Case Study

Reduce mean time to remediate (MTTR) from weeks to hours

Oil and gas company adopts Skybox Vulnerability Control to analyze their attack surface without impacting network operations. The company also increased the accuracy, efficiency, and effectiveness of their vulnerability remediation process.

Learn how you can:

- Reduce false positivity rates.
- Increase vulnerability remediation accuracy, efficiency, and effectiveness
- Eliminate network disruption through passive and scanless vulnerability assessment.
- Reduce scanning costs and business disruption.
- Automate and optimize attack surface analysis.

One of the world's largest petroleum refining companies, this company must address cybersecurity threats as soon as they are identified. However, active scanning causes vulnerability remediation delays and subsequent risks. They chose Skybox Vulnerability Control to provide an accurate, continuous view of the attack surface.

Business challenge

Identify, prioritize, and remediate vulnerabilities faster

Headquartered in Spain and operating in 28 countries, this company sought an alternative to traditional scanning that wouldn't impact network operations. The security team needed continuous monitoring to **identify vulnerabilities faster and shorten the time frame for remediation.** They also needed to reduce the 20 percent false positive rate generated by scan results. With thousands of servers and disparate firewalls, load balancers and routers, the company needed a more thorough solution.

> "We no longer have to deal with false positives," said the CISO. "We've been using Skybox Vulnerability Control for more than a year, and our false positive rate has dropped significantly from the 20 percent we were experiencing. We can now prioritize our efforts on deploying patches."

Solution

Automate and optimize attack surface analysis to reduce costs

The company chose **Skybox Vulnerability Control** to **obtain full visibility and context of their attack surface** across their network, cloud, and security infrastructure. With this view, they find where they are exposed to cyber-attacks, quantify the risks of exploitation, prioritize vulnerabilities, and obtain optimal remediation options to reduce the highest levels of risk. Using Skybox, the company conducts passive and scanless vulnerability assessments that eliminate network disruptions, detect vulnerabilities on traditionally "unscannable" devices and zones, and prioritize and remediate vulnerabilities daily. The company continues traditional active scanning but no longer needs to run active scans as often or scan critical services, reducing the costs associated with running regular scans.

The network operations and security teams benefit from improved workflow communications, as each team has access to a common intuitive dashboard highlighting immediate remediation actions. No more guessing, unnecessary patching, or wasted work.

Results

Reduce MTTR and improve operational efficiency

Using Skybox Vulnerability Control, the company identifies vulnerabilities and remediates them faster and more accurately, **reducing the window of exposure from weeks to hours.** Passive and scanless vulnerability assessment eliminates network disruption, enables access to critical services, provides daily, accurate vulnerability intelligence, and reduces costs. The solution significantly reduces false positives and allows the team to shift scarce security resources to other priorities.

Through Skybox automation, the company has continuous vulnerability discovery and reporting, thereby improving operational efficiency.