

Cybersecurity Technology Consulting Client.

Xepps is a web consulting business specialising in helping start-up companies grow with fractional senior leadership resources.

Managing Director Kristian Epps recently took a start-up company from almost zero internal processes through to successful completion of ISO 27001.

The process revealed large gaps in the startup's existing process and was a real challenge to implement.

Challenges



- **Lack of Existing process:** everything had to be set up and documented to demonstrate adherence to the standards.

- **High Cost:** Senior engineering time had to be carved out to ensure compliance with ISO 27001, and create the risk appetite, risk registers and appropriate technical standards and best practice documentation and apply it.

- **Threat Intelligence:** proving that you're really taking external threat intelligence and applying it to future risks is hard. A dedicated CISO may have lots more data sources, but for those without a dedicated function, it's difficult to implement. Not only do you need to be up-to-date with the latest threats, you then have to map the potential threats to your sector, and specific tech stack.
- **False Positives:** Although the pentest reports were comprehensive, they also delivered many potential vulnerabilities that needed investigation, which sucked time from the security leadership team. Many of these 'vulnerabilities' when investigated, proved to be false positives, erroneous or were not high impact.
- **Board Assurance:** Often the adoption of Cybersecurity standards is to help the Senior Leadership articulate a clear and independent view to report confidently on risk exposure, as it seeks additional investment and partnerships. Senior leadership buy-in is critical for success but hard to achieve.



Deployment and Approach

Rapid Setup: The system was live and delivering results very quickly, requiring minimal internal resources and training.



Comprehensive Coverage:

Verified Threat scanned across domains, IPs, cloud assets, & API's surfacing exposures not previously identified.



Actionable Reporting:

Delivered technical detail for engineers, but also clear executive summaries that were aligned to business impact.



Prioritisation:

Risks were ranked by exploitability and relevance, enabling the security team to focus on what mattered most.



Zero False Alerts

Every alert was verified with evidence. A full vulnerability exposure and log details are available to deep dive.



Always on Coverage

24/7 Red Team virtual monitoring at enterprise scale ensures continual assessment is active constantly.



Realtime AI Remediation

VerifiedThreat layers across existing defence setups, scales out autonomously and combines verified vulnerability testing with instant AI remediation.



Security Standards

Support for ISO 270001, SOC 2 & NIST Frameworks takes the pain out of manually recording incident and logging risk data, and automatically maps to each relevant control.



Attack Vector Chaining

Attackers can exploit weakly segmented domains to move laterally and escalate privileges. VerifiedThreat stops the attacks at the reconnaissance stage - before they can cause damage. This dramatically reduces the reconnaissance stage attacks by 70-90% and prevents more serious attack escalation in the future based on exploiting the weak defences.



Benefits

Typically customers see an immediate decrease in reconnaissance activity which leads to 30-40% decrease in unexpected server maintenance and overhead. Benefits can be measured by setting up custom tags for each major risk area, department or risk owner, and can be reported on an enterprise-wide basis to give complete 360° visibility.

Why Verified Threat?

The company selected VerifiedThreat because it gave the company a powerful way of providing on-going threat intelligence, continual external based assessments and reports, which could map directly into their existing risk ledger set-up.

The company had good success with a training portal that took the pain of ISO 27001 reporting and evidential proof needed to comply with the standard. Managing Director Kristian Epps said:

"Demonstrating that you have the latest threat intelligence, proving that you're not only reading, but applying the threat intel is not an easy task. We loved VerifiedThreat's dynamic intelligence, that wasn't some generic report, but actually demonstrated real threat intelligence on our platforms, with the verified proof of the vulnerability."

Epps continued:

"Signing into a portal with automated threat intelligence, more than ticked the box, it made the threat data demonstrable and useful. Sticking threat data into a CSV just means the data dies. It's now in the portal, it's live, it's useful, and it provides the third-party validation needed."

Results

- **Improved Threat Intelligence:** Automating the threat intelligence and applying it to the company's risk profile saved a lot of manual effort, and was a painless way to incorporate true risk threat data.
- **Improved Confidence:** External investors board and leadership team gained from improved confidence that the company wasn't just paying lip service to threat detection, but had mature systems and processes in place to ensure continuous monitoring and compliance..
- **Operational Efficiency:** Senior staff had to spend last time on manual work and compiling threat data and risk register items. Using the portal greatly simplified the process.

Impact

The major impacts are summarised below:

- **Technical:** Continuous visibility, faster identification of real-world vulnerabilities, and structured prioritisation for remediation.
- **Business:** Greater confidence for investors, board and senior leadership team. Ensured better protection of sensitive client data and confidence for eco-system partners.

"It's one thing to have knowledge of a possible threat, but it's a real game changer to be able to show what you are doing to track and mitigate the threat. VerifiedThreat made our reporting useful and directly actionable - it would have taken a lot of manual effort to keep the threat intelligence up-to-date and make it useful."

Kristian Epps, MD xepps Ltd.

Please reach out to our sales team and book in a demo to see the platform in action.

www.verifiedthreat.com

