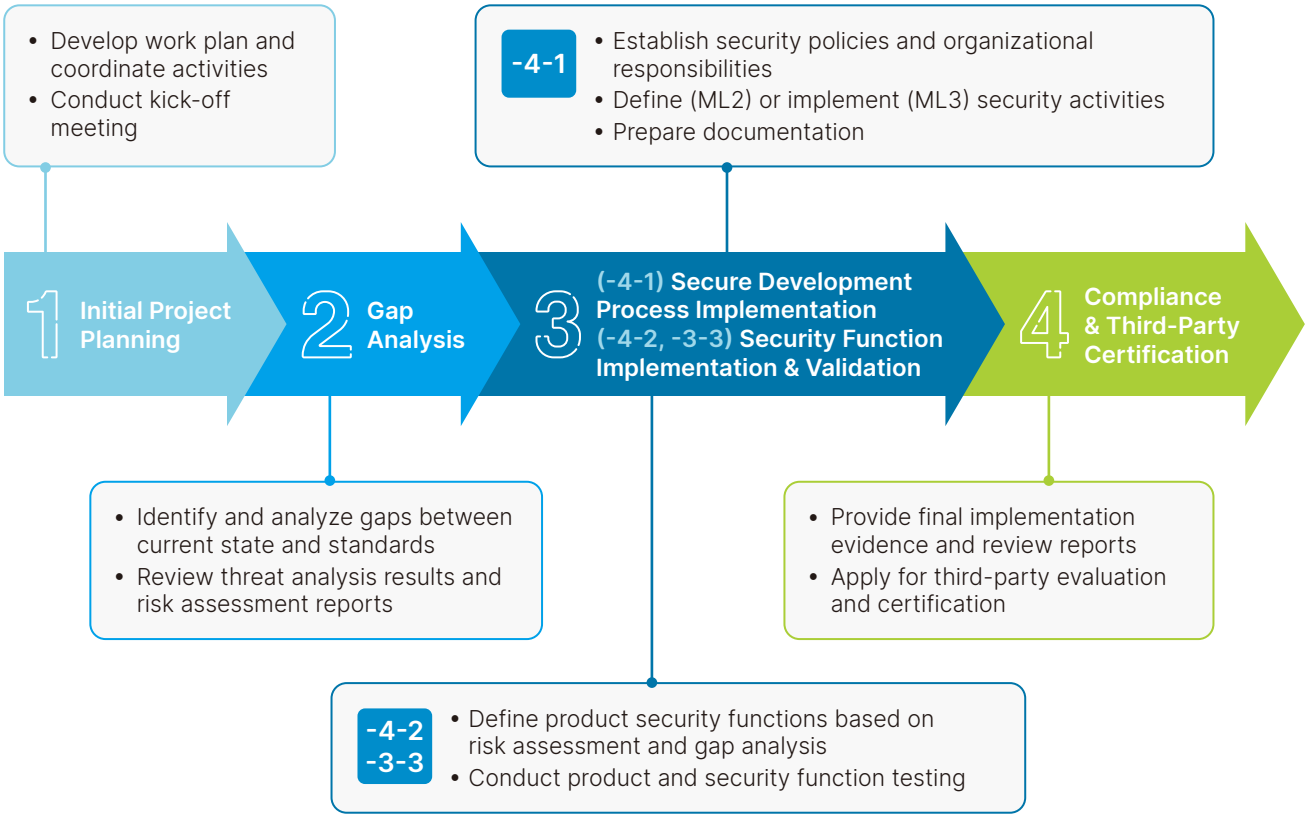
Ensure regulatory compliance to strengthen market competitiveness

Enhance product security to reduce operational and cybersecurity risks

Implement systematic security management to improve internal process efficiency

Strengthen customer trust and capture more business opportunities

IEC 62443 Compliance Project – Execution Steps



EU Cyber Resilience Act (CRA)

The EU Cyber Resilience Act (CRA) establishes unified cybersecurity requirements for digital products, covering hardware and software. Products must adopt security by design and default, complete risk assessments, and carry the CE mark. High-risk products require third-party certification. This regulation replaces fragmented standards, enhancing supply chain security and market transparency.

Supply chain security

Secure design principles

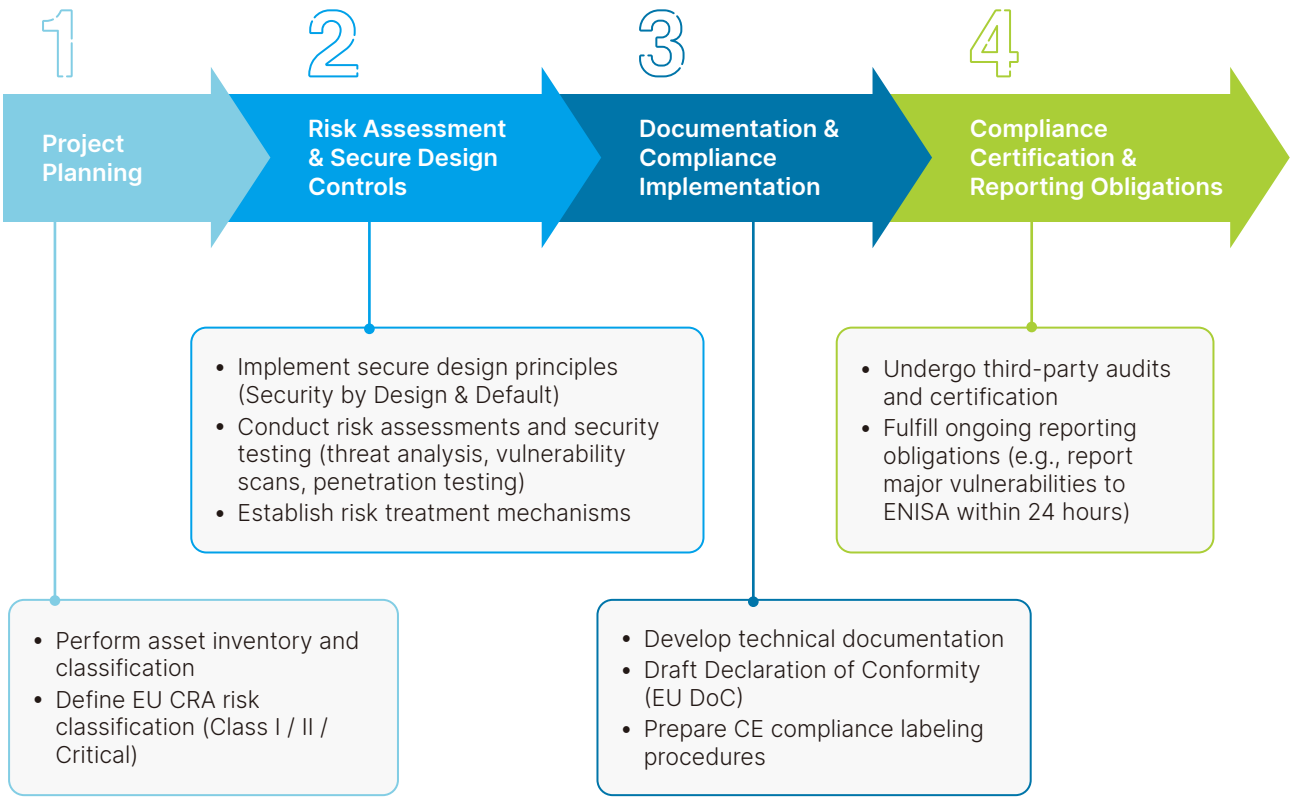
Testing & certification

Documentation management

Incident response handling

Firmware updates & vulnerability management

EU CRA Compliance Project – Execution Steps



RED-DA (Delegated Act of the Radio Equipment Directive)

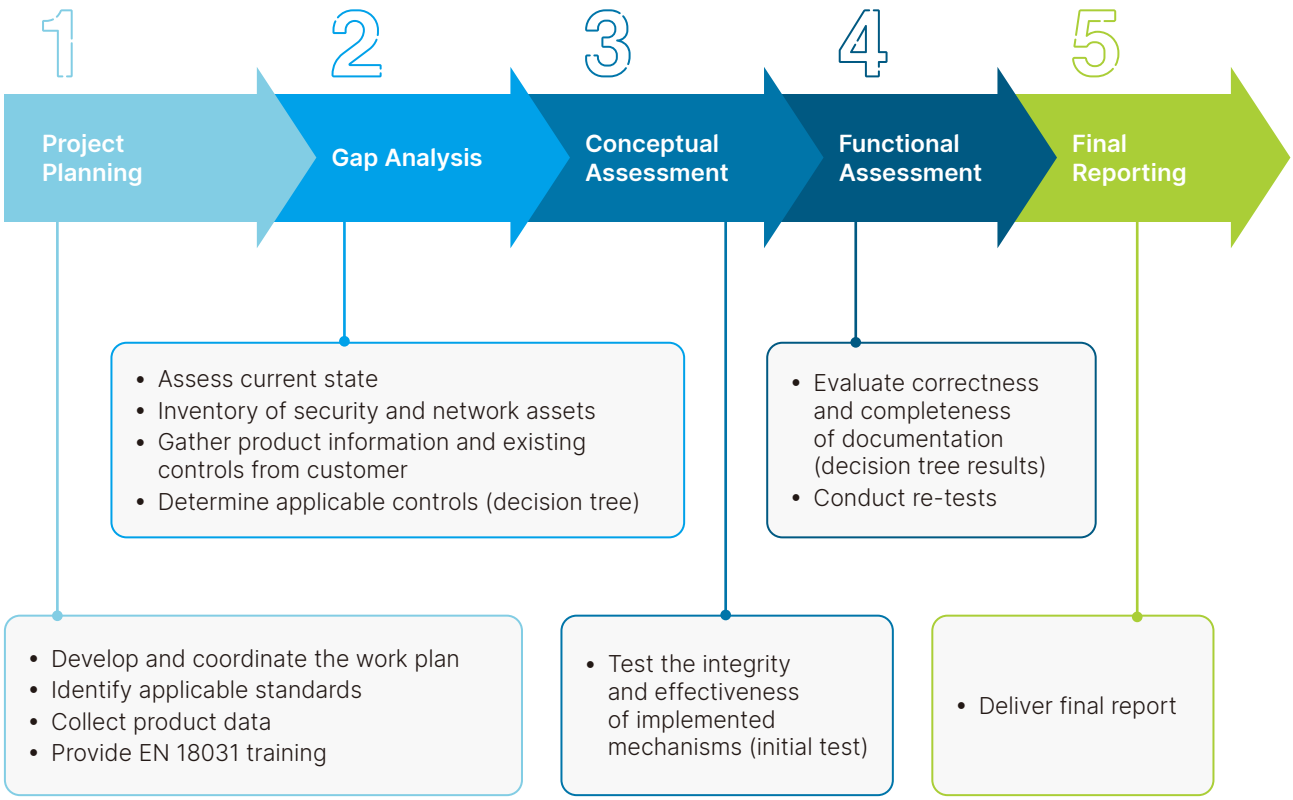
RED-DA (Delegated Act of the Radio Equipment Directive) is an EU regulation aimed at ensuring the cybersecurity of radio equipment. The focus is on connected devices, which must be capable of preventing unauthorized access and misuse of data. If products involve processing of personal or privacy-related data, enhanced data protection and privacy-by-design are required. Products supporting financial or transactional functions must implement strong encryption and authentication mechanisms. The regulation mandates manufacturers to embed security considerations at the early design stage to ensure compliance.

Article 3.3(d)
Enhance network resilience

Article 3.3(e)
Improve personal data protection

Article 3.3(f)
Reduce fraud risk

RED-DA Compliance Project – Execution Steps



TISAX (Trusted Information Security Assessment Exchange)

TISAX (Trusted Information Security Assessment Exchange), managed by the ENX Association, is an assessment and result exchange mechanism based on the VDA ISA (VDA Information Security Assessment). It verifies cybersecurity maturity and auditability across the automotive supply chain. Covering scenarios such as prototype and confidential data handling, TISAX has become a market entry requirement for European automotive OEMs, reducing redundant audits and accelerating project launches. Applicable participants include OEMs, Tier-1/Tier-2 suppliers, design, prototyping and testing service providers, as well as IT, cloud, and R&D outsourcing partners.

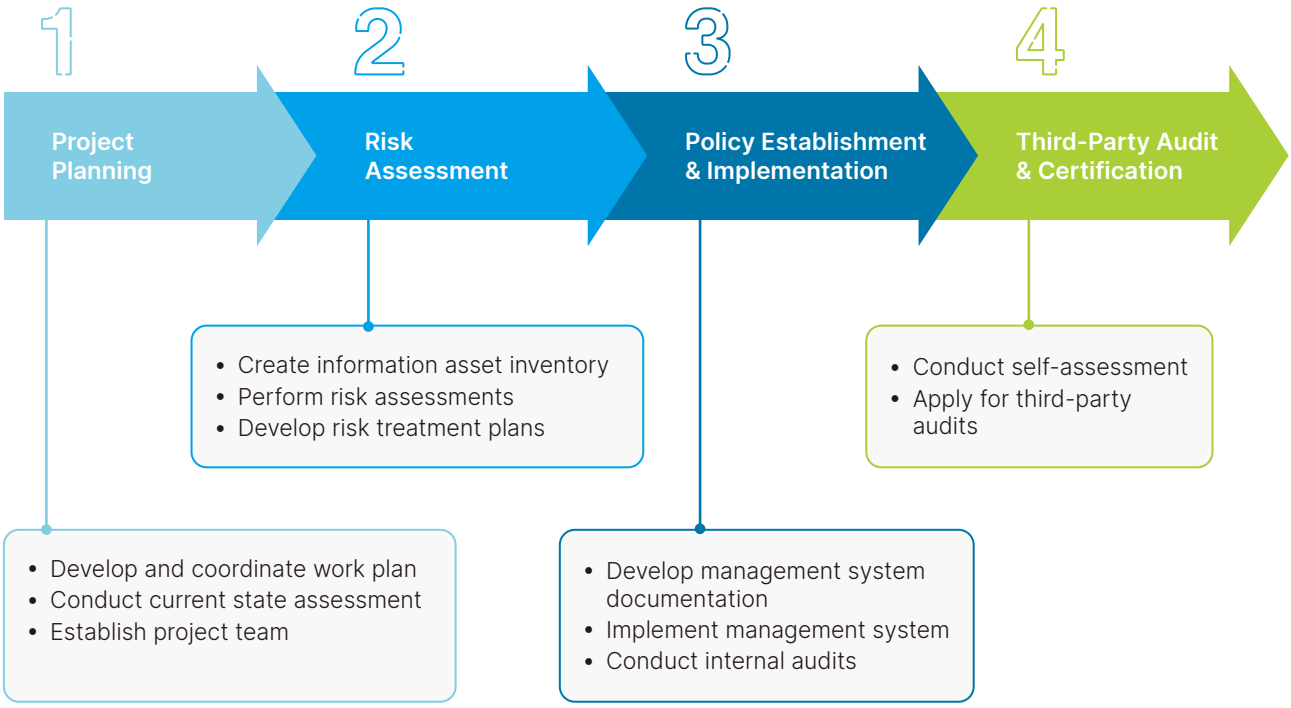
Enhanced protection of confidential and prototype data

Fast-track access to European automotive supply chains

Standardized policies, processes, records, and technical testing

Strengthened supply chain cybersecurity governance

TISAX Information Security – Implementation Steps



SEMI E187 (Specification for Cybersecurity of Semiconductor Manufacturing Equipment)

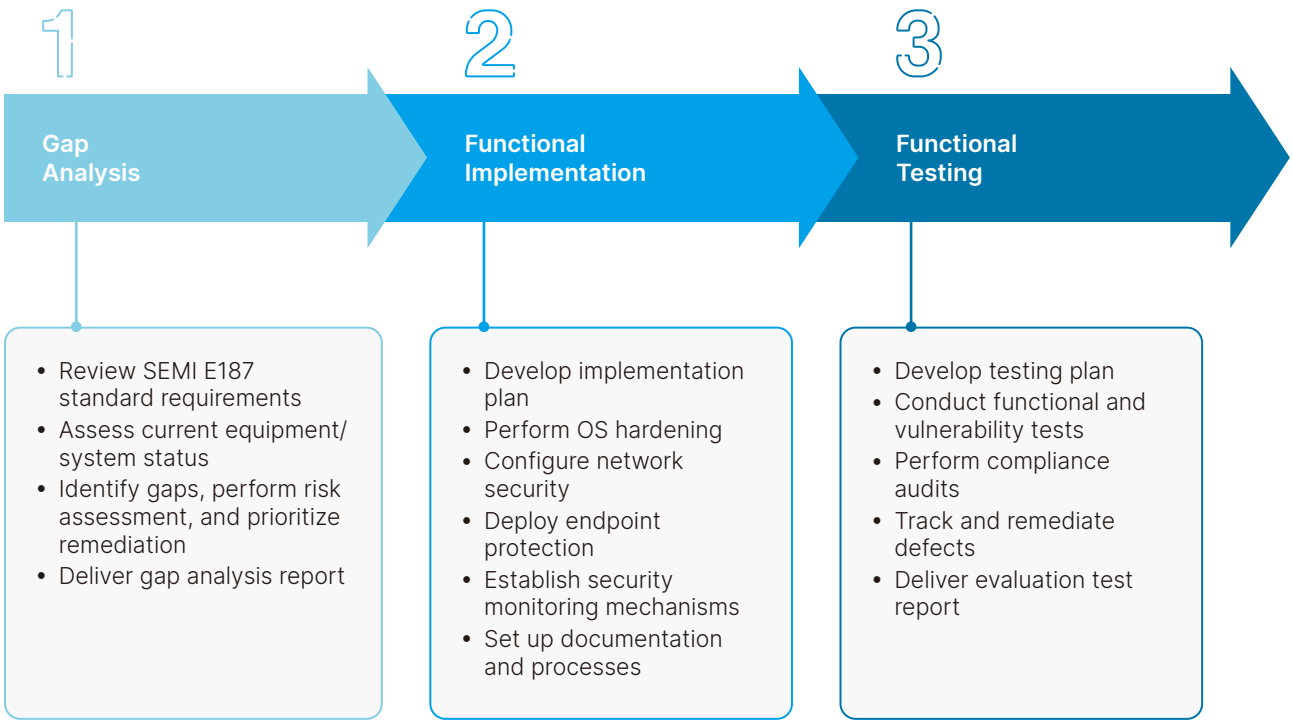
SEMI E187 defines the cybersecurity baseline for semiconductor manufacturing equipment, covering OS hardening, network segmentation/encryption, endpoint protection, and logging/monitoring, following an OT zero-trust approach. It applies to wafer fab equipment based on Windows or Linux platforms. Its adoption enables standardized delivery across fabs, reduces cybersecurity risks, and strengthens customer trust.

Standardized cybersecurity for manufacturing tools

Reduced potential cybersecurity risks in equipment

Enhanced equipment security and operational resilience

SEMI E187 – Implementation Process



Delta Product Security Assessment Services

Delta's security assessment services combine attacker perspective with compliance validation, turning risks into actionable engineering tasks. Through threat modeling, vulnerability scanning, penetration and fuzz testing, we identify critical risks and real-world impacts. For OT, ICT, automotive, and semiconductor environments, we deliver contextual test scenarios, risk scoring, attack path mapping, prioritized remediation, and retesting. All results are aligned with IEC 62443, EU CRA, RED-DA, TISAX, SEMI E187, and custom criteria, supporting compliance for market launch and audits. Findings integrate back into R&D and operations (SDL, SBOM, vulnerability management) to strengthen product security with minimal overhead.

CONTACT US
www.deltaww.com
security.sales@deltaww.com

Product Security Service Platform

Product Security Assessment Services

Comprehensive testing to accurately uncover vulnerabilities

- Threat Modeling & Risk Analysis
- Vulnerability Scanning
- Fuzz Testing
- Penetration Testing

International Standard Alignment

- EU CRA (Cyber Resilience Act)
- RED-DA (Radio Equipment Directive – Delegated Act)
- IEC 62443 (Industrial Control Security)

Advanced Security Testing Services

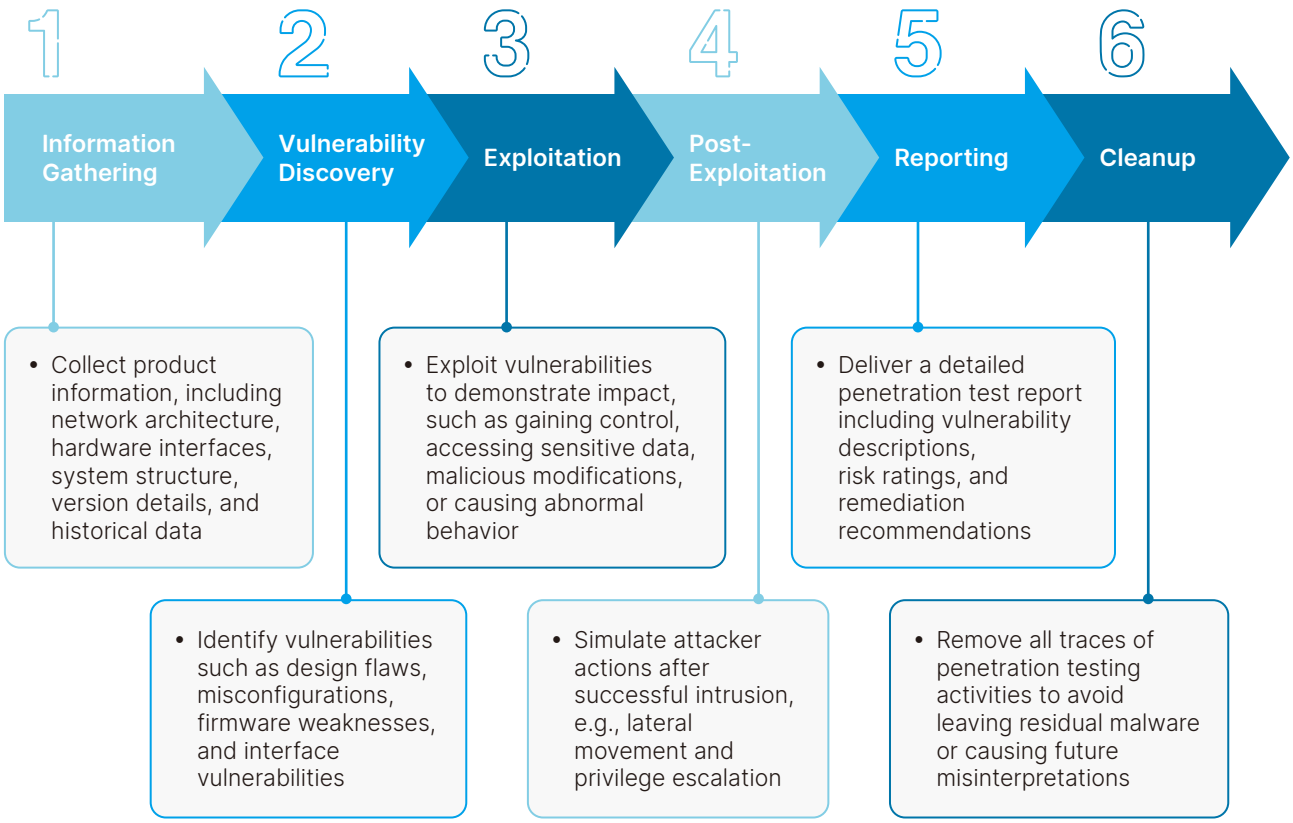
- ISO/IEC 17025 accredited cybersecurity lab
- Tailored testing programs for different industries
- Support enterprises in establishing secure product development lifecycles
- Compressive security testing to keep products at their highest level of security

Penetration Testing

Penetration testing focuses on attack paths, using techniques such as lateral movement, privilege escalation, and logic manipulation to evaluate OT assets. By conducting comprehensive intrusion attempts across product hardware, interfaces, firmware, software, services, and communications, we identify exploitable vulnerabilities and attack vectors—helping to prevent security incidents and mitigate potential major losses.

- **Meet cybersecurity standards**
- **Expert in OT & embedded testing**
- **Simulate real-world cyberattacks**
- **Help identify high-risk vulnerabilities**
- **Design security into products**
- **Validate defense effectiveness**

Penetration Testing Services – Implementation Process

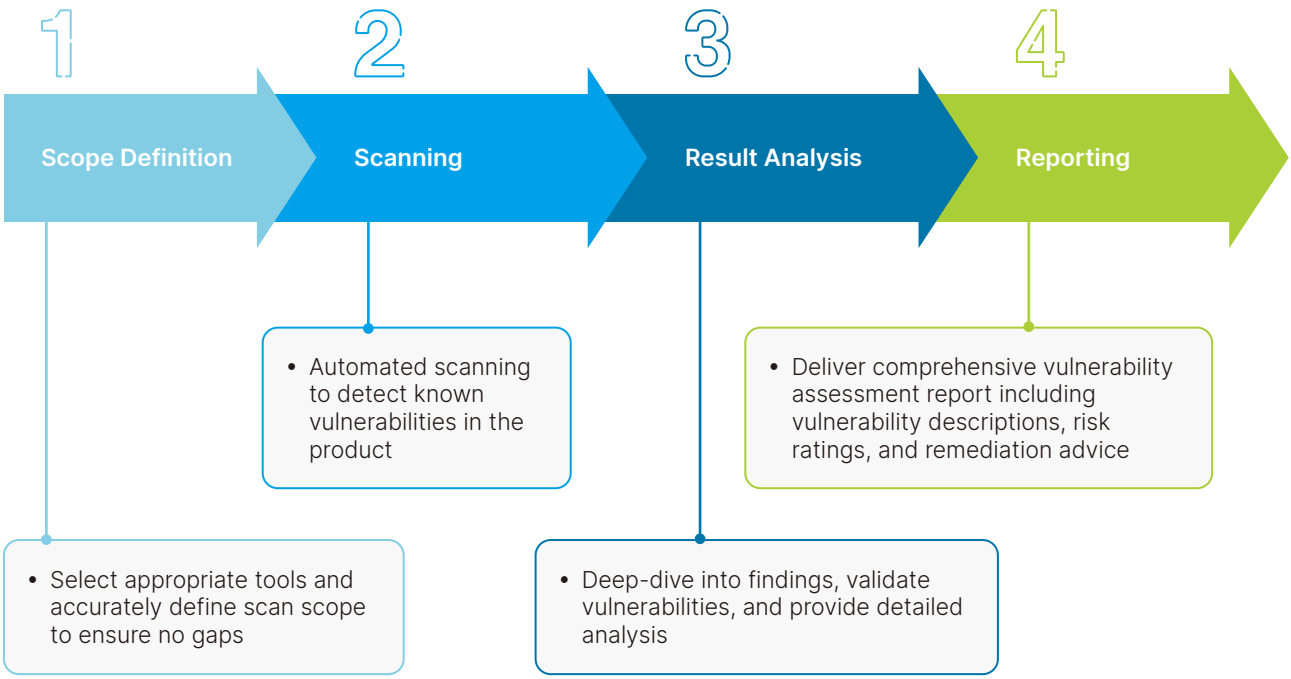


Vulnerability Assessment

Vulnerability assessment uses automation to quickly identify known vulnerabilities, misconfigurations, outdated components, weak passwords, and unnecessary open services. The process is low-impact and non-destructive. Upon completion, a list of issues, risk ratings, and remediation recommendations are provided. Retesting and scheduled periodic scans can be arranged to continuously raise the baseline of cybersecurity. This service applies to websites, hosts, applications, and similar products.

- **Cost-effective solution**
- **Meets regulatory and certification requirements**
- **Significantly reduces risk and potential damages from incidents**
- **Easily repeatable for periodic execution, raising security baseline**
- **Product-oriented security assessment expertise**

Vulnerability Assessment – Implementation Process

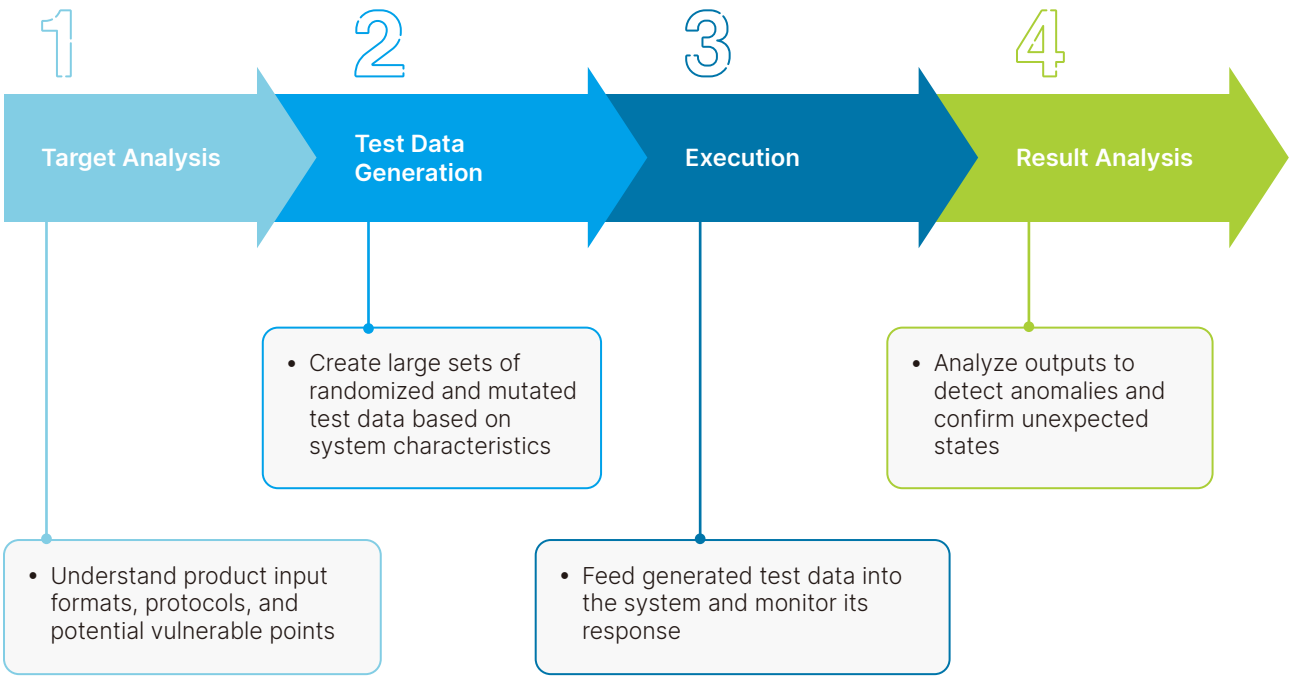


Fuzz Testing

Fuzz testing is an automated or semi-automated evaluation service focusing on product reliability and security. By sending a large volume of malformed or unexpected inputs to the target system, it monitors whether the product enters abnormal states, revealing hidden vulnerabilities that could impact stability and security. Fuzz testing is applicable to general hosts, automotive systems, and networking products.

- **Identifies vulnerabilities missed by traditional scans**
- **Validates fault tolerance and resilience of devices/systems**
- **Improves protocol and parser security**
- **Supports automated testing**
- **Enhances secure coding quality**
- **Accelerates product security validation and compliance readiness**

Fuzz Testing – Implementation Process



PVM : Intelligent Risk Management Platform for Product Security

PVM integrates global threat intelligence, continuous vulnerability monitoring, and risk prioritization. It supports mainstream SCA tools and multiple file formats (Black Duck CSV, Jenkins XML, custom Excel). It helps enterprises throughout the product lifecycle, from risk identification to proactive decision-making, achieving efficient compliance and comprehensive vulnerability tracking.

CONTACT US
www.deltaww.com
security.sales@deltaww.com

Product Security
Service Platform

From Monitoring to Decision-Making, Powering CRA Compliance Success

Continuous Monitoring – 24/7 Global Risk Radar

- Real-time sync with top intelligence sources (NIST, CISA, FIRST)
- Version-level analysis to avoid false positives
- Customized threat insights, enabling proactive defense
- Complete audit trails for compliance

Smart Decision-Making – Security Command Center

- Focus on <10% critical risks with attack scoring
- Real-time team collaboration and progress tracking
- Actionable remediation recommendations
- Knowledge base with accumulated fixes

Automated Compliance – One-Click Regulatory Response Center

- Digitalized CRA compliance workflows
- Automatic report generation (CRA appendices, VEX, etc.)
- Professional services for complex cases

PVM Value Proposition

- Beyond NIST integration, PVM consolidates CISA, FIRST, and multiple intelligence sources to manage third-party component vulnerabilities, significantly reducing compliance preparation time.
- Eliminates long vulnerability lists with automated prioritization, allowing development teams to focus on truly critical risks.
- Supports mainstream SCA and CI/CD tools without changing existing workflows, reducing overall costs.
- Predicts potential risks by analyzing attack trends, preparing defenses before threats materialize.

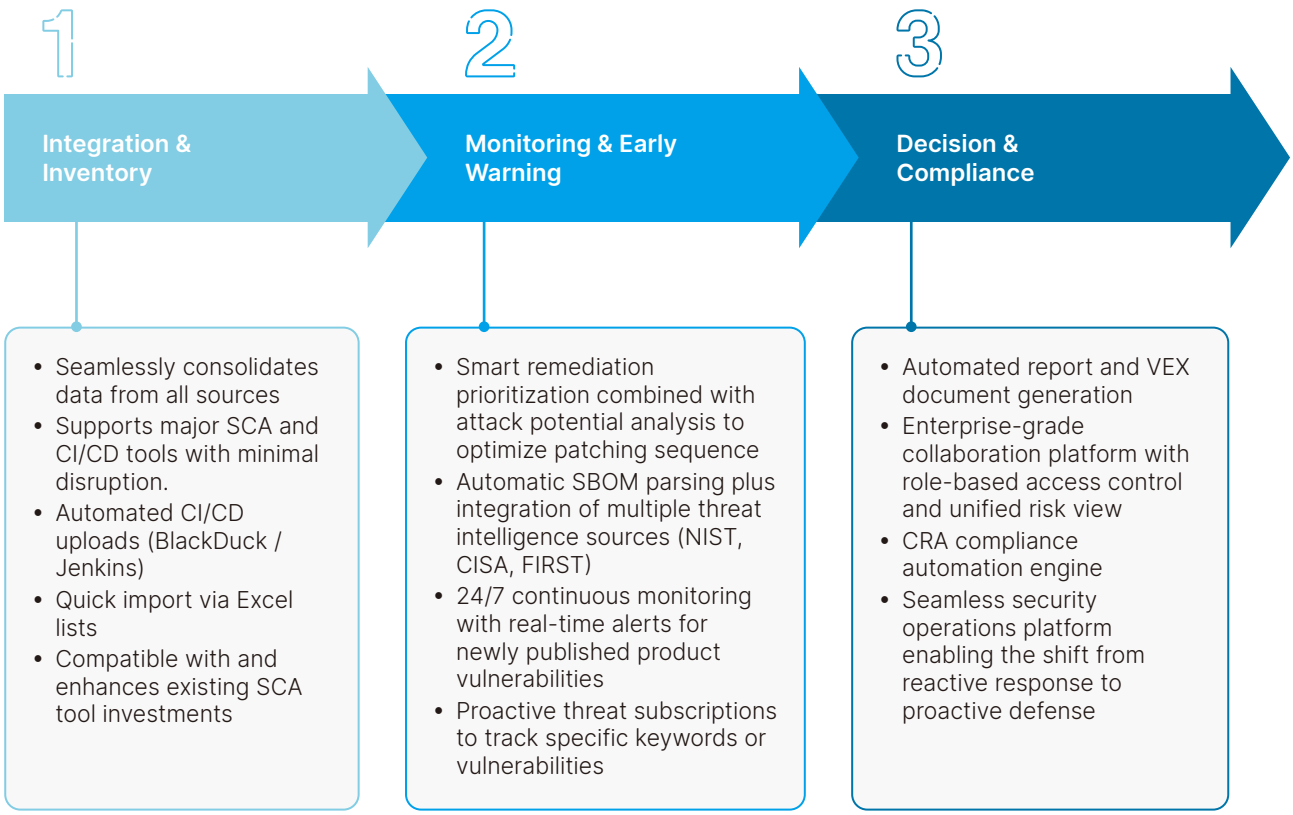
CRA Compliance Automation Engine

Smart Remediation Navigation

Seamless Security Operations Platform

From Reactive Defense to Proactive Protection

PVM Solution: The Three Pillars of Product Security



www.deltaww.com

No. 186, Ruiguang Rd., Neihu District, Taipei City 114501
Taiwan Corporate Headquarters
TEL: +886-2-8797-2088 FAX: +886-2-8797-2120