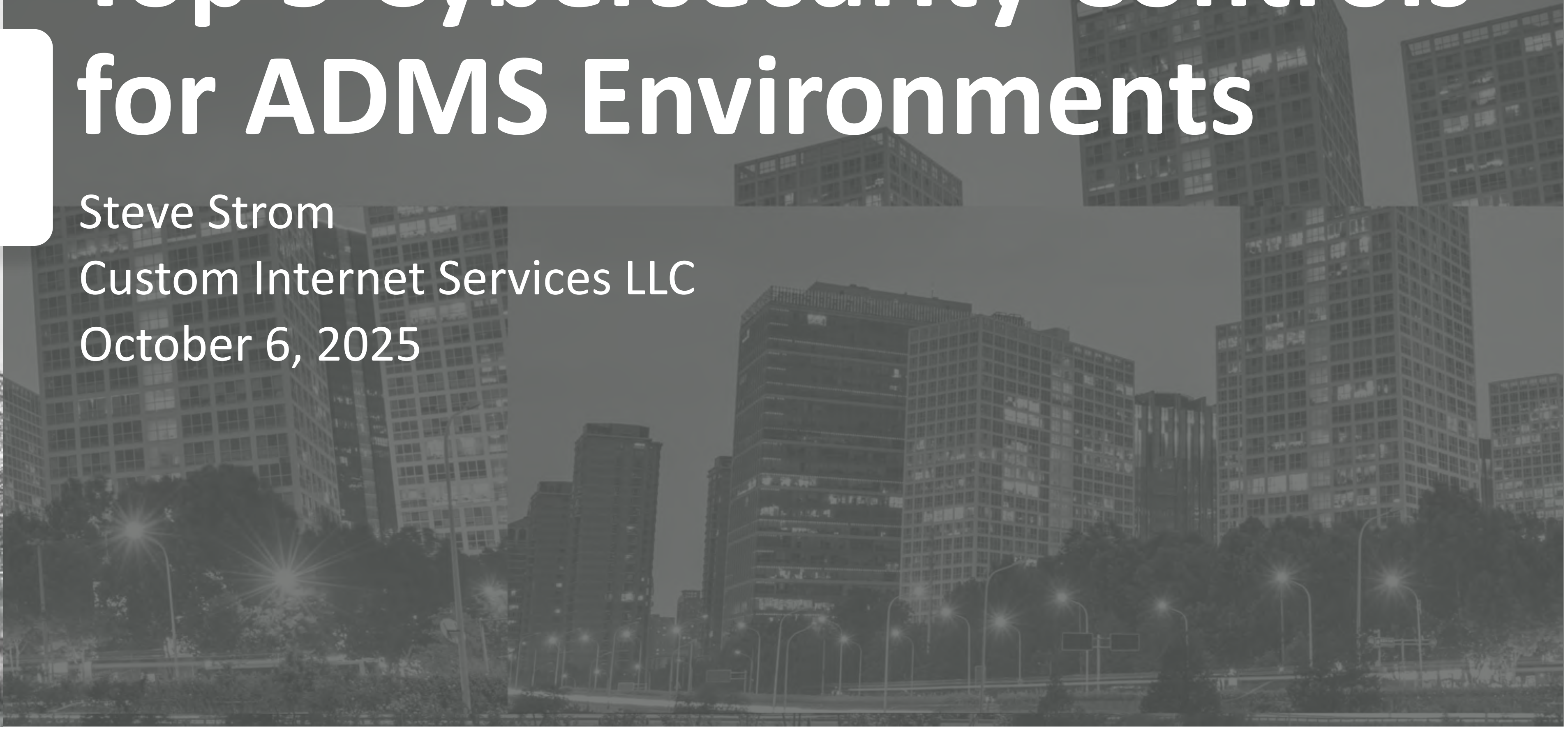
Survalent.

Top 5 Cybersecurity Controls for ADMS Environments

Steve Strom
Custom Internet Services LLC

October 6, 2025



Why Security Matters

Increasing attacks on OT/ICS systems.

Ransomware attacks up 87% over previous year.

25% of ransomware incidents resulted in full OT/ICS shutdown.

22% of advisories were network exploitable and perimeter facing in 2024.

Increase in cyber operations from geopolitical tension.

Affects both safety & reliability.

All statistics from Dragos 2025 Year in Review (www.dragos.com).

IT vs. OT: Different Risks

- IT Goals: Confidentiality, Integrity, Availability.
- OT Goals: Safety, Reliability, Availability.
- Long hardware lifecycle (10-20 years or longer).
- Proprietary protocols (DNP3, IEC61850).
- Legacy systems with limited patching.
- Increasing IT/OT Convergence = Bigger Attack Surface.

Introducing the CIS Critical Security Controls

Developed by CISecurity.org (non-profit).

Prioritized set of 18 best-practice security safeguards.

Widely adopted across industries, including OT.

Roadmap from basic cyber hygiene to advanced defense.

Complements compliance mandates like NERC CIP.

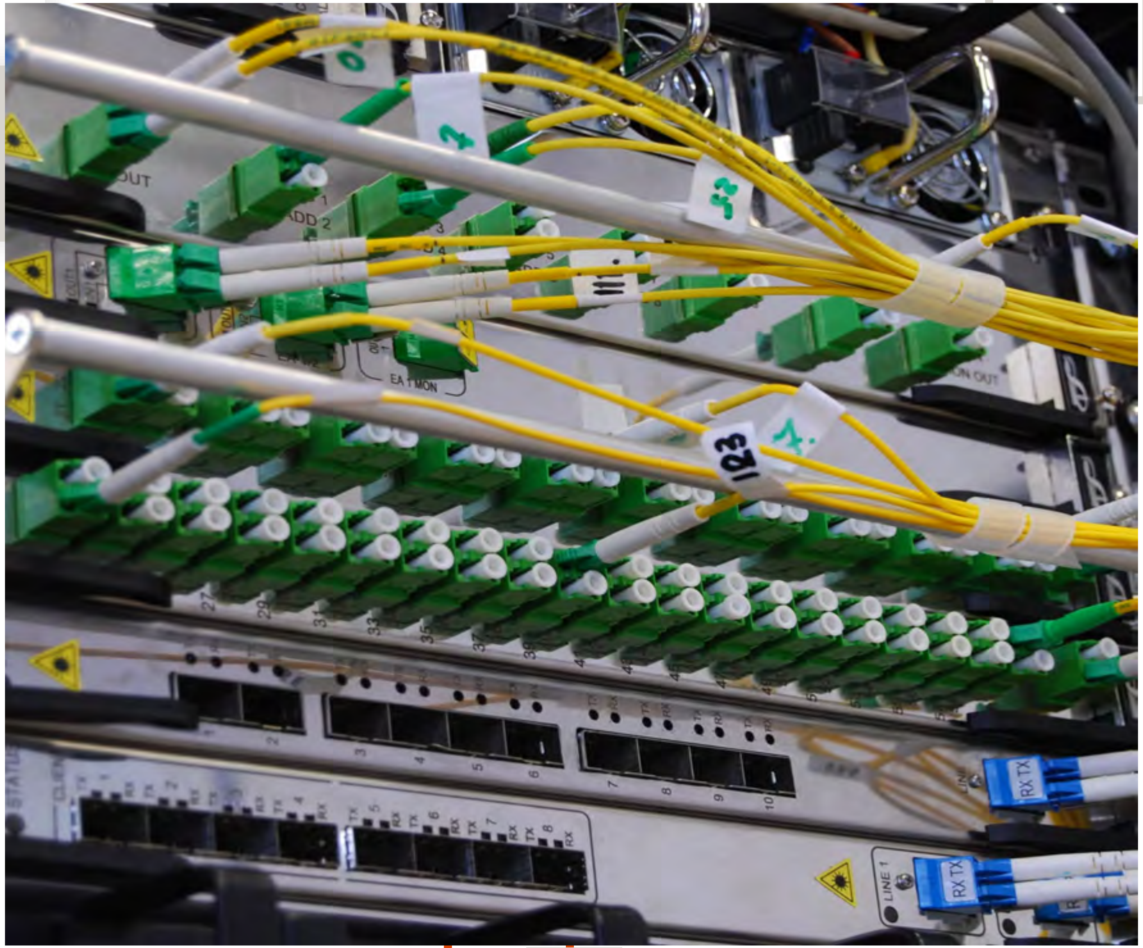
CISecurity has mapping document of Critical Security Controls to NERC CIP.

Our Focus Today

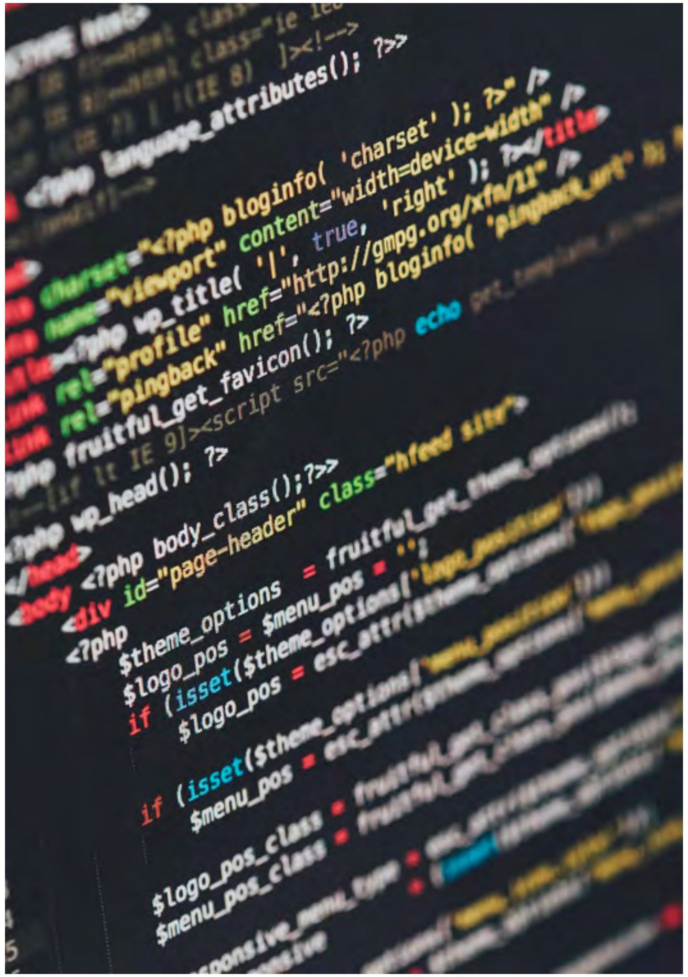
- Control 1: Inventory of Assets.
- Control 2: Inventory of Software.
- Control 3: Vulnerability Management.
- Control 4: Secure Configuration.
- Control 5: Account Management & Access Control

Control 1: Inventory of Assets

- Risk: Rogue/untracked devices are blind spots.
- Action:
  - Discover devices.
  - Baseline devices.
  - Monitor devices.
- How?:
  - Physical discovery.
  - Passive network monitoring.



Control 2: Inventory of Software Assets



- Risk: Unauthorized or outdated apps & firmware => exploitable!
- Action:
  - Track software, firmware, patch levels.
  - Upgrade when possible.
  - Wrap additional controls when patching not possible.
- How?:
  - Physical discovery.
  - Computer software monitoring tools.

Control 3: Vulnerability Management

- Problem: Patch windows limited, patches not available.
- Risk: Exploitable flaws if left unmanaged.
- Actions
  - Monitor vulnerability notices from vendors, ISAC’s, NVD, others.
  - Patch when possible.
  - Upgrade hardware when needed.
  - Use ‘virtual patching’ or compensating controls when patching delayed or impossible.

Control 4: Secure Configuration

- Risk: Default settings are an easy target.
- Actions (partial list)
  - Change passwords.
  - Build secure network architecture.
  - Enforce baselines.
  - **Implement secure remote access.**
  - Control change.
  - Pen test network.

Control 5: Account Management & Access Control

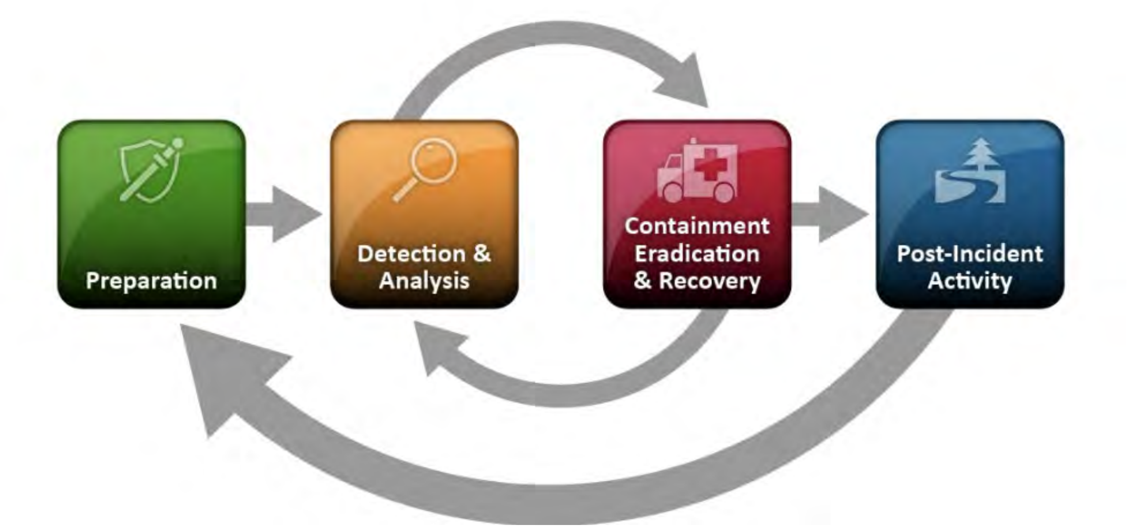
Risk: Weak authentication => High risk.

Actions

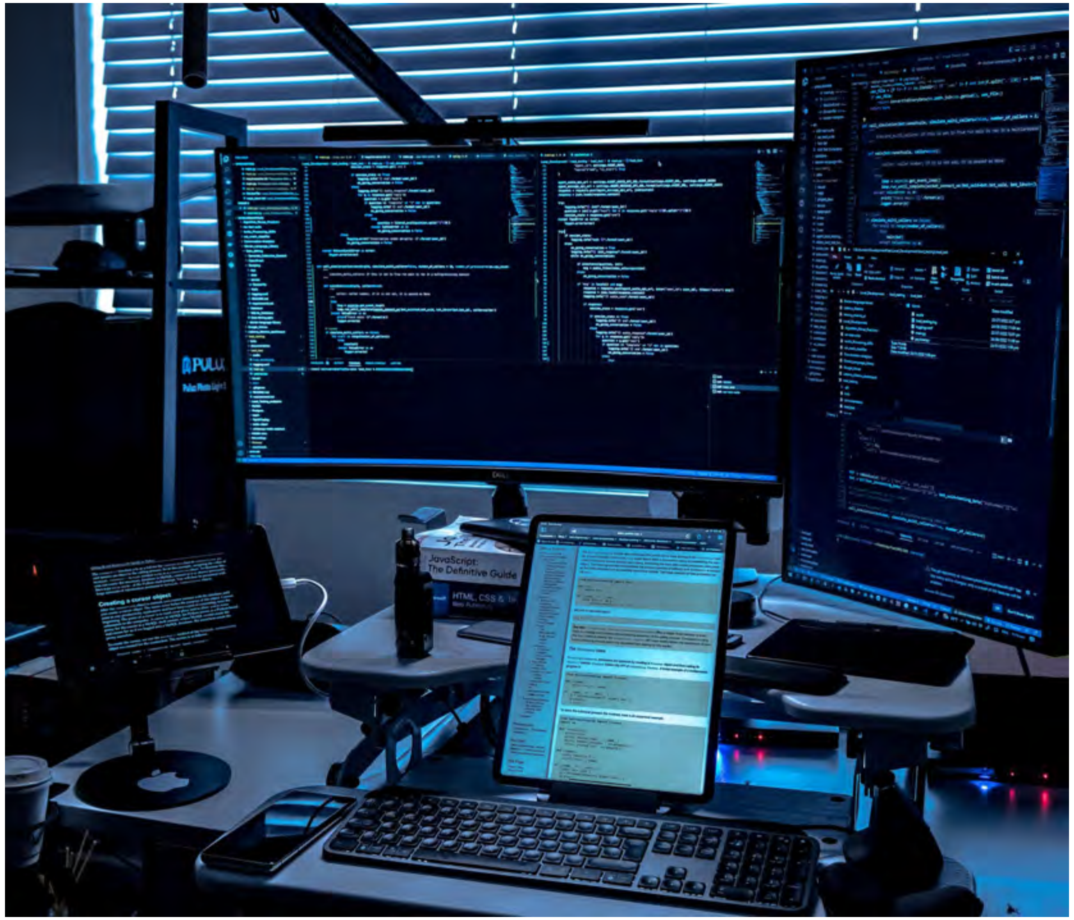
- Use unique accounts with strong passwords.
- Implement least privilege.
- When possible, remove shared accounts.
- Apply network segmentation
- Implement MFA where possible.

Incident Response Planning (Overview)

- Why it matters
  - People depend on your service.
  - Incidents will happen.
- Core Reference: NIST SP 800-61r3



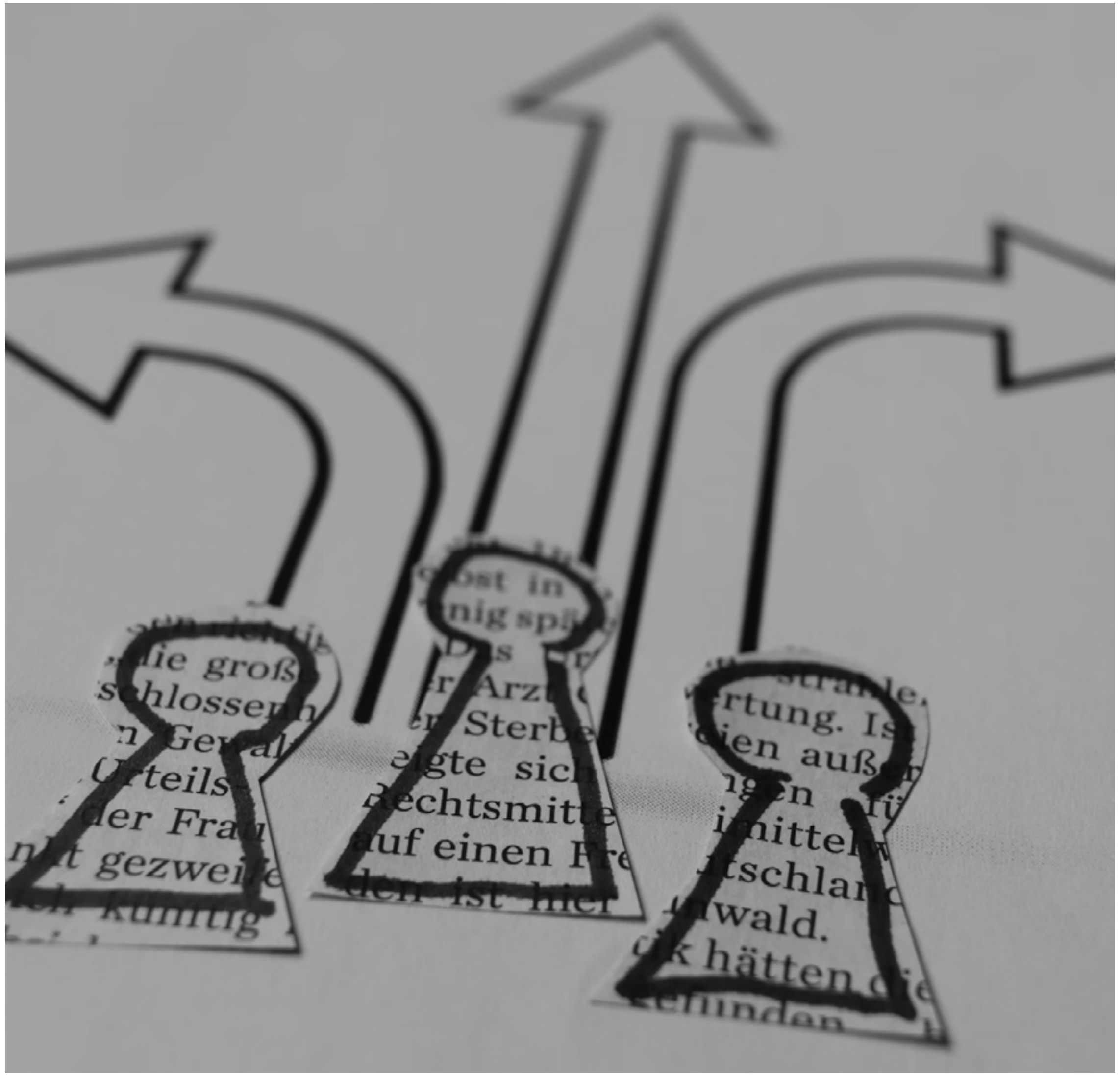
Core IR Lifecycle



- Preparation.
- Detection & Analysis.
- Containment, Eradication & Recovery.
- Post-Incident Activity, Lessons Learned

Key Takeaways

- SCADA/ADMS Security = safety & reliability.
- Cyber incidents will occur.
- CIS Controls: Practical, proven safeguards.
- CIS Controls map to NERC CIP compliance.
- Start with **asset visibility → mature to IR readiness**.
- Small, steady steps create resilient operations.



Questions?

Survalent.

Top 5 Cybersecurity Controls for ADMS Environments

Erik Wolf

VP, Software Development

Survalent

Software Authenticity = Genuine Updates

Secure Distribution

Software downloads are protected with MD5 and SHA-256 hash values that you can verify. Our managed file transfer system uses reverse proxy technology and encryption to secure the entire distribution process.

Digital Signatures & Verification

Every software build and patch is digitally signed using DigiCert certificates. This cryptographic signature acts like a tamper-evident seal, ensuring the software hasn't been modified by unauthorized parties during distribution.

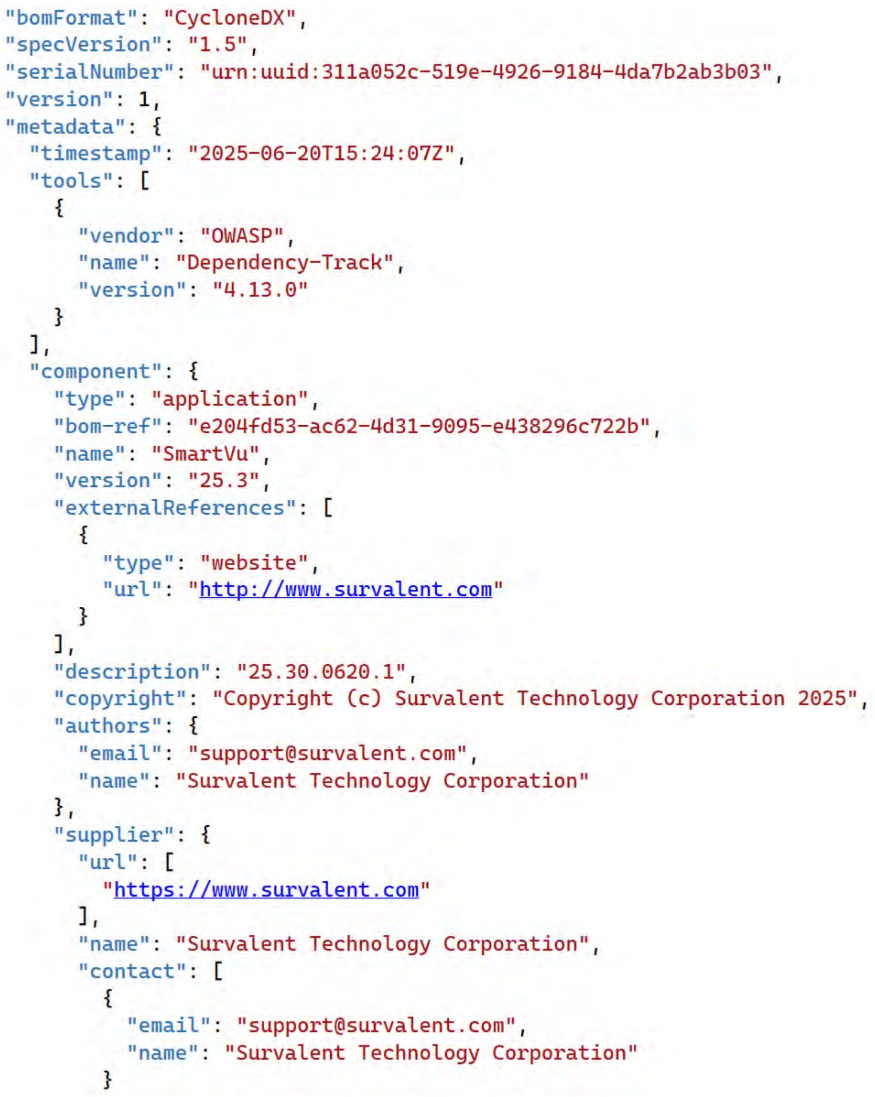
Complete Component Tracking

Our Software Bill of Materials (SBOM) provides a detailed inventory of every component and version in your system. Think of it as a complete parts list that helps identify potential vulnerabilities and ensures transparency.

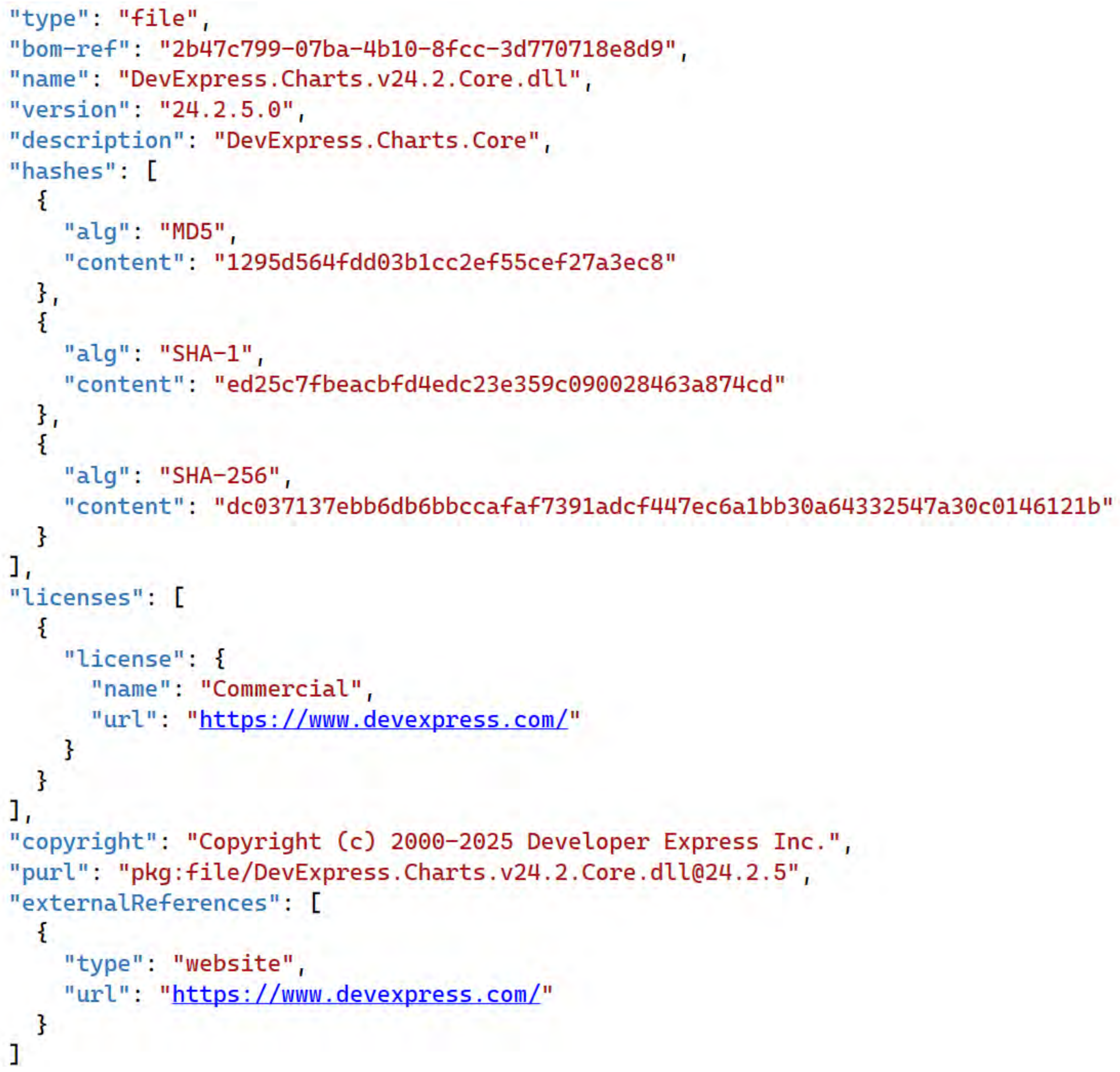
Operator Benefits

You can trust that every software update is genuine, safe, and fully traceable. No guesswork about what's running on your critical systems.

Component Tracking via SBOM



```
"bomFormat": "CycloneDX",
"specVersion": "1.5",
"serialNumber": "urn:uuid:311a052c-519e-4926-9184-4da7b2ab3b03",
"version": 1,
"metadata": {
  "timestamp": "2025-06-20T15:24:07Z",
  "tools": [
    {
      "vendor": "OWASP",
      "name": "Dependency-Track",
      "version": "4.13.0"
    }
  ],
  "component": {
    "type": "application",
    "bom-ref": "e204fd53-ac62-4d31-9095-e438296c722b",
    "name": "SmartVu",
    "version": "25.3",
    "externalReferences": [
      {
        "type": "website",
        "url": "http://www.survalent.com"
      }
    ],
    "description": "25.30.0620.1",
    "copyright": "Copyright (c) Survalent Technology Corporation 2025",
    "authors": {
      "email": "support@survalent.com",
      "name": "Survalent Technology Corporation"
    },
    "supplier": {
      "url": [
        "https://www.survalent.com"
      ],
      "name": "Survalent Technology Corporation",
      "contact": [
        {
          "email": "support@survalent.com",
          "name": "Survalent Technology Corporation"
        }
```



```
"type": "file",
"bom-ref": "2b47c799-07ba-4b10-8fcc-3d770718e8d9",
"name": "DevExpress.Charts.v24.2.Core.dll",
"version": "24.2.5.0",
"description": "DevExpress.Charts.Core",
"hashes": [
  {
    "alg": "MD5",
    "content": "1295d564fdd03b1cc2ef55cef27a3ec8"
  },
  {
    "alg": "SHA-1",
    "content": "ed25c7fbeacbfd4edc23e359c090028463a874cd"
  },
  {
    "alg": "SHA-256",
    "content": "dc037137ebb6db6bbccafaf7391adcf447ec6a1bb30a64332547a30c0146121b"
  }
],
"licenses": [
  {
    "license": {
      "name": "Commercial",
      "url": "https://www.devexpress.com/"
    }
  }
],
"copyright": "Copyright (c) 2000-2025 Developer Express Inc.",
"purl": "pkg:file/DevExpress.Charts.v24.2.Core.dll@24.2.5",
"externalReferences": [
  {
    "type": "website",
    "url": "https://www.devexpress.com/"
  }
]
```

Our Vulnerability Response

01

Planning

Establish and update response plans, define team roles, train staff, run drills, and prepare communication templates for product vulnerability incidents.

02

Awareness

Continuously scan code with vulnerability tools, run penetration tests, and log findings in Jira to track and prioritize potential security issues

03

Assessment

Evaluate each vulnerability's severity and customer impact, decide if code or configuration changes are needed, and prioritize fixes based on urgency.

04

Remediation

Develop, test, and release patches; critical flaws may require emergency fixes, while others are bundled into scheduled software update.

05

Customer Engagement

Notify customers of critical vulnerabilities within 24 hours, issue Security Bulletins, and include all fixes in release notes for transparency.

06

Continuous Improvement

Capture lessons learned, review feedback, and integrate improvements into annual ISO 27001 management reviews to strengthen future vulnerability handling.

2025 Vulnerability Tracking

Out of 92 vulnerabilities created, only 2 were considered Urgent. In total, 86% have been closed and released. The remaining are scheduled for 25.5 and 26.0!

Secure Software Development Process

Coding Standards -> Reviews

Consistent, secure design practices across all development teams ensure reliable code that operators can trust. Multiple developers review every code change to identify potential security issues early in the process.

Static Analysis

Static analysis tools like Sonar catch vulnerabilities before they reach your control room systems.

Automated Testing and Penetration Testing

Automated tests executed on EVERY code change which allows fast feedback and to confirm reliability before release. Penetration tests conducted 2-3X annually.

Open-Source Management

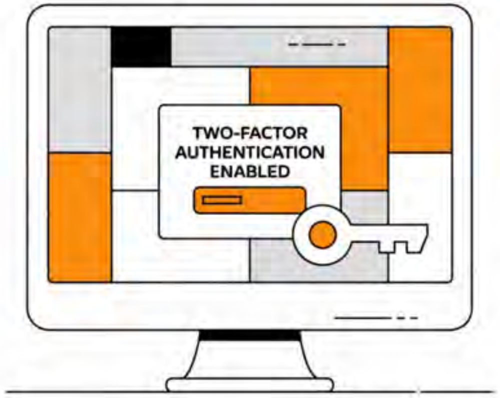
Careful selection and vulnerability scanning of third-party components protects against supply chain attacks.

Reviewing for 2026: ISO 62443-4-1 Certification

Speaks directly to our secure software development lifecycle.

Application Security

Password Security



Strong Authentication Controls

- **Complex password requirements**: Minimum length, character variety, and regular updates
- **Two-factor authentication**: Additional security layer beyond just passwords
- **Automatic lockout**: Accounts lock after failed attempts to prevent brute force attacks
- **Session timeouts**: Inactive sessions automatically log out to prevent unauthorized access

Domain Integration

LDAP and LDAPS integration means you use the same credentials as your domain login. No need to remember separate passwords - your existing IT infrastructure handles authentication seamlessly.

Coming in 2026: OAuth2 and SSO Support

Enhanced support in the DMZ, covering all APIs and web applications for OAuth2-based authentication and authorization.

Operator Privileges

Zone Groups

Control system access is organized by operational zones. Operators only see and control equipment within their assigned areas, reducing complexity and preventing accidental operations.

Privilege Modes

Different access levels for monitoring versus control operations. View-only access for training scenarios, full control for certified operators during normal operations.

Control Passwords

Additional authentication required for critical control actions like breaker operations or protection settings changes. This prevents accidental or unauthorized control commands.

Lockout Points

System administrators can instantly restrict access to specific equipment or functions during maintenance, emergencies, or security incidents without affecting other operations.

Coming in 2026: Customer Data Privileges

Access to customer information will be a choice.

Secure Communication Protocols

SECURE COMMUNICATION

ICCP (Inter-Control Center Protocol)

Secure real-time data exchange between control centers using TLS encryption and certificate authentication. Critical for coordinated grid operations across utility boundaries.

DNP3 Secure Authentication

Enhanced DNP3 protocol with cryptographic authentication prevents unauthorized commands to field devices. Every message is verified before execution.

OPC UA Security

Industry-standard secure communication for connecting to third-party systems. Built-in encryption and authentication protect against man-in-the-middle attacks.

Coming in 2026: IEC 104 Protocol

Enhanced support for international standard IEC 60870-5-104 with security extensions, expanding secure connectivity options for global operations.

Survalent.

Questions?

Thank You