Immediate Threat Reduction for *Skyreach Telecom

Given the sensitive nature of the details shared in this case study, our customer chose to remain anonymous. We have thus assigned a *pseudonym (Skyreach Telecom) for our customer herein.

INTRODUCTION

In today's world, profitable organizations are pressed to meet their competition in digital evolution and advancements. With every technology they create and adopt comes an ever-increasing number of vulnerabilities and potential threats. To maintain a competitive advantage, profitable companies must evolve to compete in two areas: against their markets and against cyber threat actors. The competitive logic is not so different. For the latter competition against cyber threat actors, as much as the former, they need technology that will enable them to think ahead and outcompete with their security defenses, else they will drown under the weight of their risks.

*SKYREACH TELECOM

*Skyreach Telecom, a leading telecommunications company, invested in **various technologies related to vulnerability and threat management**; however, they were still struggling with some serious problems:

1. Continuous asset discovery across an ever changing and fragmented business environment
2. Combining, filtering, and correlating threat and vulnerability intelligence from different sources
3. Prioritizing thousands of vulnerabilities for remediation
4. Collaborating with their infrastructure team on vulnerability remediation and risk reduction

The problem became unmanageable in such a way that *Skyreach Telecom was **constantly overburdened by long lists of unresolved remediations**, constant arbitration with their infrastructure team, and a dangerous risk posture. The deluge of security alerts to required manual investigations and vague prioritization was also too much to handle.

To address these challenges, *Skyreach Telecom decided to try HivePro Uni5: Threat Exposure Management, and they were quick to implement HivePro Uni5 shortly after. Their story is detailed below.

CASE STUDY OVERVIEW: *SKYREACH TELECOM

Size	Location	Revenue
15k Employees	EMEA Region	$20B+

Challenges Before HivePro Uni5

- ☒ 7 Days to Uncover Vulnerabilities
- ☒ 14 Days to Fix Critical Vulnerabilities
- ☒ 30 Days to Fix Critical Assets
- ☒ Active Targeting at 5% of Open Vulnerabilities
- ☒ Critical Assets At Risk for 90 Days
- ☒ 60 Day Mean Duration of Threat Exposure
- ☒ Quarterly System Update Expenses: $50,000

Impacts After HivePro Uni5

- ✓ 5 Days to Uncover Vulnerabilities
- ✓ 10 Days to Fix Critical Vulnerabilities
- ✓ 20 Days to Fix Critical Assets
- ✓ Active Targeting Down to 3%
- ✓ Critical Assets At Risk for 60 Days
- ✓ 45 Days of Mean Duration of Threat Exposure
- ✓ Quarterly System Update Expenses: $45,000

THE CHALLENGE

> *“Before implementing HivePro Uni5, we struggled with asset oversight and prioritizing the most important vulnerabilities in a timely manner.”*
>
> **Senior Director, SOC**

*Skyreach Telecom took on average, 7 days to uncover vulnerabilities across 5000 known assets. On the surface, this metric is relative to any company’s risk appetite, but for *Skyreach Telecom this metric was a problem. It was indicative of a few issues they were suffering with internally which include but were not limited to fragmented remediation processes, low asset visibility, and difficulties in correlating the right threat and vulnerability intelligence.

Without automated asset discovery and vulnerability prioritization technology, it took *Skyreach Telecom 14 days to fix critical vulnerabilities and 30 days to fix critical assets. Critical assets are herein defined as assets that are more sensitive to downtime because they are necessary to maintain business continuity. This was a problem for *Skyreach Telecom because the longer they waited to fix critical assets, the higher their exposure window became. This difficulty added on to their troubles with adequately defining relevant threat intelligence feeds.

> *"Despite our best efforts, the inefficiencies of our previous vulnerability management approach left us exposed to potential cyber attacks."*
>
> **Lead Analyst, SOC**

THE SOLUTION

*Skyreach Telecom was introduced to Hive Pro through one of their partners. They were able to **implement a PoC in less than 2 weeks** from sign-off to initiation and the results were immediate.

With HivePro Uni5 TEM, the Security team at *Skyreach Telecom implemented a **continuous asset search** according to their compliance and risk management needs. Given their stronger understanding of their variable asset environment using HivePro Uni5, *Skyreach Telecom reduced their time to uncover critical vulnerabilities from 7 days to 5 days, a 30% improvement. This operational metric is constantly improving over time.

Additionally, *Skyreach Telecom immediately **reduced their time to fix critical vulnerabilities** from 14 days to 10 days, and reduced their time to fix critical assets from 30 days to 20 days. One of their strongest blockers to **fixing critical vulnerabilities and assets** was their friction with the Infrastructure team. The HivePro Uni5 TEM platform was able to help in two critical ways:

1. The HivePro Uni5 TEM platform allows for **cross-functional stakeholders**, like the Infrastructure team to maintain visibility, inherit responsibilities and collaborate on several processes (i.e. ongoing and new assessment, tests, remediation processes; remediation efforts)
2. The HivePro Uni5 TEM platform **generates actionable and evidence-based reports** for stakeholders at all levels of relevance and seniority.

As a result of a few key beneficial features of the HivePro Uni5 TEM platform, *Skyreach Telecom reduced their **mean duration to threat exposure** from 60 days to 45 days. The platform enabled them to discover assets thoroughly, build focused threat and vulnerability intelligence, prioritize vulnerabilities accordingly and to collaborate with the necessary drivers for vulnerability remediation.

The solution provided visibility into *Skyreach Telecom’s security posture and helped the company to improve its risk and operational metrics.

> *"HivePro Uni5 TEM is what our SOC was looking for. It’s affordable, practical and useful. We have Tier 1 analysts who can immediately understand and use the platform. Our CISO can also relay improvements to our risk management program in a more informed way."*
>
> **Lead Analyst, SOC**

IMPROVED RISK MANAGEMENT & REDUCED COSTS

With HivePro Uni5, *Skyreach Telecom was able to **improve its risk management** by reducing the average duration to fix critical assets with vulnerabilities, reducing the time to uncover critical vulnerabilities, and reducing the average time to fix critical vulnerabilities. This improved risk management allowed *Skyreach Telecom to better protect its critical assets and reduce the risk of cyber attacks.

At Hive Pro, we were excited to learn that *Skyreach Telecom additionally reduced their quarterly system update costs from $50,000 to $45,000, accumulating in savings of $20,000 a year with which they were able to use towards process efficiency and horizontal upskilling across the cybersecurity function.

The result of *Skyreach Telecom's implementation of HivePro Uni5 Threat Exposure Management is and continues to be outstanding. With HivePro Uni5, *Skyreach Telecom is able to **improve its risk management, enhance its operational efficiency, and save costs.** HivePro Uni5 allowed *Skyreach Telecom to proactively manage its security posture and reduce its overall security risk. *Skyreach Telecom's implementation of HivePro Uni5 Threat Exposure Management serves as a best practice for organizations looking to **improve their cyber security posture and reduce their risk of cyber attacks.**

Below, we include a table expressing *Skyreach Telecom's process improvements across several factors.

Metric	Before	After	Results
Avg. duration to fix critical assets with vulnerabilities	30 days	20 days	33%
Time to uncover critical vulnerabilities	7 days	5 days	28%
Avg. time to fix critical vulnerabilities	14 days	10 days	29%
Proportion of known vulnerabilities being actively targeted	5%	3%	40% reduction
Avg. length of time critical assets at risk	90 days	60 days	33%
Fraction of critical assets with approved exceptions	2%	1%	50% reduction
Proportion of critical assets with vulnerabilities & no mitigation	3%	1%	67% reduction
Fraction of assets under vulnerability management coverage	95%	98%	3% improvement
Median time to identify vulnerabilities	5 days	4 days	20%
Avg. time to fix vulnerabilities	10 days	7 days	30%
Mean duration of exposure	60 days	45 days	25%
Total number of approved exceptions	50	40	20% reduction
Percentage of assets unable to be patched	2%	1%	50% reduction
Mean duration of exposure	45 days	35 days	22%
Proportion of cloud assets with vulnerabilities	5%	3%	40% reduction
Expenses incurred every quarter for system updates	$50,000	$45,000	10% reduction

Achieve immediate threat reduction for your telecommunications company

Request a demo today!

Hive Pro

Get in Touch
Hive Pro Inc. | info@hivepro.com | www.hivepro.com

Contact Us

Start Your Free Trial

Read Our Blog