ALTIMETRIK

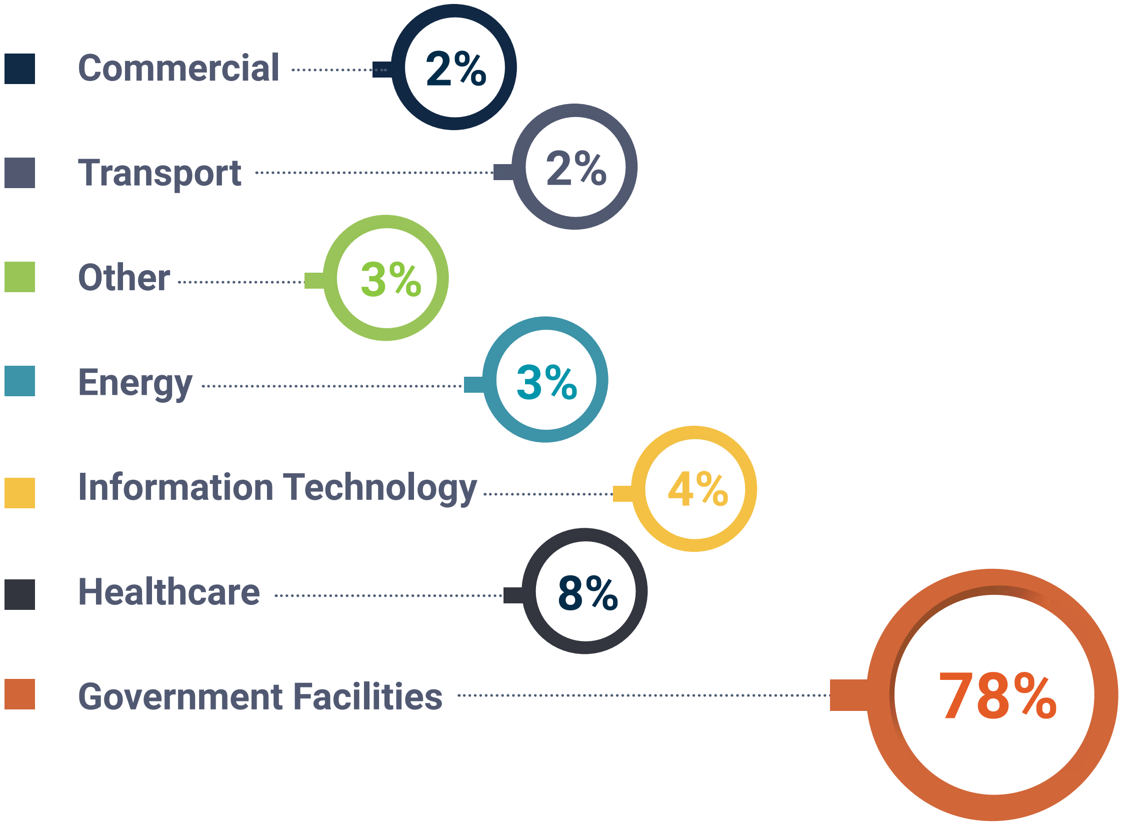
ICS - SCADA - OT
Security Services
Datasheet

teNotice">…</div>
"mw-indicators"> </div>
"firstHeading" class="firstHeading
"bodyContent" class="vector-body
id="siteSub" class="noprint"
"contentSub"></div>
"contentSub2"></div>
"jump-to-nav"></div>
"mw-jump-link" href="#mw-head"
"mw-jump-link" href="#search"
"mw-content-text" class="
"mw-parser-output">…</div>
</noscript>
"printfooter" data-nosnippet
"catlinks" data
//mobile

Introduction

The Department of Homeland Security (DHS), alongside the Cybersecurity and Infrastructure Security Agency (CISA) and the United States Computer Emergency Readiness Team (US-CERT), collectively respond to a staggering number of ICS cybersecurity incidents each year. In recent years, DHS, CISA and US-CERT responded to 2,609 cybersecurity incidents. These figures illustrate the pressing reality that industrial control systems (ICS), which are the backbone of critical infrastructure, are no exception to the pervasive threats encountered within conventional IT networks.

INCIDENTS BY SECTOR



ICS vulnerabilities can expose critical infrastructure to risks, ranging from cyberattacks that disrupt operations to compromises that endanger public safety. By understanding and addressing these vulnerabilities, industries can mitigate the potential for operational downtime, financial losses, and reputational damage.

Common ICS Vulnerabilities

1. **Poor Code Quality:** Code issues are often exacerbated in control systems that may be decades old, and running code that has not been updated since its installation. Changing coding practices or rewriting the source code for a flagship product can be expensive for vendors and customers, and applying patches in an operational environment is often difficult.
2. **Vulnerable Web Services:** Unpatched or vulnerable web services with poor authentication, directory traversal, broken authentication issues, and potential SQL injection points
3. **Poor Network Protocol Implementations:** Vulnerabilities stemming from buffer overflow and lack of bounds checking in control system services, weak or no authentication, control system protocols using weak integrity checks or reliance on standard IT protocol using weak or poorly implemented cryptography
4. **Poor Patch Management:** Unpatched or old versions of third-party software incorporated into ICS software, unpatched operating systems and older legacy operating systems can lead to compromise over time
5. **Weak Authentication:** Issues stemming from systems incorporating standard IT protocol that are using weak or poorly implemented encryption, cleartext authentication, client-side enforcement of server-side security, improper security configurations, and weak passwords and policies
6. **Least User Privileges Violation:** This issue occurs when services are running with unnecessary privileges
7. **Information Disclosure:** This vulnerability occurs with unencrypted proprietary and non-proprietary control system protocols, open network shares on control system hosts and information leak through unsecured services
8. **Network Design:** Some ICS network architectures use flat networks with no zones, no port security, and weak enforcement of remote access policies. To compound this problem, ICS networks may be directly connected to corporate environments without firewalls and zones, or allow direct connections to the Internet.
9. **Network Component Configurations:** Lack of IP whitelisting or port security implemented on network equipment

It is crucial to adopt a proactive stance against threats by identifying vulnerabilities, implementing robust security measures, and preparing for potential incidents. Taking these steps not only helps secure your company but also ensures that you are well-prepared to respond effectively in the event of a cybersecurity breach.

Altimetrik

ICS Security Services

Altimetrik ICS, SCADA and IoT Security Services is your trusted partner in safeguarding your organization’s digital assets and ensuring resilience against the ever-evolving landscape of cybersecurity threats. With a commitment to excellence and a focus on proactive defense, our team of seasoned experts offers a comprehensive suite of solutions designed to fortify your defenses. From threat detection and incident response to compliance management and vulnerability assessments, our services are tailored to meet your specific needs and industry standards. With a dedication to staying ahead of emerging threats, we empower organizations to thrive in a secure digital environment while minimizing risks, reducing vulnerabilities, and fortifying their critical infrastructure.

Key Features

1. Architecture Risk Analysis

We begin our security assessment with architectural risk analysis and threat modeling, to understand and document your current network environment thoroughly. This involves an in-depth review of existing architecture diagrams, dataflow, and design, along with an evaluation of the industrial/operational communication protocols in use. We also review and implement proper network segmentation to protect your internal network from external threats.

Next we develop a threat model through collaborative workshops with your IT and operations/engineering teams. We construct visual representations of potential control system attacks using the NIST Cybersecurity Framework. This approach helps prioritize security control implementations by identifying the most critical attack vectors, thereby reducing your company’s risk and exposure

2. Vulnerability Assessment

Altimetrik's ICS, SCADA and IoT Vulnerability Assessment services offer a comprehensive evaluation of your system or facility's cybersecurity posture without the need for intrusive techniques. We understand the unique concerns of organizations operating in industrial environments where operational risk is a top priority. Our team perform real-time scans of your environment for potentially vulnerable services and logs all issues to a central repository for tracking and remediation. Stakeholders are notified and our experts work with you to remediate the issues.

We collaborate directly with your engineers to tailor cybersecurity best practices to your specific environment. Additionally, we empower your IT security leaders with the necessary domain knowledge and credibility to engage effectively with teams in cybersecurity discussions.

3. ICS - SCADA – OT Penetration Testing

We deploy real-world attack techniques using the MITRE ATT&CK framework, meticulously identifying vulnerable devices and safeguarding crucial ICS assets from unauthorized access. Through simulated attacks, we identify potential threat paths, providing actionable insights to fortify your OT cybersecurity posture. Our approach covers every angle - from wireless attacks, physical security and pinpointing exploitable system vulnerabilities that could compromise your OT infrastructure to assisting in patch management and vulnerability management.

4. Threat Detection and Prevention

Our Threat Detection services include a comprehensive network security review, where we analyze network packet captures from your ICS, SCADA and OT network to identify security risks such as unintended connectivity to the internet or business network and anomalous connections. We also assess the configuration and rule sets of network security devices and network segmentation to ensure that your networks are properly isolated from the internet.

After the assessment, you will receive a comprehensive technical report of our findings. This report encompasses a thorough analysis of any detected security vulnerabilities, configuration issues, structural deficiencies, unusual network traffic, or anomalous behaviors.

5. Anomaly Detection

We specialize in the identification of rare outliers and data points that deviate from established trends within your OT environment. These anomalies can serve as early indicators of suspicious events, malfunctions, defects, or potential fraud, making their detection paramount to your cybersecurity strategy.

By using best of breed anomaly detection tools our team excels in identifying irregularities within your data and deviations from common statistical distributions. By leveraging this expertise, we equip your organization with the ability to promptly spot and address anomalies that could pose a threat to your industrial control systems.

6. CSIRT (Incident Response)

Our team of cybersecurity experts is dedicated to providing rapid incident detection, response, and recovery and ensuring minimal disruption to your operations. Leveraging best-of-breed technologies and industry best practices, we offer round-the-clock monitoring, proactive threat hunting, and incident response. We communicate and collaborate with stakeholders closely to track and remediate issues.

Before initiating remediation, we conduct a thorough assessment to identify the root causes of the incident. This includes pinpointing vulnerabilities, misconfigurations, and security gaps that may have contributed to the breach. We work closely with your organization to contain and eradicate the threat, minimize data loss, and assist in the restoration of your business-critical services.

7. SGRC - Compliance and Reporting

Altimetrik's Security, Governance, Risk Management, and Compliance (SGRC) services for ICS – SCADA - OT security are designed to assist your organization in achieving compliance with the relevant standards and frameworks while enhancing the resilience of your ICS, SCADA and OT environment.

Here's how our SGRC services align:

U.S. Department of Homeland Security: Our services align with DHS guidelines, including the Catalog of Control Systems Security, ICS-CERT and SCADA Procurement Language.

ISO/IEC 27001: We assist in achieving ISO/IEC 27001 certification for comprehensive information security management.

NIST Guidelines (SP 800-53R4, SP 800-82R2, SP 800-37, FIPS 140-2): Our services align with NIST guidelines for robust cybersecurity, risk management, and secure system deployment.

CISA BOD (Binding Operational Directive): We assist in aligning with the CISA BOD guidelines for securing industrial control systems, ensuring compliance and robust cybersecurity.

Benefits

Enhanced Cybersecurity Posture

Clients will benefit from a significantly improved cybersecurity posture for their Industrial Control Systems (ICS) and Operational Technology (OT) environments. This enhanced security will safeguard critical infrastructure, reduce vulnerabilities, and protect against a wide range of cyber threats.

Regulatory Compliance

Our services ensure that clients meet various regulatory requirements and standards such as GDPR, CCPA, NIS2 Directive (EU), NERC CIP, C2M2, and more. Compliance with these standards not only avoids legal penalties but also demonstrates a commitment to data privacy and security.

Reduced Risk and Cost Savings

By identifying vulnerabilities and implementing robust security controls, Altimetrik security services help clients mitigate risks associated with cyberattacks, operational disruptions, and data breaches. This risk reduction minimizes potential financial losses and reputational damage.

Cyber Threat Hunting

Clients benefit from continuous, real-time monitoring and threat hunting, allowing for early detection and proactive response to emerging threats. This capability minimizes the potential damage of cyber incidents.

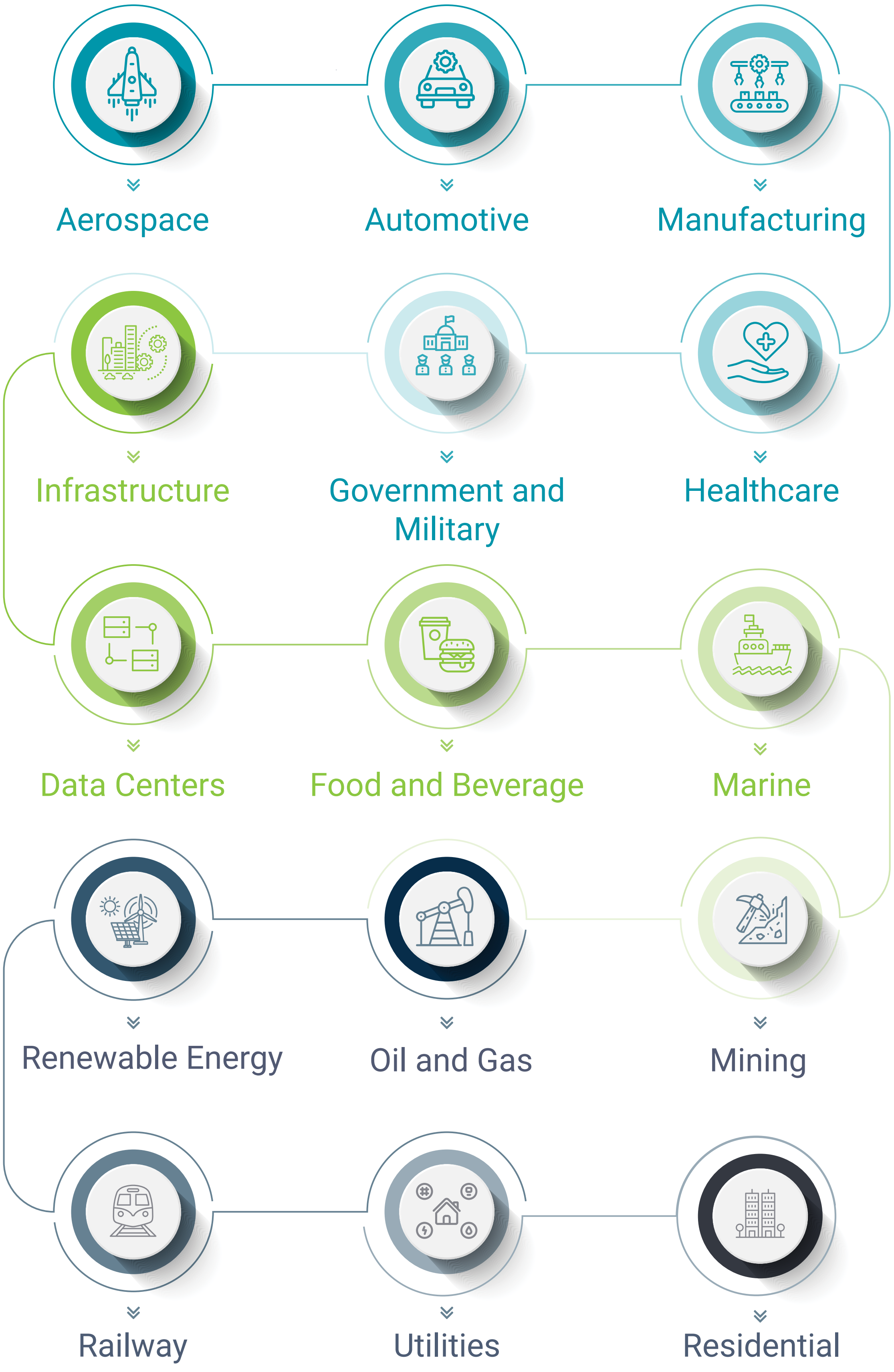
Resilience and Continuity

Altimetrik helps clients build resilience in their ICS – SCADA - OT environments. This resilience ensures continuity of operations even in the face of cyber threats, enhancing overall business continuity and minimizing downtime.

Incident Response Preparedness

Clients gain confidence in their ability to respond effectively to cybersecurity incidents. Our incident response procedures and threat detection capabilities ensure swift identification, containment, and resolution of security breaches.

Industries Served



Aerospace

Automotive

Manufacturing

Healthcare

Government and Military

Infrastructure

Data Centers

Food and Beverage

Marine

Mining

Oil and Gas

Renewable Energy

Railway

Utilities

Residential

Conclusion

Altimetrik is your trusted partner in navigating the landscape of ICS, SCADA and OT cybersecurity. As technology advances so do the threats to critical infrastructure. We are committed to empowering organizations with tailored solutions that enhance security, reduce vulnerabilities, and fortify their ICS, SCADA and OT environments. With a comprehensive suite of services, spanning from architecture risk analysis, vulnerability management, penetration testing, threat hunting, incident response planning and compliance. We provide the expertise and support needed to safeguard operations, protect assets, and maintain the resilience of business critical services.

Altimetrik is a leading globally trusted pure-play digital enablement company accelerating digital business growth with speed, scale, and consistency. Witnessing a growth of 50% y-o-y over the last few years, Altimetrik leverages agile and pragmatic approach that focuses on bite-sized outcomes essential to accelerate business growth. The company's digital business methodology provides a blueprint to develop, scale, and launch new products to market faster without disruption. Over 5,500 employees including practitioners with software, data, and cloud engineering expertise create a vibrant culture of innovation and agility that enhances team performance, modernizes technology, and builds new business models. Altimetrik follows a unique approach of employing a Digital Business Platform (DBP) enforcing the Digital Business Methodology (DBM) across the enterprise for consistency and scale. The company actively supports education, sustainability, and social welfare initiatives, making a positive impact in the communities they serve. For more information on Altimterik, please visit https://altimetrik.com/