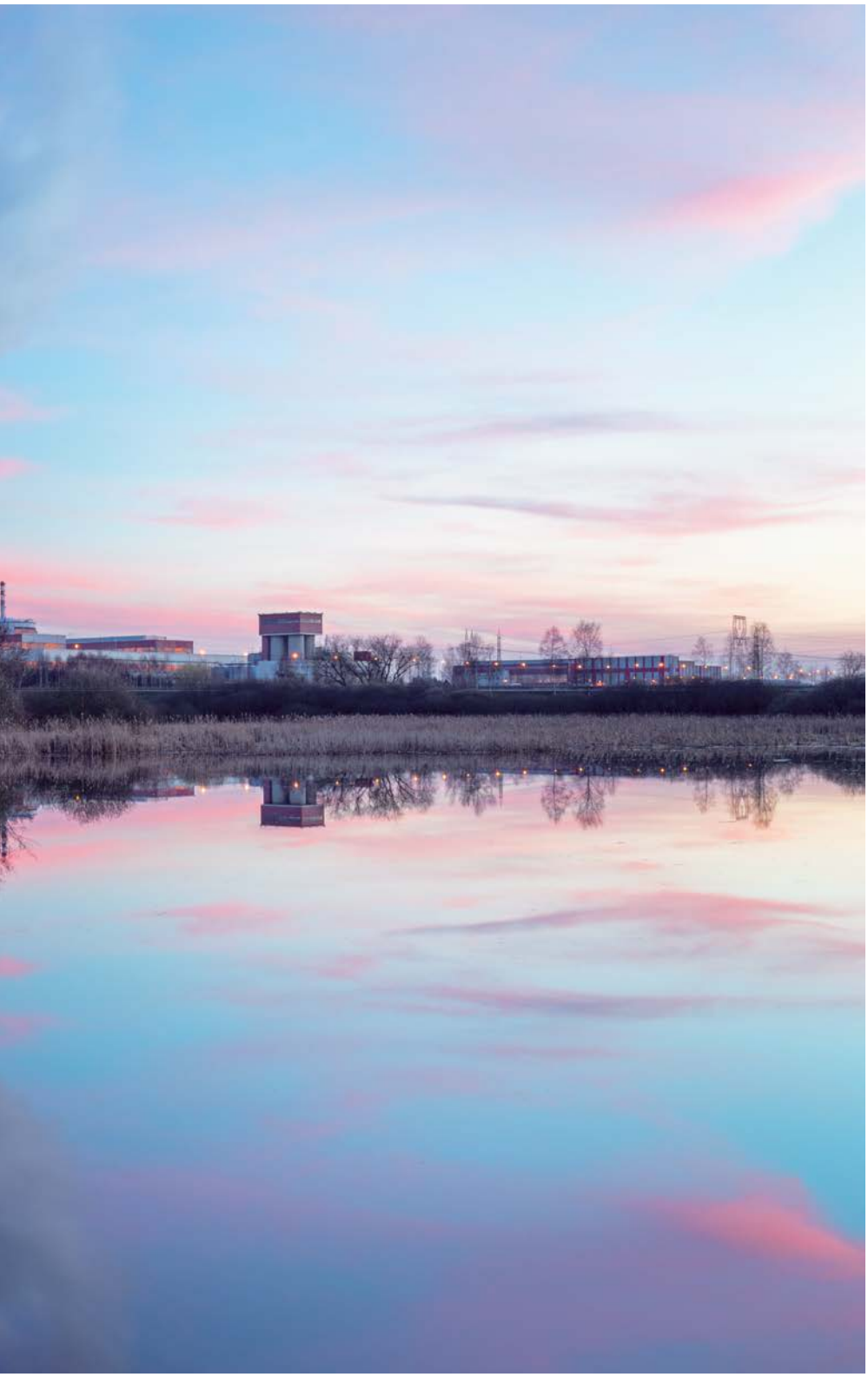
vehere

Case study

Critical infrastructure/Government



Summary

Industry/Organisation

Critical infrastructure/Government

Challenges

- Concerns about the prevalence of fast-moving, automated attacks
- Adopt a proactive approach to cyber defense
- Attain comprehensive visibility into critical infrastructure stations
- Secure itself from breaches, data thefts, malware/zero-day attacks
- Too many false positives
- Insider threats
- Surfeit of reactive and lack of proactive measures

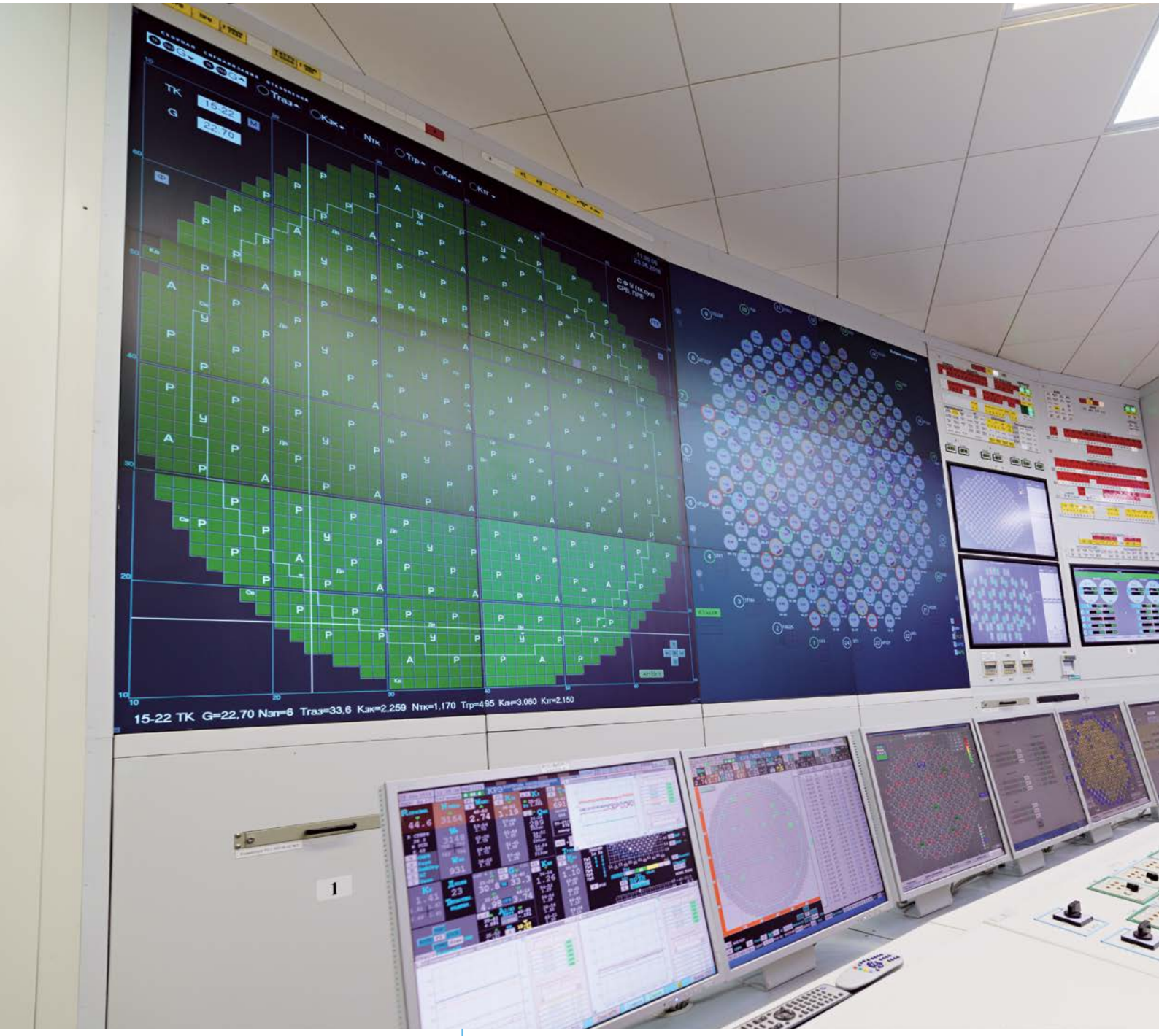
Solution

PacketWorker 10G and professional services

Benefits

- 100%-network visibility including in ICS protocols
- Improved response time by >100%
- Reduction in cybersecurity risks, data losses and subsequent costs of restoration
- Compliance with contractual and regulatory obligations
- Detection of automated attacks in real time
- Increased efficiency with proactive alerts

vehere



Critical infrastructure owners need more resilience, with fewer siloes and the competency to detect, scrutinise and respond to issues in real-time – as they occur.

"A wide range of risks are now being played out in the cyber domain and pose a real and growing threat to the energy and utilities industry."

- Name withheld, Client

> "Disruption of critical infrastructure has tremendous psychological impact as large-scale disruption to civilian facilities leave a profound impact".
>
> - Name withheld, Client

Background

As an integral part of national critical infrastructure, cyber security has been a priority for the client (a public sector enterprise) for some years. However, recent high-profile attacks on operational technology uncovered significant gaps in security posture. With the threat landscape rapidly advancing, and mounting cost of mitigating security breaches, a new approach to cyber defense for Industrial Control Systems became an urgent requirement. As attacks continue to increase in volume and sophistication, critical infrastructure owner had to evolve.

The client acquired significant cyber threat and risk intelligence data from multiple sources. However, despite application of available intelligence to various security controls, client continued to experience security incidents.

Business challenges

In the context of an increasingly sophisticated threat landscape, the client was essentially worried about impact of an attack on its rather infrequently-updated and under-protected SCADA network. Specifically, it was concerned about fast-moving and automated threats, like ransomwares/cryptwares, that have the potential to jeopardise operations at the earliest opportunity. With a security stack that primarily depended on border defense based on rules and signatures, the client was unable to take a proactive approach when it came to cyber defense.

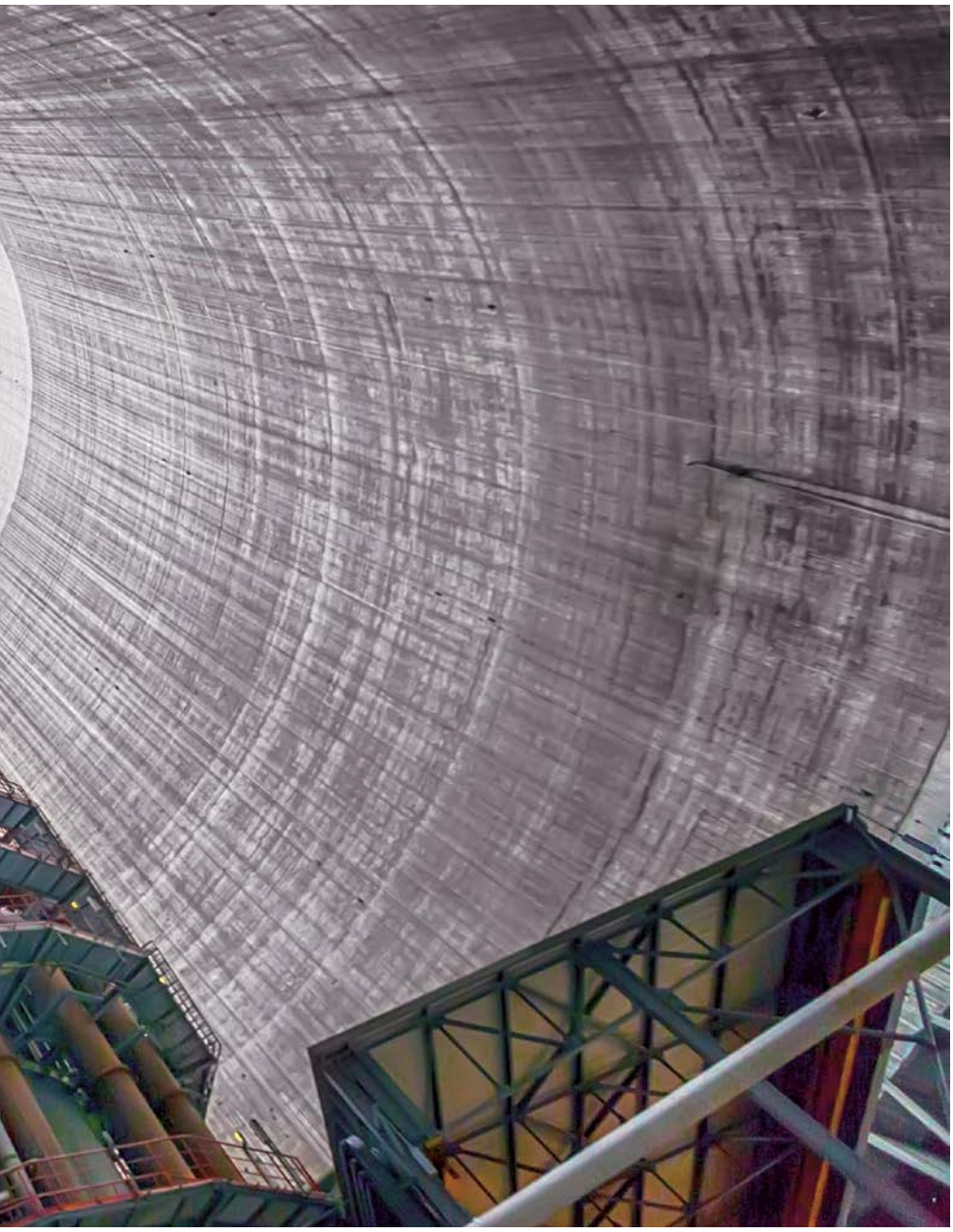
In addition to confronting evolving cyber threats, the client was affected by tight budgets and lack of resources, complex processes, and a need to stay up-to-date with latest regulatory mandates, attack methods, and technologies.

Additionally, client felt it lacked visibility into its internal network. It wanted a solution that could provide insights into the behaviours of users, devices, and the network as a whole. Keeping resource constraints, training and integration needs in mind, the client set out to identify an easy-to-deploy solution to combat next-generation threats, including zero-day and advanced persistent threats, to supplement legacy security defenses across the corporate infrastructure.

vehere

"PacketWorker's Machine Learning technology has proven instrumental in terms of providing visibility of devices we didn't even know we had on our network".

- Name withheld, Client



Solution – PacketWorker 10G

Following a quick installation, security analysts were able to identify abnormal activities and disrupt exploitative actions in the early stages, before any damage was done. It also provided the client with total network visibility. From day one, PacketWorker started to analyse users, devices and network behaviours, in real time and, detecting anomalies pertaining to cyber risks.

PacketWorker demonstrated the inherent value of its self-learning threat detection abilities, uniquely capable of forming an understanding of normal and abnormal behaviours without any prior knowledge.

PacketWorker proved to be an effective cyber threat detection and response solution that helped the client respond swiftly to cyber threats. It facilitated efficient resolution of identified security incidents with concrete evidence, actionable intelligence and response workflow integrations.

Machine Learning is a principal ally in terms of defense of assets from cyber-criminals and malicious insiders. The technology detects the slightest of abnormal behaviours across network in real time, including 'unknown unknowns', enabling the security team to detect and respond to attacks before any harm befalls.

Benefits

With PacketWorker's Machine Learning abilities, the client re-established trust in its security operations to defend itself from evolving and increasingly automated attacks. Since the solution prioritises detection outcome by potential gravity, it enables security professionals to optimise their resources for increased effectiveness.

PacketWorker allows the security and risk management teams to proactively assess security postures and then sets up detection rules to maintain their edge over malicious behaviours besides using advanced predictive analytics to detect unknowns. All this is done without any disruption to ongoing business processes.

Exemplary performance and detailed contextual availability enabled the cyber security team to focus on responding to threats quickly, minimising operational and business impact.

Over time, the client was able to identify and alleviate threats more efficiently compared to the previous year.