Case study

Manufacturing

Summary

Industry/Organisation

Manufacturing

Challenges

- Lack of consistency and accuracy in cybersecurity monitoring of organisational assets
- Inability to detect anomalous events
- Inadequate context when it came to analysing security events
- Absence of monitoring of IT-OT integration for real-time risk detection and response

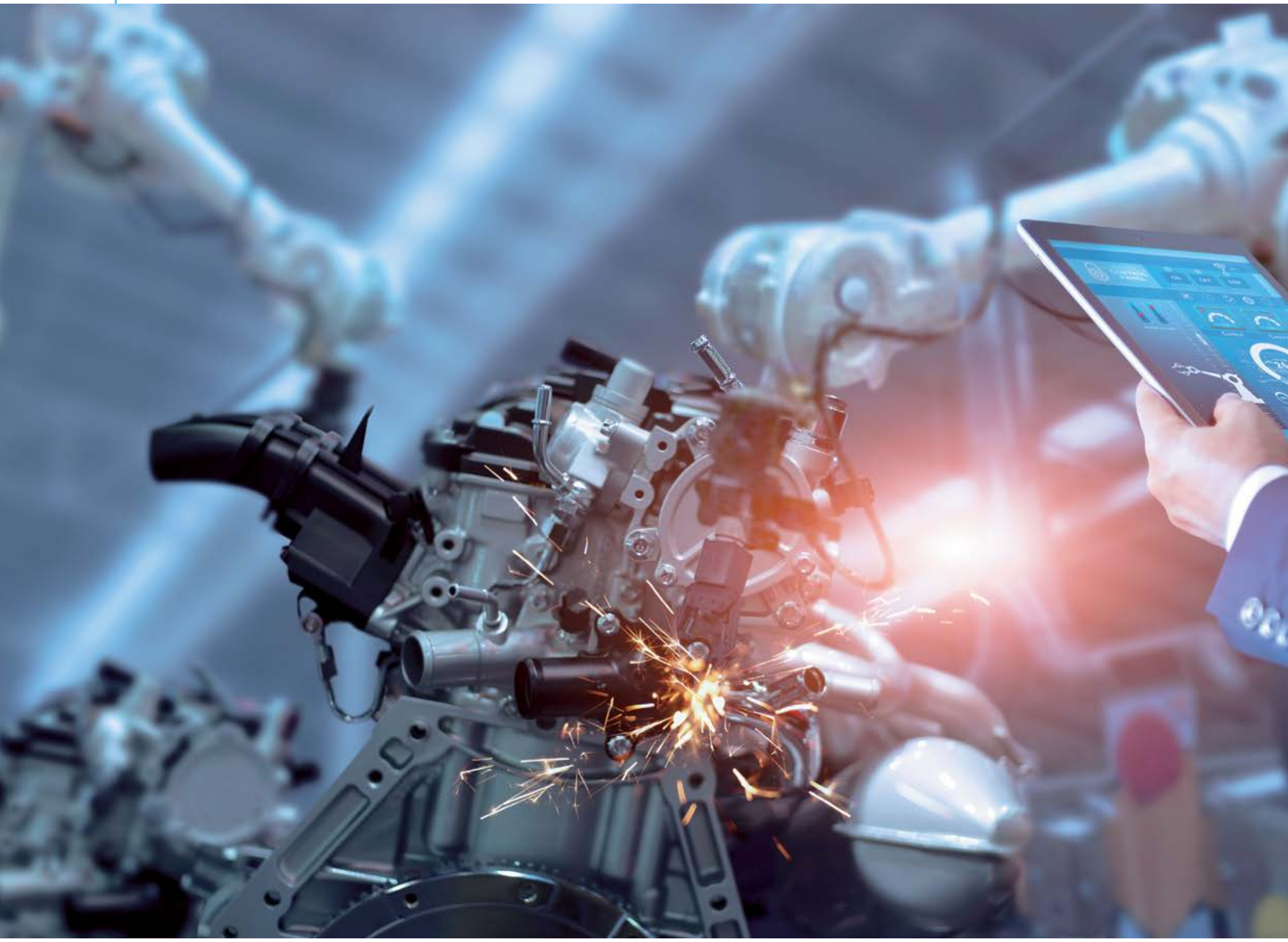
Solution

PacketWorker 1G

Benefits

- 100%-visibility into cyber activities of organisational assets
- 70% improvement in network/ security issue triages
- Real-time detection of anomalous events and activities

> “Many manufacturing powerhouse companies fear disruptive attacks the most, regardless of whether it is done by internal or external attackers.”
>
> - Name withheld, Client



ICS and SCADA

ICS is an umbrella term covering many historically different types of control systems such as SCADA (supervisory control and data acquisition) and DCS (distributed control systems). Also known as IACS (Industrial automation and control systems), they are a form of operational technology. In practice, media publications often use 'SCADA' interchangeably with 'ICS'.

Background

Cyber attacks against industrial control systems (ICS) weren't noticeable till about recently, and were purportedly less frequent than IT attacks because numerous ICS attacks don't get revealed. However, ICS are presently among the top targets of cyber threats and attacks worldwide. Malware infection, ransomware and other attacks, on ICS assets can have serious ramifications. With IT-OT integration, the risks of cyber-attack on ICS endpoints are expanding.

Interconnections between control systems and public networks deliver important business benefits. However, without appropriate security measures, it can compromise control system availability and cause service disruptions.

A 2017 industry report found that attacks targeting ICSs have increased by >110% compared to the previous year. While, a 2018 SANS study found that 69% of ICS security practitioners believe threats to the ICS systems are high or severe and critical.

Business challenges

Traditional solutions don't work in ICS/SCADA environments. The customer needed technology to monitor their enterprise IT and SCADA networks as coherent entities of the enterprise network. Given the mission-critical nature of assets deployed in ICS environment, enhancing or upgrading these systems with preventive security controls was deemed unacceptable.

"The energy sector has become a major focus for targeted attacks and is among the top-five most targeted sectors, worldwide".

- Name withheld, Client

The threat to the energy/manufacturing sector is serious and it's becoming increasingly difficult to guard against lateral movements as a result of integration of IT with operational technology (OT) systems. This integration offers attack vectors the chance to seep into OT networks, which were unmonitored and unprotected, leaving the company with little technological help to effectively respond to such risks.

The client's in-use tools offered little or no visibility into network traffic and the security operations were found to be inadequately prepared to manage never-before-seen threats in SCADA environment. The client required a solution that would give comprehensive visibility into the network, and also lower some of the burden their security team was carrying.

> "PacketWorker has added another dimension of refinement to our defense systems and productively identified threats with the potential to disrupt our networks".
>
> - Name withheld, Client

Solution – PacketWorker 1G

Following a tightly-guarded security event whose remnants were detected by PacketWorker during a later proof-of-concept trial followed by a pragmatic policy review cycle, the company decided to adopt PacketWorker 1G for their IT and OT networks.

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

ICSs confront various cybersecurity threat vectors with varying degrees of loss potential, ranging from non-compliance to disruption of operations, and beyond.

Cost of post-event mitigation is significantly higher, not to mention the financial loss. Hence, it is a prudent strategy to 'efficiently detect and respond swiftly' to security threats in ICS networks to keep costs low.

PacketWorker is a fundamental innovation that views data from an ICS network in real time and sets up a developing pattern for what is normal for operators, workstations and automated systems within that environment. With PacketWorker's Machine Learning, organisations can distinguish and react to emerging threats in real time. Advanced behavioural analysis can detect even previously unseen novel or custom-fitted attacks, regardless of whether they originate in the corporate IT or OT domains or navigate between them.

Total prevention of all cyber compromises is not a realistic goal, but, if identified early enough, threats can be alleviated before they become full-blown crises. PacketWorker's technology can be deployed across both IT and OT environments to provide full coverage to an organisation.

Benefits

PacketWorker has rapidly turned into an essential part of client cyber security strategies, because of its one-of-a-kind methodology and capacity to detect emerging threats before they have the potential to cause significant damage.

On deploying PacketWorker, the organisation was immediately alerted of potential intrusions inside its systems that had already bypassed its other security tools. Following an easy implementation process, it now currently utilises PacketWorker to persistently analyse the overall health of its system and to spot sporadic activities that have a high likelihood of being pernicious, hazardous or non-compliant.

The advanced cyber defense technology allows clients to secure themselves from the most deceptive attacks that endanger critical infrastructure systems, regardless of whether those threats originate from within or outside the organisation.