vehere

Case study

Energy and Utilities

> “We have a lot of suspicious communication that we don’t necessarily get time to analyse but PacketWorker helps focus our efforts just on the riskiest ones and enables us to safely investigate their true nature and intent”.
>
> - Name withheld, Client

Summary

Industry/Organisation

Energy and Utilities

Challenges

- Need to improve detection rates without impacting business continuity or taking excessive measures to lock down machines
- Enhanced compliance posture
- Long and tedious operations and security investigations lacked visibility
- Concern about prevalence of fast-moving, automated attacks

Solution

PacketWorker 10G and professional services

Benefits

- Gained real-time operational visibility
- Reduced operational disruption and remediation costs
- Consolidated intelligence and reporting
- Ensured immediate and significant drop in attacks

Background

Cyber security and compliance continues to be a challenge for many energy sector organisations. Hackers, including both state and non-state actors, are getting progressively advanced in their attacks, making it increasingly hard to keep up with the latest threats.

Analysts noted an increase of >60% in hacktivism targeting the energy sector. A 2018 survey of IT professionals across the oil, gas, utility and energy sectors found that fewer than half believed their organisations could immediately detect a cyber-attack, although ~65% believed that they were a target. Furthermore, 81% believed that attacks could do 'serious damage'. All the statistics pointed to a clear state of uncertainty with the prevalent style of risk management and adoption of security controls.

Business challenges

Although there has been an increased focus on cyber security in the recent years, threats against the energy sector continue to go undetected for an average of six months.

A key reason behind this is alert overload. Standard cyber security deployments generate thousands of alerts per week, but the client organisation only had the resources to investigate ~5-6% . With 20% reliability rate, the client believed they were wasting precious time and money each year chasing false positives or performing investigations with inadequate insights.

The main hindrance faced was that users could not get a context or insights from multiple security solutions quickly enough and in one place to perform an efficient investigation. This is precisely why adopting Machine Learning can help improve versatility cyber hygiene and compliance.

The client's previous tool set had led to a number of challenges, including:

- Slower threat detection and response due to too many disparate tools, too much information and the need for a lot of manual correlation to find the right data.
- Limited data retention capabilities.
- No compatibility with other technologies.

To protect its digital infrastructure, the client required situational awareness of its security posture, context and relevant insights for its departments and stakeholders.

Benefits

PacketWorker empowered the client to detect and neutralise cyber threats in real time. PacketWorker immediately affirmed that the bulk of client infrastructure was clean but did detect the presence of a certain malware in their network and allowed them to zero in on a specific workstation for remediation.

From the first day of deployment, clients have seldom had issues with false-positives of the rule engine. This has given them the certainty to resolve security incidents.

With large volumes of data transfer going on daily, the client was unable to analyse everything.

Exemplary performance and high detail availability enabled the cyber security team to respond to threats quickly, minimising operational and business impact.

PacketWorker facilitated simplification of implementing big data-led security analytics in a secops environment by eliminating the considerations around event rate and the need for collectors for different applications/processes. It is a platform for readily-available structured data lifted from the source – Packets on the network.

> “No business in the energy industry is immune to security issues and fear of disruptive attacks, regardless of whether it is done by internal or external attackers.”.
>
> - Name withheld, Client

Key facts and figures

- Energy attacks went up by 20% between 2017 and 2018. This trend is expected to continue as governments pours more resources into cyber warfare
- 75% of companies in the oil, gas and electricity reported a cyber attack in 2018. Intruders were able to bypass protections that were in place.
- Cyber-attacks against energy companies usually take months to discover.
- 48% of energy and utility CEOs think a cybersecurity attack is inevitable, sooner or later.

Solution – PacketWorker 10G

Deployed in promiscuous mode to monitor networks, PacketWorker proved to be an effective detection and response solution that helped respond swiftly to cyber threats. It facilitated efficient resolution of identified security incidents using concrete evidence, actionable intelligence and response workflow integrations.

The client had an account that was the target of an email-based attack. PacketWorker put the right protection in place and stopped the ransomware from deploying.

PacketWorker was immediately able to identify a lot of malicious malware that had been entering the client’s environment. The client saw the cost savings generated in terms of preventing the attacks and the gains in efficiency resulting from PacketWorker.

PacketWorker does not require weeks and weeks of consulting to implement and the speed at which it can operate and mitigate risk is a key differentiator.

Clients often need easy access to real-time data and actionable information to understand where they need to focus.