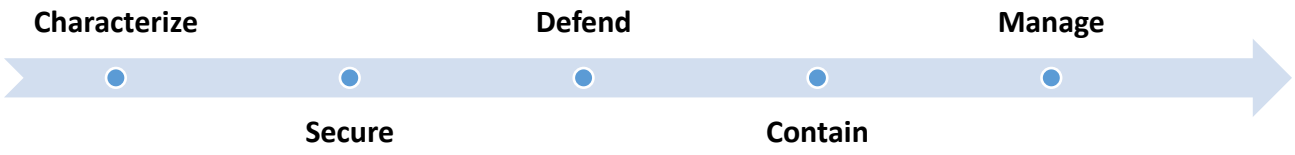
ICS Cybersecurity Solutions

The ICS Cyber Security Challenge. Industrial Control Systems are the computer-controlled electro-mechanical systems that enable operations. The term "Industrial Control System" is an umbrella term encompassing specific systems such as Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS), Energy Management Control System (EMCS), Building Automation System (BAS), and others, but they all perform a similar primary function. In broad terms, they manage, command, direct, and/or regulate the operation of devices or systems using control loops. The hardware components that comprise an ICS (for example, programmable logic controllers (PLC)) are classed as operational technology (OT) versus information technology (IT), which refers to personal computers and servers, amongst other things. The convergence of OT and IT is bridging networks and exposing control systems to risks they were previously isolated from, through network segmentation. This convergence, along with the growing prevalence of remote access tools, has enhanced the need for ICS cybersecurity and a continuous vulnerability management framework that can protect these mission critical systems.

The DSA Solution. To address the challenges associated with the current standard ICS cybersecurity approach (i.e. assessing and remediating fragmented systems independently), Data Systems Analysts, Inc. (DSA) has developed an ICS-focused cybersecurity framework. To ensure the connection of various systems - and different networks - does not increase an organization's risk profile, DSA performs physical security assessments, penetration testing and continuous vulnerability management. Our approach leverages DSA intellectual property alongside best-in-class software applications to deliver holistic cybersecurity situational awareness. DSA's testing approach follows SysAdmin, Audit, Network, and Security (SANS) Institute best practices to ensure all assessments are comprehensive. The process begins with a holistic characterization that includes a physical assessment and mapping external and internal networks; following this initial characterization, penetration testing and penetration verification testing are conducted on all assets. The results of the tests are analyzed for vulnerabilities, which are assigned a risk level based upon the pervasiveness of the threat, the significance of the vulnerability, and the potential impact. The risk level accounts for the importance of the asset or the type of data which could exist on the assets. The implication of the vulnerabilities to customer data and interconnects are evaluated to assure the assessment is specific to each customer and network.

In every circumstance, DSA's goal is to simultaneously reduce the **likelihood** of an incident and to reduce the **impact** of any incident that may occur.

DSA Process Overview.



Employee-Owned, Mission-Driven

Our suite of cybersecurity tools leverages industry solutions, industry compliance, and DSA experience to build a custom cyber solution. The solution addresses all aspects of ICS cybersecurity including: physical security & asset inventory; unidirectional gateways & DMZs; Firewalls & Whitelisting; and breach detection & incident management. Critically, DSA leverages the RiskSense vulnerability management software platform to provide ongoing cyber awareness between cyber assessments. DSA's Cybersecurity subject matter experts work with your IT group to design a secure deployment that appropriately connects systems and networks (e.g. firewalls, data diodes) and also integrates with existing network security policies. Once the system has been deployed, DSA's hybrid cyber-monitoring approach combines continuous vulnerability management with periodic penetration testing to ensure the overall architecture remains secure throughout its entire lifecycle. DSA uses a standard methodology based on NIST, SANS, and other industry frameworks; our approach is modified slightly based on the standards and guidelines that apply to each customer.

DSA ICS Cybersecurity Toolkit

Governance and Compliance	
• Telos Xacta 360	• RiskSense
• DOJ CSAM	• RSA Archer
Vulnerability Assessments	
• Tenable Nessus SecurityCenter	• Fortify WebInspect
• Nexpose	• Trustwave DbProtect
Penetration Testing	
• Metasploit	• Wireshark
• Acunetix / BurpSuite	• Core Impact
• Kali Linux	• Netsparker
Security Operations	
• SolarWinds SEM	• Splunk
• McAfee ePO	• ForeScout
• IBM BigFix	• SailPoint

DSA ICS Cybersecurity Engineering Qualifications:

- Certified Information Systems Security Professional (CISSP)
- Information System Security Engineering Professional (ISSEP)
- Certified Ethical Hacker (CEH)
- Certified Business Continuity Planner (CBCP)
- Certified Privacy Professional (CPP)
- Certified Protection Professional (CPP)
- SANS GIAC Certified Incident Handler (GCIH)
- SANS GIAC Security Essentials (GSEC)
- SANS GIAC Certified Forensic Analyst (GCFA)
- SANS GIAC Response and Industrial Defense (GRID)
- SANS Institute Certifications in Secure System/Network Administration and Management

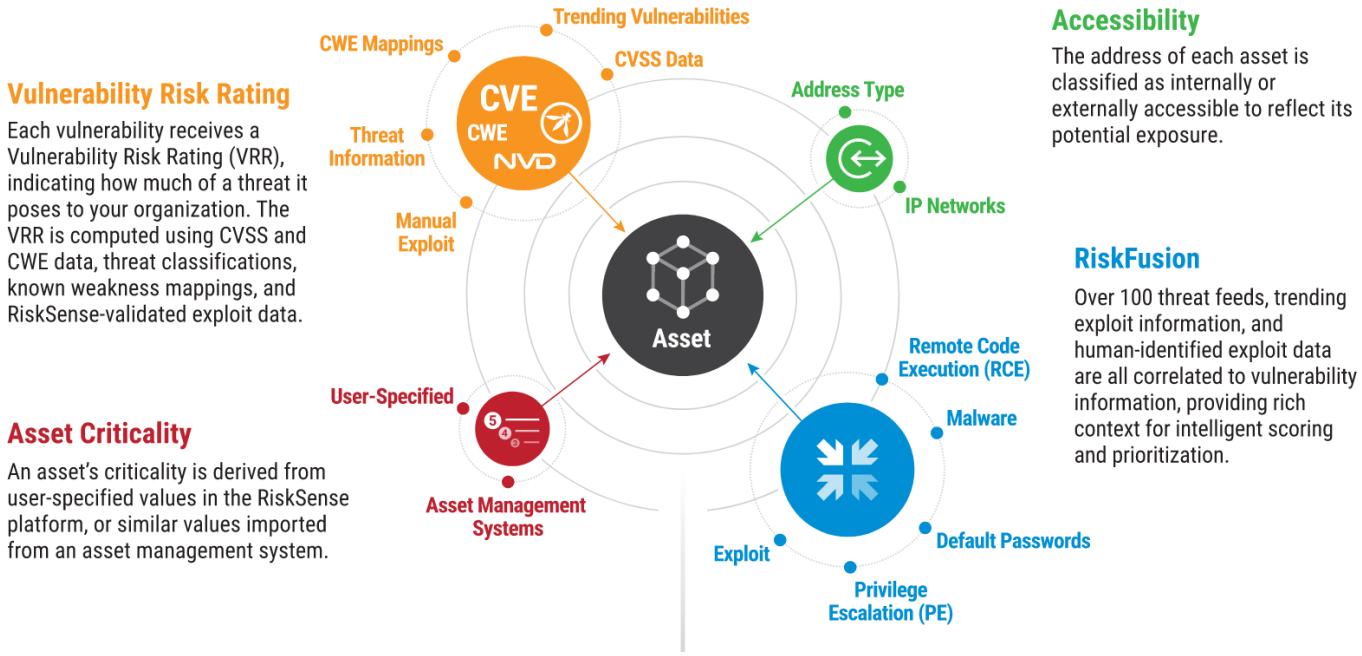
Cybersecurity Awareness. DSA uses standard industry products to map and test for vulnerabilities and then create a remediation checklist that streamlines the hardening process for customers by prioritizing what needs to be patched and secured. DSA's remediation checklist is prioritized based on each issue's vulnerability score. A vulnerability is a weakness which allows an attacker to reduce a system's information assurance; it is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To score a vulnerability, we account for the following factors:

- **Ease of discovery:** How easy is it for this group of threat agents to discover this vulnerability?
- **Ease of exploitation:** How easy is it for this group of threat agents to actually exploit this vulnerability?
- **Awareness:** How well known is this vulnerability to this group of threat agents?
- **Intrusion detection:** How likely is an exploit to be detected?

Our remediation prioritization methodology also takes account of technical Impact Factors. Technical impact can be broken down into factors aligned with the traditional security areas of concern: confidentiality, integrity, availability, and accountability. These are rated from critical to low based on magnitude of the impact on the system if the vulnerability were to be exploited.

- **Loss of confidentiality:** How much data could be disclosed and how sensitive is it?
- **Loss of integrity:** How much data could be corrupted and how damaged is it?
- **Loss of availability:** How much service could be lost and how vital is it?
- **Loss of accountability:** Are the threat agents' actions traceable to an individual?

Figure 1. DSA / Risk Sense RS3 Risk Scoring Model



Comprehensive Risk Management Services. Our highly trained security consultants keep abreast of emerging security issues and challenges by attending conferences, participating in formal technical security training, and being active members of professional security organizations. Our Cyber-Sentry Offering offers a comprehensive risk management approach that focuses on people, processes, and technology and draws on the expertise of DSA's core practice areas:

Security Governance and Oversight

- Implementing and operating enterprise-wide IT security programs
- Security Risk Management & Compliance
- CISO Advisory
- Security Awareness and Training
- Information System Security Officer (ISSO) Support
- Regulatory Review, Assessment, and Guidance

Secure Enterprise Solutions

- Vulnerability Scanning & Remediation
- Penetration Testing
- DevSecOps - Securing the Software Application Lifecycle

Security Operations

- Security Operation Center (SOC) Administration and Support
- Critical Infrastructure Protection

For more information on our services or to schedule a briefing, please contact us at CyberReady@DSAINC.com

DSA Customers