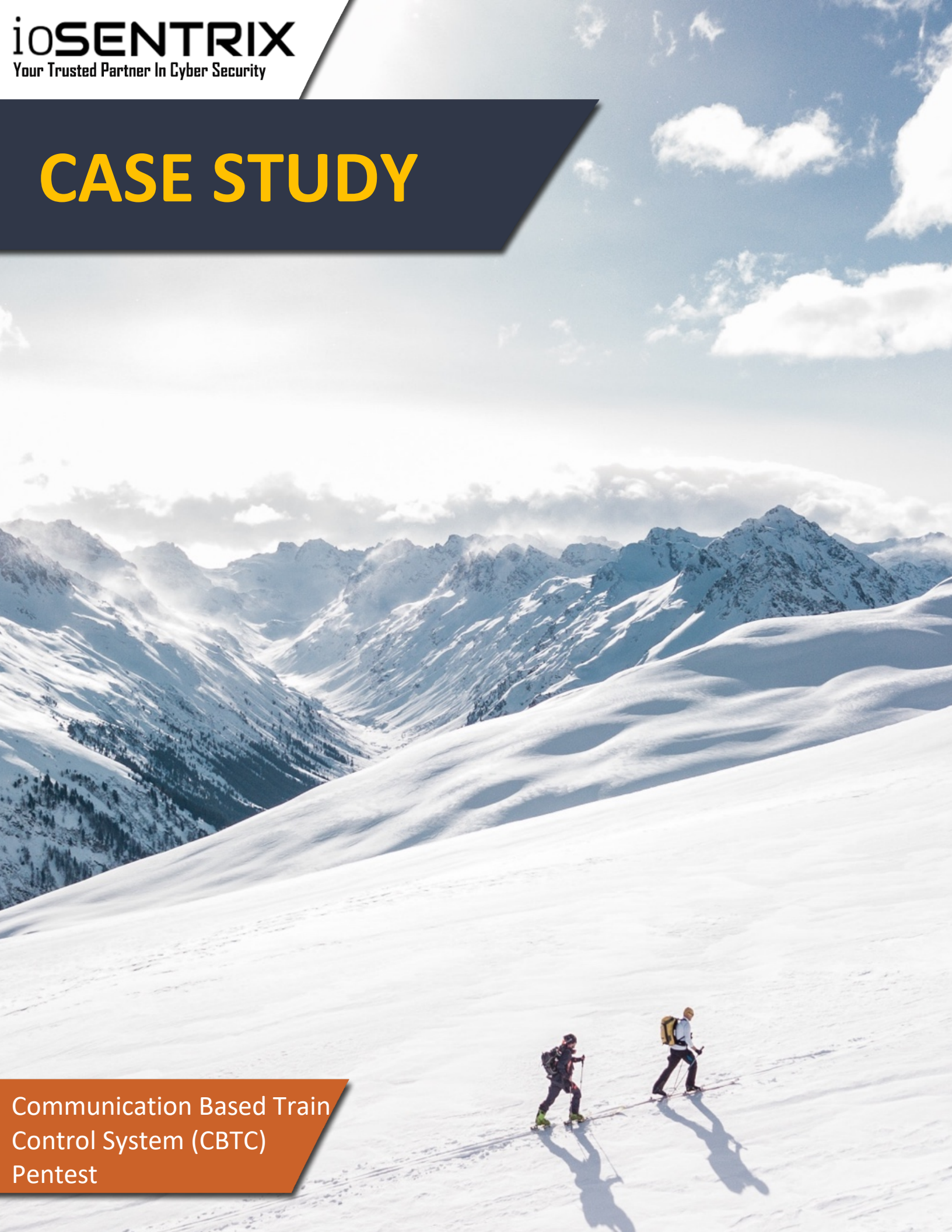
ioSENTRIX
Your Trusted Partner In Cyber Security

CASE STUDY



Communication Based Train Control System (CBTC) Pentest

Background

One of the passenger rail transport providers engaged ioSENTRIX to perform a security assessment of their Communication Based Train Control System (CBTC) that is deployed and has been in use for several years. Although CBTC systems are designed to be fail-safe from passenger's safety perspective, cyber-attacks are still possible due to greater use of network infrastructure, operating systems and other supporting software. Apart from reputational risks, the cyber-attacks could be enough to shut down the entire operation for a couple of days at least which could be disastrous in a certain situation -- Imagine a city that primarily uses railway systems as transport. Bringing down the transport system for a day when they are hosting a big event like the Olympics will be a pretty daunting situation. Therefore, ioSENTRIX was hired to perform a simulated cyber-attack (penetration test) to discover the vulnerabilities in their CBTC based infrastructure.

The Challenges

The client had a heavily segmented network with a lot of proprietary equipment and software in their infrastructure. Pentesting proprietary software and Industrial Control Systems (ICS) related to passenger railway require a significant effort to learn and exploit since they don't have open standards.

The first most significant challenge for the client was to develop a lab that was significantly identical to production -- minus the real train system. This was required to understand the real threats that the client may face during a cyber-attack. The second biggest challenge for the client was to immediately patch the identified vulnerabilities in the production environment (after testing) since the environment was already operational.

Our Approach & Process

Below is our standard approach for Network and Infrastructure penetration test.

With a team of two (2) testers for six (6) weeks, we were able to compromise the entire network including several ICS as well. Our testers started targeting the exposed network segment and after successful compromise, they targeted the nodes that were connecting multiple network segments and used pivoting to compromise other segmented networks as well.

We were able to obtain access to the sensitive nodes which were controlling the train system communication. Although the CBTC systems are designed to be fail-safe for passenger's safety, we were able to simulate the shutdown for several trains which caused a simulated outage in different operational regions.

We concluded the test and provided a detailed report that included details of vulnerabilities, severity ratings based on NIST standard, evidence and remediation strategies. We also helped the client with the risk management support such as, which significant vulnerabilities should be fixed given their threat landscape versus which ones could be accepted for a limited period of time given that some controls are present.

Kick off & Planning

- Kick off call with the stakeholders
- Identify the scope of the engagement
- Define rules of engagement and responsibilities for both the client and our testers
- Target information gathering
- Develop a Threat Model

Testing

- Conduct the vulnerability assessment
- Carry out penetration testing
- Validate the identified issues

Post Exploitation

- Privilege escalation
- Identified new target
- Analyze other networks if included in the scope
- Pivot and attack on newly identified targets

Reporting

- Draft all the vulnerabilities with the evidence and remediation steps
- Calculate business impact from the technical impact
- Rate the vulnerabilities for risk assessment.
- Peer Review and Deliver

The Results

By conducting an in-depth network and Infrastructure penetration test, the client gained valuable insights on the impact of the cyberattack on CBTC system and the effectiveness of their current security controls in place. The client also learned about the new threats and the remediation strategies which were unknown to them before the engagement. The latest threats were then used to revise the incident response plan.

Overall, the client was very happy with the end results and requested ioSENTRIX to re-assess the identified vulnerabilities after remediation.

About ioSENTRIX:

ioSENTRIX LLC is a Security Consulting firm. We provide a wide range of security consulting services to our clients worldwide. Our list of clients spans the fortune 500, large enterprises to small start-ups, financial institutions, and several high-tech companies.

We are an innovative consulting company offering a full range of cyber security services to businesses of all sizes, tailored to meet any budget requirements. We help our clients by identifying, mitigating and preventing vulnerabilities in their software, infrastructure, and cloud.

We offer a comprehensive vulnerability assessment that includes design-review, threat model, penetration test, code review, and open source software security. We've got the necessary tools and the expertise to secure your business so you can focus on growing it.

Learn more about our services at **https://www.iosentrix.com.**

ioSENTRIX LLC.

150 S. Sterling Blvd, Suite 543
Sterling Virginia 20164 (USA)

Sales: 1 (888) 958-0554
Email: sales@iosentrix.com