ActZero

Case Study

ActZero helps southeast U.S. medical center focus its cybersecurity efforts

ORGANIZATION OVERVIEW

Our client is a mid-sized medical center based in the U.S. southeast. The organization employs approximately 3500 full- and part-time staff, operating more than 8500 endpoints

THE BUSINESS CHALLENGES

- Increasing cyber attacks on healthcare sector
- Current tooling and MSSP failing penetration tests
- Poor visibility into cybersecurity posture
- Inefficient vendor response
- Limited IT staff

THE BUSINESS RESULTS

- Immediate trust in ActZero's detection and response capability
- Eliminated alert fatigue across their small IT team
- Increased visibility and clarity into risks and gap closure priorities

Adding a new security solution into an existing set of tools isn't always desirable or easy, but in some cases, it's exactly what the doctor asked for. In the case of a southeast U.S.-based medical center, they leveraged ActZero to replace older technologies, and holistically address their foundational security - building a cybersecurity solution that scales with their organization.

Understanding the Business Requirements

In late 2021, the medical center client approached ActZero looking to improve its cybersecurity posture. While they are a large organization, budget demands for medical practitioners, staff, and medical equipment took priority over IT security spend. As a result, the IT team had only 2 direct security members, and minimal budget. To protects its critical infrastructure, the organization often turned to free or self-managed security tools, as well as deploying a managed-SIEM solution provided by an Managed Security Services Provider (MSSP). Unfortunately, the MSSP didn't deliver, leaving the client unprotected; the vendor failed penetration tests, overwhelmed the client with needless unfiltered alerts, provided dismal threat response and remediation, and offered no visibility into vulnerabilities or areas for improvement.

Through the discussion, the clients demonstrated requirement for:

- **Better service experience**, 24/7 support, responsive, informative
- **Disparate & insufficient tool avoidance**, that can find efficiencies in tooling, provide a better TCO, and unify alerts and reporting
- **Elimination of alert fatigue**, resulting from a significant reduction of needless or false alerts
- **Deeper visibility into their environment and potential breaches**, with insight into logs, security hygiene, and vulnerabilities
- **Meaningful maturity metrics & reporting**: Clear dashboards and reporting showing what's improved, and client service metrics

ActZero

CASE STUDY

THE SOLUTION

- **Comprehensive coverage** for endpoints, network and cloud
- **24/7 customer support**
- **Better Accuracy in Detections:** Reduced false positives and needless alerts
- **Strong Visibility & Guidance**
  - **Technical Account Managers** to oversee monthly progress
  - **ActZero Customer Portal** 24/7 visibility into security hygiene and vulnerabilities
  - **Security maturity model** Assess cybersecurity readiness, prioritize and plan
  - **ActZero vCISO services** Policy, compliance and security maturity guidance

THE NUMBERS

10-day
onboarding

~ 95% reduction
in false positive alerts

$75K+ Net savings
annual through removal of MSSP managed-SIEM

ActZero is purpose-built to detect, identify, block, contain, and respond to threats across organizations, and provide the guidance needed to close risk gaps.

Immediate vulnerability detection and mitigation

Within the client onboarding process, initial scans discovered nearly 7500 assets with vulnerabilities. ActZero walked the client through the customer portal and hygiene information, focusing on prioritizing missing patches, SSL/TLS issues, enforcing MFA, and improving "Admin" rights management. We also recommended that they continue to upgrade Windows 7 machines, as well as look into updating iDRACs and iLOs as an easy way to reduce the number of critical vulnerabilities.

Alert volume vs. meaningful alerts

During the cutover period, the client noted their departing vendor suddenly started to send them more notifications seeking to prove that ActZero may not be monitoring the same activities that they are. ActZero provided evidence that, in fact, our detections were greater, and that our machine learning and threat hunters are demonstrably better at weeding out the false positives - a point not lost on the client who'd suffered from meaningless alerts.

Deeper visibility and strategic improved advice

The number one concern that client had with their previous company was a lack of communication and visibility into what was going on in their networks. ActZero eliminated this critical roadblock to success. From ongoing direction provided by our Technical Account Managers, to our Customer Portal and our vCISO service, ActZero provided the timely guidance needed to stay ahead of threats.

In the client's words...

"In three months, we got more actionable alerts from ActZero than from our previous service provider over three years. Now, we're not flooded with bad alerts. When we get an alert, we know we need to look at it. The monthly report is phenomenal, the CIO is very pleased with the service. We're way more secure now than we were when we started."

-VP of IT, large regional hospital, US Southeast

CONTACT US

Learn how our MDR solution can bring protection and clarity to your cybersecurity journey

Email: info@actzero.ai
Phone: +1.855.917.4981