MIXMODE'S AI NETWORK SECURITY MONITORING PLATFORM HELPS HIGHCASTLE MONITOR AND REACT TO THREATS WITH 10X GREATER EFFICIENCY

"MixMode's AI significantly reduces false positive alerts, creating an opportunity for us to be ten times more efficient with our resources in monitoring and reacting to actual threats."

Meghan Gorman
Founder & CEO

HIGHCASTLE CYBERSECURITY
Your Risk. Secured.

Challenge: Increasing ROI while maintaining a high level of customer service

HighCastle's team was challenged to correctly price its cybersecurity offering, usually without a great deal of knowledge of the client environment prior to solution pricing. "It is tough to price a comprehensive cybersecurity offering before you've seen what you're dealing with in a client's environment. It is resource-intensive to review data logs. We need to understand the client's vulnerabilities quickly and accurately in order to save time in the evaluation phase and make the value of our proposed solution immediately clear to the client," says Meghan Gorman, Founder & CEO, HighCastle.

While HighCastle's clients often share logs from their security information and event management (SIEM) systems, it can be a lengthy process to identify and assess threats from this information. According to McAfee, the average enterprise generates 2.7 billion actions in cloud services per month, of which 2,500 are anomalous and only 23 are actual threats, a ratio of nearly 110:1.[1] In order to distinguish the signal from the noise, while simultaneously maintaining client diligence, HighCastle needed a way to quickly identify actionable information.

According to the Ponemon Institute,[2] organizations with over 500 employees waste an average of 395-man-hours a week "chasing erroneous alerts." To maximize efficiency, HighCastle needed a solution that would provide insights so its client managers and Security Operations Center (SOC) analysts could better understand clients' cyber risks, minimize time spent chasing false positives and ensure the team was spending the bulk of its time responding to actionable information.

Companies average 17K malware alerts weekly and only investigate 4%. [3]

"MixMode's AI significantly reduces false positive alerts, creating an opportunity for us to be ten times more efficient with our resources in monitoring and reacting to actual threats. We have received thousands of alerts per month using other IDS solutions, and those numbers are significantly reduced now."

"To be specific, with MixMode, we have seen 90-95% alert reduction consistently for a financial services client. In addition, the alert precision is excellent as we have seen fewer false negatives versus other solutions," says Gorman.

Using MixMode, HighCastle has:

- **Reduced false positive alerts 90-95%**
- **10x greater efficiency with resources in monitoring and reacting to actual threats**
- **Implemented MixMode with 80% of prospects**

About HighCastle

Industry: Cybersecurity
Headquarters: New York City
Specialty: Helping companies with security compliance
www.highcastlecyberrecon.com

HighCastle provides a range of professional and managed services to help smaller, resource-constrained companies assess and mitigate cybersecurity risk and exposure. Focused on compliance, HighCastle helps clients and their business partners meet N.Y. Department of Financial Services, HIPAA, NIST, SOC and PCI CSF regulations among others.

Closing More Business: Assessing and Addressing Specific Client Needs with MixMode

With insights uncovered by MixMode, HighCastle can quickly assess the prospect's situation and propose a solution that addresses their specific needs. Many prospects have a choice between:

- Point-in-time penetration tests
- Point-in-time vulnerability assessments
- Continuous monitoring and remediation

While HighCastle will conduct penetration tests if a client needs them for regulatory reasons, Gorman firmly believes in continuous monitoring because client environments and the threat landscape are always evolving.

"We use MixMode with 80% of prospects. It absolutely helps us close business because MixMode makes the value of continuous monitoring extremely clear," says Gorman. "Point-in-time tests are not robust enough because the risk landscape is dynamic. You cannot do an assessment once a year and call it good, because as soon as it's done, it's outdated."

After performing an initial risk assessment using MixMode, HighCastle creates a security roadmap to help clients achieve compliance. Once the roadmap is agreed upon, the company puts controls in place--and monitors those controls on a daily basis with MixMode to assure clients that their infrastructure is secure. "We use MixMode as our continuous monitoring tool--something that keeps a pulse on what's happening across the client infrastructure," Gorman says.

Gorman is committed to complementing their SIEM with MixMode because a SIEM's log analysis is resource-intensive and vulnerable to intrusion--a good intruder can alter logs and cover their tracks. She says, "I really like having MixMode as a second layer of assurance that we are not being fooled by modified logs. With MixMode we are much faster at getting a clear picture of what's an event, what's an incident, and the seriousness of each of those versus relying on log analysis alone to figure it out."

Summary

"It's eliminated the majority of work we did chasing false positives. We're not spending hours and days trying to understand the client's vulnerabilities and determine the best course of action. MixMode gives us the continuous monitoring we need to protect our clients and to help them demonstrate compliance with some of the government's most stringent regulations."
- Meghan Gorman, Founder & CEO

[1] McAfee. "Definitive Guide to Cloud Threat Protection". https://www.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/wp-definitive-guide-to-cloud-threat-protection-ebook.pdf
[2] Ponemon Institute. "The Cost of Malware Containment". https://www.ponemon.org/local/upload/file/Damballa Malware Containment FINAL 3.pdf
[3] Ponemon Institute. "The Cost of Malware Containment". https://www.ponemon.org/local/upload/file/Damballa Malware Containment FINAL 3.pdf

About MixMode

MixMode is a revolutionary AI focused Cybersecurity Company using patented third-wave AI originally developed for projects at DARPA and the DoD. MixMode's Network Security Monitoring Platform provides deep network visibility and predictive threat detection capabilities, enabling your security team to efficiently perform real-time and retrospective threat detection and visualization. Used by breach response teams worldwide, security analysts and SOC teams can integrate MixMode into their playbooks, SIEMs, or utilize MixMode on a standalone basis to dramatically reduce investigation time, cost and expertise required to respond to persistent threats, malware, insider attacks and nation state espionage efforts. Based in Santa Barbara with an additional office in San Diego, the company is backed by investors including Keshif Ventures and Blu Venture Investors.