CASE STUDY

Oil & Gas Service Provider Elevates Security with Crowdsourced Penetration Testing

About NOV

NOV is a worldwide leader in the design, manufacture and sale of equipment and components used in oil & gas drilling and production, the provision of oilfield inspection and other services, and supply chain integration services to the upstream oil and gas industry. NOV has more than 27,000 employees and had revenues of $5.52B in 2021.

Key challenges

- Point-in-time penetration tests leave time gaps between security tests
- Results from prior penetration testing vendors difficult to compare, due to variability in methodology and reporting framework
- Few high, critical vulnerabilities found due to limited penetration testers per engagement
- No real-time access to penetration test findings

Solution

1. Continuous, crowdsourced penetration testing by a single provider
2. Flat fee, ongoing Synack365 penetration testing
3. Deployment of 500+ Synack-tested, background-checked security researchers

NOV knows people around the world depend on their thousands of customers.

Results

- More than 20,000 testing hours from the Synack Red Team (SRT)
- NOV quickly learned about exploitable vulnerabilities that warranted immediate remediation
- Synack researchers were able to find vulnerabilities (CVSS Avg. 7.6) with proof of exploitability for each report, in greater quantities than prior years
- Unusual for long-term testing, severity improved year-over-year, resulting in NOV outperforming Synack's oil and gas industry average
- Security and DevOps teams had real-time access to technical, detailed findings for replication, remediation and verification
- Penetration testers available for discussions and questions
- NOV & customers gain confidence that its infrastructure security is monitored and improved

> *“Security is critical to NOV because we power the industry that powers the world. Every connected company has security vulnerabilities, and as an industry leader and cybersecurity advocate, we share what works so that we're all safe and secure.”*
>
> JAMES COOPER – DIRECTOR, PRODUCT SECURITY AT NOV

Although NOV had regularly tested its infrastructure using multiple penetration testing firms, NOV had constant issues with their inconsistent, limited findings. NOV Security leadership team was ready to try more effective approaches to security testing using crowdsourcing and testing platform software.

After NOV's first test, it was clear that a Synack test could provide high-quality vulnerability reports in greater volumes than all prior solutions used by NOV for pen testing.

"Before Synack, we wondered if our security system was really effective or if previous testers had simply missed the vulnerabilities, due to limited sets of pentesters in those engagements" says Casey Lee, Director, IT Security.

> "*We now have greater confidence in our security because Synack showed us vulnerabilities that matter, found by their crowdsourced group of 500+ researchers, then told us what we needed to improve and how to fix it."*
>
> CASEY LEE – DIRECTOR, IT SECURITY

Skilled, vetted testers get results in first two weeks

Synack security researchers focused on NOV's websites, apps, cloud and host infrastructure. NOV's entire hosted infrastructure was selected for initial testing. Synack was confident its researchers would find a range of vulnerabilities, so they tested all NOV IPs to see how their security could be improved.

In the first two weeks, Synack's team found vulnerabilities where their predecessors had failed to find any. As NOV has remediated the vulnerabilities and strengthened best practices, fewer vulnerabilities are being found per target, which is exactly what better security looks like.

"Synack's results and the company's flat-fee pricing, which includes testing, remediation guidance and re-testing, confirmed Synack was the right choice for us," says Cooper, who notes NOV has continually upgraded its Synack services every year since 2018.

From the outset, NOV benefited from Synack's consistent standards and methodologies and its commitment to its talent pool. Synack vets, skills-tests, interviews, background checks, and confirms their experience before assigning researchers to customers like NOV.

Only Synack consistently removes inactive and underperforming security researchers to maintain its team's integrity and quality. To further inspire stellar results, Synack tracks researchers' performance metrics and incentivizes them with accolades and tangible rewards.

New and high severity findings

NOV used Synack's Discover and Campaigns offerings to confirm its security best practices were effective. High and critical vulnerabilities accounted for 44% of Synack's findings, an improvement on the 32% typically found in the National Vulnerability Database.

In its first year, the vulnerabilities Synack found had CVSS scores that equaled Synack's oil and gas industry average. In subsequent years, as Synack Red Team members became more familiar with NOV's assets, the CVSS scores exceeded the industry average. As a result, NOV receives the best results among Synack customers in the oil and gas industry.

NOV also used Synack Campaigns to confirm best practices were consistently in place on multiple assets. Typical Campaigns search for well-documented weaknesses via attempts at SQL injection or cross-site scripting. Many of those were checked via a NIST 800-53 Campaign, which also helps with compliance.

Proof of security gives customers peace-of-mind

Synack's reports help demonstrate NOV is an industry paragon for managing and controlling its security. Reports include recommended remediation and vulnerability details to help NOV develop an effective and responsive action plan. When remediation is complete, Synack's Patch Verification feature confirms NOV's work was effective and confirmed in real-time.

NOV's IT Security Team notes Synack's easy-to-read reports are customizable, searchable, concise and logically formatted. Prior reports were not as useful to NOV. Each test and report were based on different methodologies. As a result, different tests over time were so different that they couldn't easily show NOV's cybersecurity maturity. Synack's consistent and simple methodology and customizable reporting could clearly demonstrate improvement and more easily be used by developers for remediation. The customizable reports have also been used for compliance reporting purposes.

Embracing protective measures as security perspectives shift

NOV's IT Security team uses Synack's findings to show and educate business groups about vulnerabilities and risk. This has encouraged and accelerated the in-house adoption of NOV's newer authorization/authentication tools and protective measures.

"Thanks to Synack, our business groups know there are real risks of exploits, so they're behind our protective measures and we're resting better," says Cooper. "Synack makes the benefits of using DevSecOps best practices very clear."

Ron Roseman, NOV Product Security Engineer adds "At this point, a lot of people are being more proactive and asking where they can get these protections. Synack opened some eyes and changed attitudes with the business groups that were used to traditional testing methods."

Secure customer portal – accurate, real-time overview

The NOV IT Security Team has instant access to their data via the secure customer portal. It provides access to the testing results required for audits and training software developers. It also lets them see how resistant the various business units and assets are to attack.

The team can scope, kick-off, oversee, pause and restart all testing and researcher activities. The secure portal is also where NOV can pull reports, review assessment results, verify patches and monitor organizational Attacker Resistance Scores (ARS). They can track key metrics (e.g. hours, coverage of the testing scope) and results (e.g. vulnerability reports, suspected vulnerabilities, Campaigns' outcomes).

"The data is available when we need it — we don't need to call the account manager who then has to figure it out with the penetration tester," says Lee. "Synack's solution and reporting is superior to anything we've seen in the past."

Synack's portal provides an accurate, real-time overview into the true state of customers' digital security.

Make your first choice the right one

NOV leaders know anyone can be targeted at any time especially due to the surge of ransomware attacks and sophisticated espionage operations. Testing helps mitigate these risks.

Adds Cooper, "Just start with Synack — learn from NOV's experience with multiple providers and go with Synack as the sole provider because that's what ultimately worked and got NOV the results we needed."

> "*Continuous penetration testing is a key component to our Attack Surface Management program and Synack delivers!"*
>
> JOHN MCLEOD – CISO, NOV INC.