CASE STUDY

How an IT team of one quickly took control of 400 vulnerabilities.

ASSURA™

Cybersecurity uncompromised.

CASE STUDY

Challenge:

Organizations are inundated with hundreds of thousands of vulnerabilities every year. After years of experience, we know most organizations can only patch about 1 in 10 (10%) vulnerabilities discovered in their environment based on resource capacity. This is simply insufficient to meet expectations. Traditional vulnerability management approaches that rely on CVSS scoring and static SLAs have proved ineffective, leading to undue pressure on IT teams. One such organization in the healthcare industry with an IT team of one sought help from Assura.

Solution:

Vulnerability Management-as-a-Service

Assura initially conducted a penetration test to evaluate the client's environment and concluded that vulnerability management was a significant challenge. The solution we recommended was implementing our Vulnerability-Management-as-a-Service (VMaaS), which offloads the burden of triaging vulnerability risk to Assura, freeing up the organization to focus on the most critical vulnerabilities that pose a genuine risk if exploited. We know from exploit and threat intelligence big data science that only about 5% of vulnerabilities are exploited, meaning that if the average organization can patch 10% of their discovered vulnerabilities, they can do a lot to reduce their overall risk as long as they're focused on the right ones.

With VMaaS up and running, Assura initially discovered that although the organization only has a handful of servers, there were about 400 vulnerabilities ranging from a few days old to years old. By assessing each asset's contextual risk to the client's mission and business and adding threat intelligence, Assura identified vulnerabilities that needed addressing and those that could be accepted based on the client's risk tolerance. Additionally, Assura identified gaps in configuration management and the patch management program.

Results:

After just two months of using Assura's VMaaS the client's vulnerability backlog had been reduced from over 400 to just 10 per month on average. This means that the client now only has to address one vulnerability based on its contextual risk realistically, a significant improvement for a team of one that initially faced the daunting task of addressing an insurmountable number of vulnerabilities.

Big picture:

We understand vulnerability management, risk, and organizations' resource limitations. Technical/security debt is real, and we can help you wrangle that in with our risk-based approach to vulnerability management. It is no longer an all-or-nothing approach but instead a sensible and practical approach that will allow you to manage your vulnerabilities, not the other way around. With Assura's risk-based approach, your organization will realize its true capabilities to manage vulnerability risk and be alerted to those top vulnerability-borne risks as they develop.

Get in touch.
Email info@Assurainc.com or call 855-9NOHACK.

Assura's Popular Services:

Fractional CISO, Risk Assessment, Penetration Testing, Security Monitoring and Response, AuditArmor™ Audit Defense, Extended Detection and Response, Multifactor Authentication, Security Awareness and Training, Continuity Planning, GRC, Disaster Recovery, DFIR

Assura provides innovative cybersecurity advisory and managed services to clients in every industry including government, healthcare, banking, manufacturing, and transportation sectors. Our unique capabilities include tying together risk-based cybersecurity with sustainable compliance and developing inventive technical solutions for our clients. **Learn more at www.Assurainc.com.**