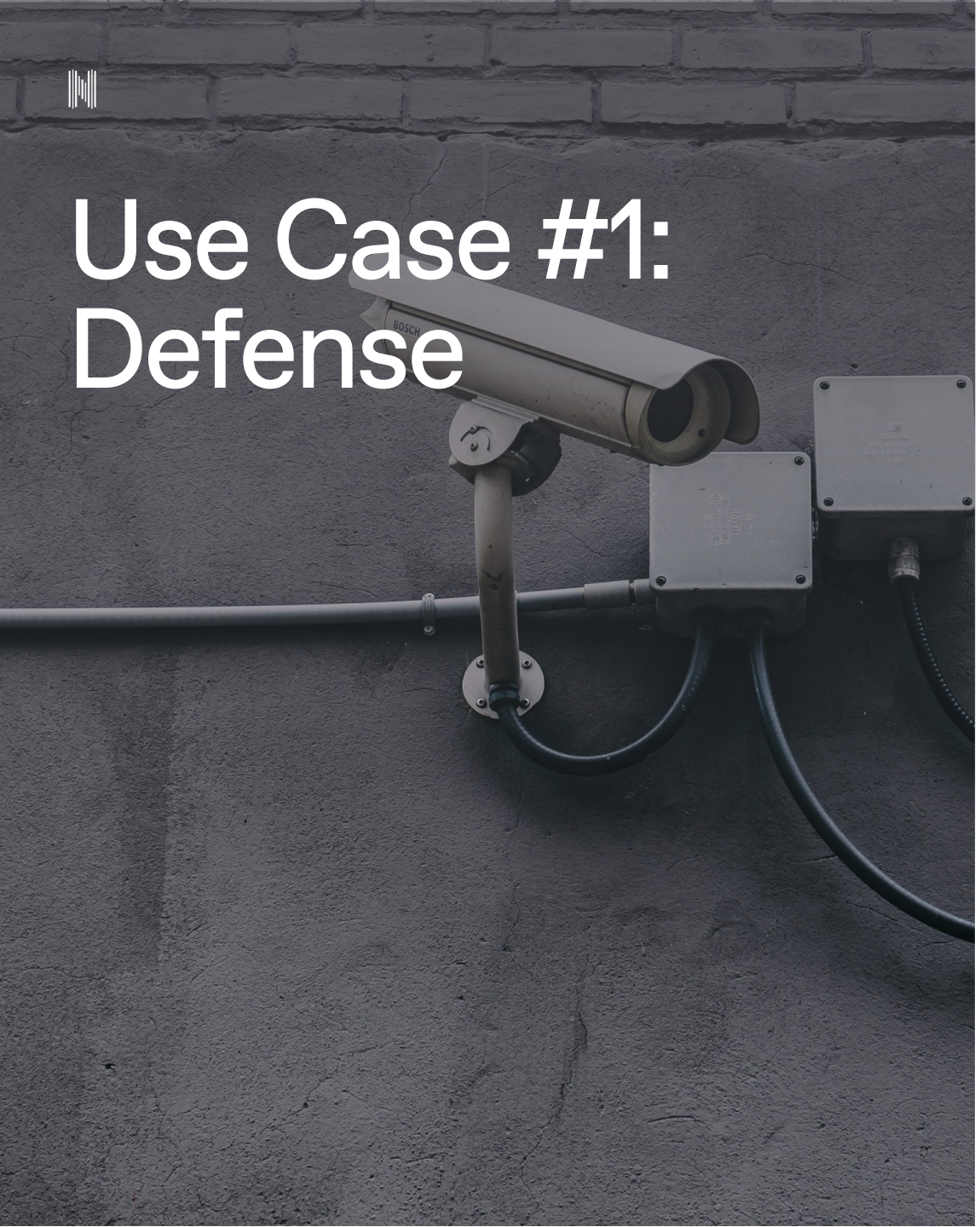
Nortal

Defense case studies



Use Case #1: Defense

Background:

With over 15 years of extensive work within the defense ecosystem, Nortal has an exceptional reputation in delivering high-quality cybersecurity architecture and security operations outcomes. We were contacted by a government defense agency to drive an urgent and critical security assessment project.

Requirement:

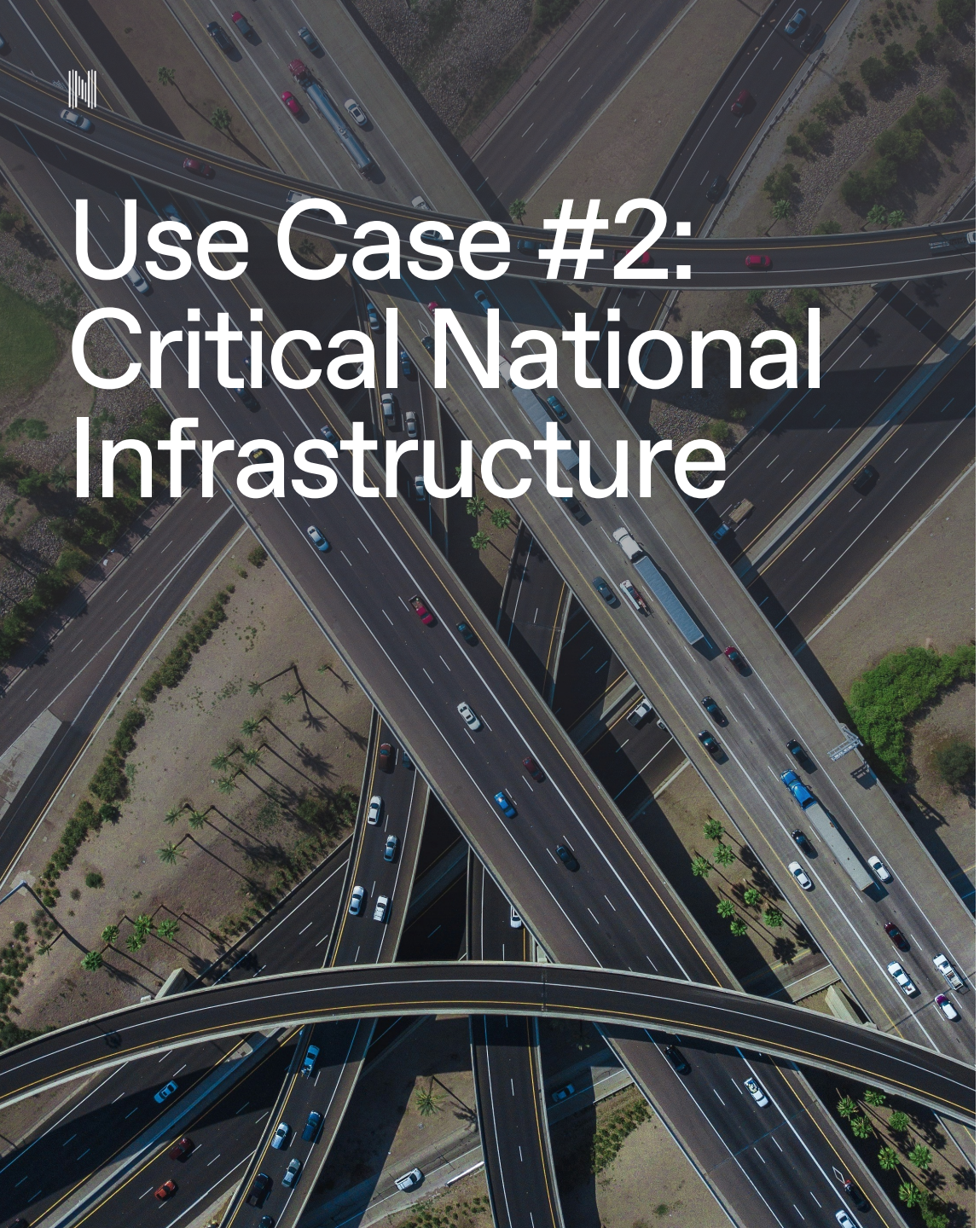
Our team was tasked with assisting our client in implementing protective monitoring (detect) and incident response (respond) within a unique and complex maritime environment. This environment encompasses both traditional information technology and industrial control systems (ICS) and operational technology (OT).

Activities:

Nortal utilized the NIST framework to assess the current status of the environment, discover the breadth of control coverage, and provide recommendations. Additionally, we led the delivery of remediations to enhance detection and response activities in this highly complex environment.

Outcome:

Our team successfully performed a gap analysis, developed a security improvement and transformation plan, and implemented several recommendations. These actions enhanced monitoring of the IT/OT infrastructure and improved incident response activities, significantly reducing cybersecurity risks.



Use Case #2: Critical National Infrastructure

Background:

Due to our strong track record with clients in the infrastructure sector, we have established a reputation as a reliable security partner, known for our ability to execute efficiently within short timescales. Consequently, an energy provider contacted us to conduct a comprehensive security assessment.

Requirement:

Our team was tasked with assessing several of the energy provider's data centers and energy delivery locations. Following their recent private equity backing, they required a realistic evaluation of their IT and OT security levels and the risks posed by ransomware and other threats.

Activities:

The engagement began with a threat assessment to understand the threat actors and tactics, techniques, and procedures (TTPs) relevant to their operations. Simultaneously, a team was deployed to physical data centers and energy delivery locations to interview key personnel, assess security controls, and report the real-world situation. Evidence was collected and reported to the client and a targeted improvement plan was created.

Outcome:

From inception to delivery, our team successfully completed this engagement in six weeks. The client was pleased with our adherence to rapid timescales and real-world insight provided. As a result, they have commissioned an additional engagement for us to assist their teams in implementing the recommendations to reduce cyber risk across their estate.

The opportunity to redesign your future is now

Your frictions and frustrations are our insights and inspirations.

Let’s discuss!