censys & NOS

How Major Telecom Provider NOS Reduces Cyber Risk and Investigates Threats with Censys

INDUSTRY:
Telecommunications

REGION:
Portugal

SIZE:
1,800+ employees

THE CHALLENGE:
NOS needed a way to swiftly mitigate risks, protect its brand reputation, and maintain high cyber risk ratings amid a rapidly evolving threat landscape.

THE GOAL:
Gain comprehensive visibility into all internet-facing assets and investigate threat actor infrastructure to minimize exposure.

THE OUTCOME:
Censys enabled NOS to aggregate and analyze internal, cloud, and customer-facing assets, significantly improving threat detection, response, and overall cyber risk posture.

THE CHALLENGE:

Gaining Full Visibility into a Vast Attack Surface

NOS is a leading Portuguese telecom and technology provider that manages approximately 2 million registered IP addresses. As telecoms are prime targets for cyberattacks, due to their expansive networks and critical infrastructure, NOS required complete visibility into their attack surface to mitigate risks effectively. The complexity of their environment—including cloud services, IoT systems, and new 5G infrastructure—added layers of risk, amplifying the need for a holistic security solution.

NOS aimed to enhance their ability to identify exposed assets and prioritize high-risk vulnerabilities by implementing a centralized **Attack Surface Management (ASM)** solution. Faced with a high volume of alerts and false positives from existing tools, they needed a solution that would prioritize real threats and guide remediation efforts accurately.

THE SOLUTION:

Censys Attack Surface Management and Search

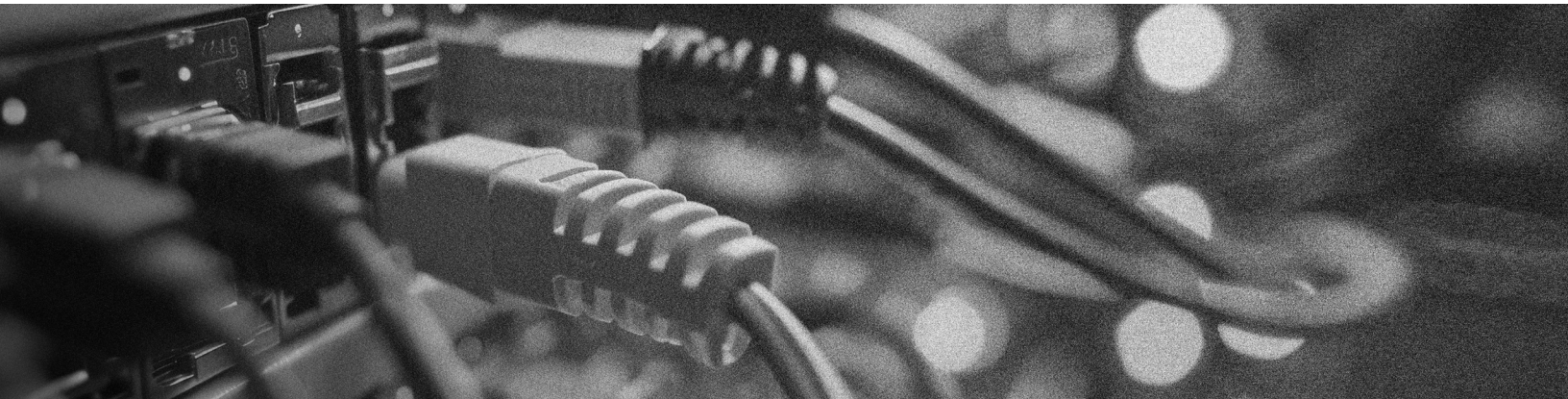
After evaluating multiple vendors, including Palo Alto Xpanse and Shodan, NOS chose Censys for its superior visibility, advanced protocol analysis, and unparalleled depth in mapping threat actor infrastructure. Censys provided NOS with a comprehensive view of their attack surface. On average, Censys identifies 65% more attack surface than leading competitors.

> **With Censys, we could see details about the attacker's infrastructure, such as web servers, certificates, and other equipment, allowing us to expand our view beyond just the targeted site. Censys is like Shodan on steroids.**
>
> Pedro Zeferino, Head of Cybersecurity, NOS

Complete Asset Discovery: Uncovering Unknown Exposures

Upon onboarding, Censys quickly aggregated data across NOS's three major cloud providers, revealing previously unknown assets connected to their attack surface. This immediate visibility enabled NOS to inventory, patch, or disable these exposures, closing critical gaps that could have served as entry points for attackers.

Using Censys, NOS also detected assets that were operating outside security controls like firewalls. They ensured these were swiftly brought back into compliance and as a result, bolstered security standards across their network.



Immediate Response to CVEs: Real-Time Remediation

Censys plays a pivotal role in NOS's real-time response to vulnerabilities, continuously scanning their IPs and public infrastructure to identify exposure to newly disclosed CVEs. Unlike traditional vulnerability management tools that lack real-time search, Censys' capabilities allowed NOS to act immediately during critical incidents, such as the recent OpenSSH vulnerability. The team mapped all exposed OpenSSH services, pinpointed affected versions, and mitigated the threat before the CVE was officially published.

> **Only with Censys could we narrow down the list of vulnerable OpenSSH services before the CVE was released.**
>
> Diogo Gonçalves, Cyber Defense Team Lead, NOS

Censys also enabled NOS to monitor ongoing risk scenarios, such as Remote Desktop Protocol (RDP) exposure, which directly impacts their cyber risk ratings and overall security posture.

Quantifying Cyber Risk: Enhancing Cyber Risk Ratings and Reducing Business Impact

For NOS, managing cyber risk goes beyond technical mitigation. By using Censys, NOS can identify exposed vulnerabilities that could negatively impact their cyber risk ratings, allowing them to address these issues proactively. This proactive approach not only reduces the likelihood of incidents but also enhances NOS's credibility with stakeholders and customers.

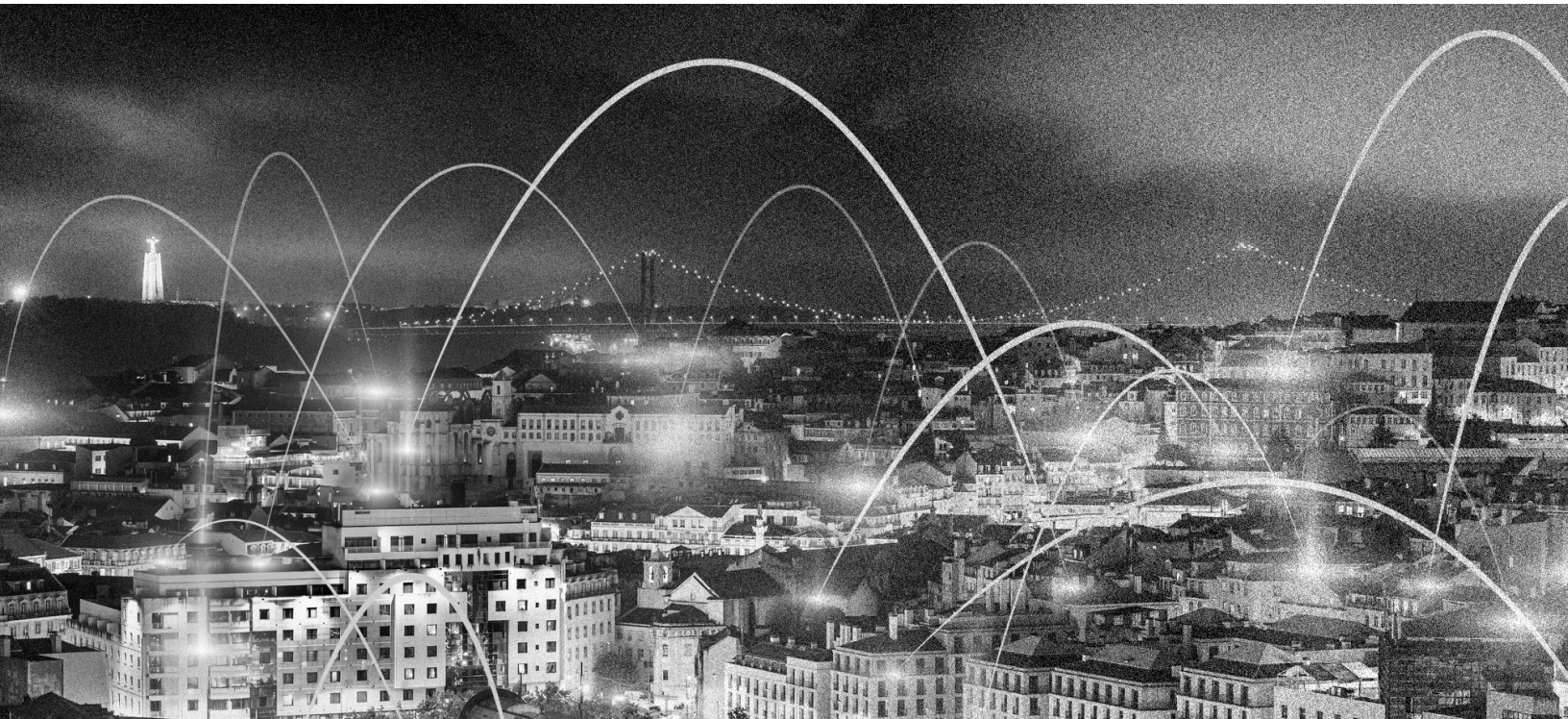
Censys' risk framework helps prioritize vulnerabilities based on active exploitation, ensuring that NOS addresses the most critical risks first. This prioritization has been vital in maintaining their security ratings and mitigating the potential financial impact of cyber risk.

Safeguarding the Brand: Identifying Malicious Infrastructure

NOS uses **Censys Search** for threat hunting and incident response, allowing them to analyze and track threat actor infrastructure, including Command and Control (C2) systems and other attacker assets. This intelligence provides NOS with a strategic advantage, enabling them to protect their own infrastructure and anticipate broader campaigns that may affect other organizations in the region.

> **When targeted, we can pinpoint the attacker's infrastructure and identify other equipment they use, giving us the intelligence to stay ahead.**
>
> Pedro Zeferino, Head of Cybersecurity, NOS

Additionally, NOS leverages Censys to detect domain spoofing through innovative methods like Favicon-based searches, identifying and mitigating malicious sites attempting to impersonate their brand.



Enhancing Third-Party Risk: Securing the Entire Ecosystem

Given the interconnected nature of telecom operations, managing third-party risk is crucial. NOS collaborates with numerous partners, and Censys has been instrumental in evaluating the security posture of these third-party entities. In one notable instance, NOS identified a ransomware attack targeting a partner and quickly blocked access, preventing further spread and cascading impacts on their network.

> **With Censys, we assess risks within our domain and beyond, securing our partnerships and public cloud environments.**
>
> Diogo Gonçalves, Cyber Defense Team Lead, NOS

Conclusion

By adopting Censys, NOS has gained unprecedented visibility into their global attack surface, enabling proactive defense against both known and emerging threats. The combination of comprehensive asset discovery, rapid vulnerability response, and advanced threat intelligence equips NOS with the insights needed to strengthen their security posture, safeguard their brand, and manage cyber risk effectively.