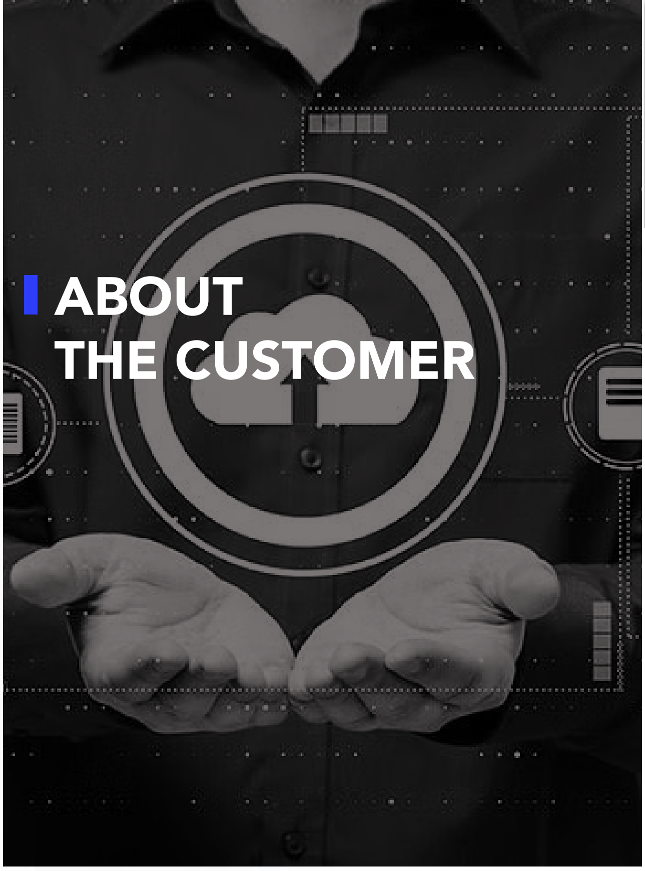
CUSTOMER SUCCESS STORY

SISA helps a global cloud-based solutions provider mitigate IoT device vulnerabilities



ABOUT THE CUSTOMER

Our client is a Massachusetts-based global provider of cloud-based software solutions tailored specifically for laboratories in the life sciences and other science-based industries. The client helps modernize lab infrastructure by integrating new and legacy instruments, applications and web services into a common, cloud-based platform. Their industry-grade IoT interface assists labs to securely connect various sensitive lab instruments with a cloud-based DLX platform, to propel scientific research through digital technologies.

THE CHALLENGE

The client's IoT interface is powered by proprietary technology and linked to their DLX cloud platform. In an environment rife with the use of outdated components, weak passwords, and insecure default settings, ecosystem interfaces and network services, the client wanted to conduct a robust security assessment of their IoT interface. With operations across the European region, any data leak involving the end users' data would have resulted in high-cost lawsuits along with reputational damage.

Determining the best approach to patch all identified vulnerabilities and ensuring that business operations proceed without being compromised, was crucial for the client. The client, however, lacked in-house expertise and required specialized testing capability to ensure the safety and security of sensitive data that is critical to the life sciences industry.

To achieve its objectives the client reached out to SISA with the following asks –

Address software-related bugs, which could disrupt device operation by overloading hardware resources, corrupt hardware state and trigger hardware faults.

Verify communication between the IoT device and the cloud service along with assessing its susceptibility to Man-in-the-Middle (MITM) attacks, and the strength of encryption algorithms.

Identify any flaws in the implementation of standard device protocols.

Assess all three layers of the IoT device, including the software, networking, and hardware for its security.

SOLUTION OFFERED BY SISA

SISA adopted a three-phased approach consisting of Security Assessment, Remediation, and Reporting to assist the client in overcoming the challenges associated with IoT device security. SISA kicked off the engagement by conducting a two-stage security assessment using a black box approach. The first stage involved security assessment, while the second stage involved validating the identified vulnerabilities in the first stage as well as checking for any other security issues that emerged as a result of the patches applied. The IoT device security assessment was carried out in SISA's world-class hardware security testing lab, using a combination of automated and manual testing techniques along with best-in-class hardware and software tools.

SISA's learnings from past forensic investigations, combined with the findings from the assessment, revealed several gaps in its cloud implementation, such as sensitive data in the GET Method and firmware being downloaded without strong authorization along with various hardware loopholes. These loopholes included a password-less/weak authentication mechanism, insecure protocols, outdated certificates, the use of vulnerable/outdated software versions, and various debug ports through which an attacker could gain access to the device's internal systems, download the proprietary firmware and potentially take control of the device. This could have allowed the attacker to perform a variety of malicious actions, such as modifying the device's firmware, injecting malicious code into the device, or accessing sensitive data stored on the device.

SISA presented a detailed report on the severity of the vulnerabilities and their effects on the client's infrastructure while also sharing best practices and suggestions. SISA also published a final report that included step-by-step remediation recommendations for patching these vulnerabilities while also allowing for tracking action.

BUSINESS IMPACT

SISA's Hardware and IoT security assessment and remediation consulting support helped the client close critical security gaps and improve the overall security of the IoT Device's firmware, hardware, and software components. Additionally, SISA's consultative approach, which included multiple rounds of discussions, helped the client understand the business impact and mitigate vulnerabilities without disrupting its business operations. The client was able to future-proof its device security by enforcing SISA's tailor-made mitigations and security measures. With SISA's CERT-IN and CREST accredited testing, the client was able to reduce the time to market by offloading its IoT security testing to SISA and establish trust in its end users.

SISA

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective cybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

Compliance

Payment Data Security

- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ
- Quarterly Health Check-ups
- Central Bank Compliance
- SWIFT

Strategy and Risk

- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Cloud Security

Security Testing

Application Security

- Application Penetration Testing
- CREST/CERT-in Approved Security Testing
- API Security Testing
- Secure Code Review

Network Security

- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Red Teaming Exercise
- Firewall Rule Review
- PCI ASV Scan
- Phishing Simulation

Hardware and IoT Security Testing

- Firmware Security Testing
- Hardware/Embedded Security Testing
- IoT Network Security Testing
- IoT/Embedded Application and Management Layer Security Testing

Cyber Resilience

Managed Detection and Response Solution – SISA ProACT

- Monitoring
- Attack Simulation
- Use-case Factory
- Advanced Threat Hunting

Digital Forensics and Incident Response

- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensics Investigation
- Internal Forensics Investigation
- Ransomware Simulation

Data Governance

Data Discovery and Classification - SISA Radar

- Card Data Discovery
- PII (Privacy) Discovery
- Data Classification
- Data Masking/Encryption

Data Security as a Service

Cyber Academy

Payment Data Security Implementation

- CPISI
- CPISI Advanced
- CPISI-D (Developers)

Security Incident Detection and Response Programs

- CIDR

Cybersecurity Awareness

Forensic Learning Sessions for Senior Management

For more Information visit us at www.sisainfosec.com
OR
write to us at *contact@sisainfosec.com*

Follow us