paloalto NETWORKS | CPSP

CASE STUDY

Trustwave

U.K. Billion-Dollar Oil Enterprise Establishes a Safer Network with a Next Generation Security System Powered by Trustwave

Industry Oil and Gas (Exploration and Production)

Company Oil and gas company

Challenge
Move to a leading-edge Managed Security Services (MSS) system for endpoint protection and network monitoring that includes proactive threat detection

Answer
Create an intelligent security system that blocks network assaults using Trustwave Managed Security Services, underpinned by Palo Alto Networks Cortex XDR technology

Results
- Improved protection capability, reducing exposure and possible remediation activities.
- Reduced average time to detect and respond to threats (8x faster as reported by Palo Alto Networks **).
- Increased threat containment actions without degrading performance.
- Enabled 24x7x365 Managed Security Services protection using artificial intelligence and continuous threat hunting.

Products and Services
Trustwave, a Managed Detection and Response (MDR) Palo Alto Networks Partner

- **Professional Services**
  Simulated attack
  Deployment of the Cortex XDR agents
  Tuning and base-lining methodology
  Trustwave subject matter experts
  Digital Forensics and Incident Response (DFIR)
- **Managed Services**
  Managed Threat Detection and Response Services

Palo Alto Networks Products:

- Cortex XDR, Cortex Data Lake

Organization

A U.K. billion-dollar oil and gas exploration/production corporation produced (and manages the operations) of 40+ gas fields, with some anchored offshore and one floating rig.

As a well-respected corporation in the industry, the corporation is committed to achieving some of the most aggressive reductions in CO2 emissions within the next three years. It is also dedicated to the safety of its employees and the security of the company's operations.

In 2020, these goals were challenged like never-before.

2020 and 2021 Challenges

Oil and gas corporations have increasingly become a prized target of cyder-attacks that disrupt operations, cause physical damages, and create safety issues. Whether hackers use spyware targeting bidding data of fields, malware infecting production control systems, or denial of service that blocks the flow of information through control systems, the cyber terrorists are becoming more dangerous to environmental safety, and human lives.

With a sharp fall in oil prices in 2020 and continuing in 2021, the oil and gas corporation leaders also recognized the need for maximizing their return on all investments, including the company's continual crucial investment in cybersecurity.

Decommissioning Under-performing MSS

The corporation was using a well-known Managed Security Service (MSS) for their endpoint protection and network monitoring, but the leaders required more for their money and greater security assurance.

They decided to decommission the existing service.

The corporation engineers outlined the requirements for the new security solution including:

- Machine learning and artificial intelligence
- Accelerated investigations
- 24/7/365 monitoring
- Endpoint Detection and Response (EDR) capabilities
- Proactive threat posture with machine capabilities
- Predictable costs

Furthermore, with a small security team, the company was looking for ways to reduce the number of false positives and provide manageable, actionable intelligence for real threats.

The IT leadership team met with Palo Alto Networks (PAN) account executives to review the latest security product capabilities. After examining Palo Alto Networks Cortex XDR, they selected the software platform for its unification of the VPN, endpoints, and cloud data, plus the software's machine learning-based behavioral analytics.

The company now needed a stronger MSS partner to complete the solution as a standalone Cortex XDR was not a viable option.

The oil and gas company selected Trustwave, known for its security consulting expertise and its complete, proactive, managed threat detection and response (MDR) services.

In 2020, both International Data Corporation (IDC) and Forrester validated Trustwave customer satisfaction and superior services. *

Trustwave is also a Management Detection and Response partner accredited by Palo Alto Networks.

Outmaneuvering Cyber Saboteurs

With Trustwave on board, the company and Trustwave engineers kick-started the project with discovery, engaging Trustwave SpiderLabs services.

"As part of the SpiderLab Service, our experts employ reverse malware engineering, learnings from hundreds of similar customers, and penetration testing to better understand current vulnerabilities that may not be self-evident," explains Damian Hicklin, EMEA Director, Consulting and Professional Services, Trustwave.

Armed with this knowledge, Trustwave solution architects supercharged the Cortex XDR platform through customized tuning of Cortex XDR, resulting in enhanced prevention, visibility, and detection of attacks.

Trustwave also quickly deployed its Managed Security Services including Security Information and Event Management (SIEM), network access control, detection and response for endpoint protection, and application control.

To help manage their costs and provide for predictable operating expenses, the company opted for a pay per use model.

"Trustwave pay-per-use model takes advantage of the public cloud economics. Customers only pay for what's needed, as it is needed, significantly reducing costs and simplifying procurement processes," says Richard Elphick, Account Executive, Trustwave.

Deployment Complication and an Innovative Fix

As Trustwave engineers worked with the oil and gas corporation to roll out the new solution, they encountered an issue related to network bandwidth for the offshore gas fields. When out to sea, an oil rig's bandwidth is generally limited to between 5 Mbps to 10 Mbps on any given vessel.

To address this issue, and reduce bandwidth load when distributing content, the team tapped into the Cortex XDR enhanced content update algorithm. The algorithm allows agents on the local area network (LAN) to retrieve the new content version from other agents that have already retrieved it.

Results that Exceed Expectations

With the new solution's automated root cause analysis and unified incident report capabilities, the oil and gas corporation has the potential to cut down its alerts by as much as 98% as documented by Palo Alto Networks.**

Furthermore, the company has greatly enhanced its visibility of all the company's Information and Communication Technology (ICT), including computers, networks, hardware, software, satellite, and more.

The replacement of their legacy system and the consolidation of security software has decreased the total cost of ownership (TCO).

"Our client is delighted with the results. The combination of the Trustwave MDR Services, alongside PAN Cortex XDR technology, reduces the number of false positives that their engineers need to triage internally. When they receive an alert, it is enriched with the actionable intelligence needed to speedily resolve the incident. At a time when there is a skill shortage, and the attack surface is expanding, giving time back to their technologists is huge," states Hicklin.

"The new cybersecurity solution has given the company a sophisticated approach to prevent (or contain) an attack. We increased the assurance of their employees' safety and business without disruption, while moving to a predictable cost model."

— Damian Hicklin, EMEA Director, Consulting and Professional Services, Trustwave

Notes:

* https://www.trustwave.com/en-us/resources/library/documents/the-forrester-wave-global-managed-security-services-providers-q3-2020/

** https://www.paloaltonetworks.com/cortex/cortex-xdr

paloalto® NETWORKS | CPSP

April 2021