Achieving Effective Vulnerability Management at Scale – and a Whole Lot More

Moffatt & Nichol uses CRITICAL**START**® MDR and VMS to reduce their vulnerability exposure, improve threat response times, and increase operational efficiency through actionable insights and expert support.

CASE STUDY

AT A GLANCE

⚙️ Industry: Global Infrastructure Consulting

📦 Founded: 1945

📍 Headquarters: Long Beach, CA

👥 Size: Mid-level Enterprise

🗂️ Company Structure: Private Equity Corporation

CORE AGENDAS

Challenge
Faced with rapid growth and an unsustainable vulnerability management process, Moffatt & Nichol needed a scalable solution to strengthen their security posture and operational efficiency.

Solution
Critical Start's MDR and VMS provided comprehensive security monitoring, streamlined vulnerability management, and prescriptive patch recommendations.

Results
Moffatt & Nichol significantly reduced their vulnerability exposure, improved threat response times, and increased operational efficiency through actionable insights and expert support from Critical Start.

Company Profile

Moffatt & Nichol is a global infrastructure consulting company that specializes in facilities planning and design. Based in Long Beach, California, this mid-sized private enterprise provides engineering and consulting services to clients in the marine terminal, transportation, energy, environmental, federal, and urban development markets around the world.

Problem Statements and Challenges

Moffatt & Nichol faced significant challenges with their security operations before partnering with Critical Start. As with any organization that works within public infrastructure, cyber security and regulatory compliance are always top of mind. However, as they grew, they knew that their incumbent service provider's solution was not sustainable – particularly around vulnerability management – even though it met compliance requirements.

"We went from just under 500 people to nearly 1400 relatively quickly," said Moffatt & Nichol Chief Information Officer (**CIO**) Jason Jewett. "We gained staff who could bolster our security beyond compliance mandates with the right service around the cybersecurity tools we had in place, but our previous provider wasn't delivering the data or level of service we needed to be fully effective."

Though Moffatt & Nichol had top-tier security tools, their Managed Security Service Provider (**MSSP**) generated spreadsheets itemizing individual vulnerabilities which were manually analyzed. Additionally, their previous provider's SIEM was not user-friendly, and customer support was difficult to reach, even during potential security incident investigations.

> **"We have a full IT staff, so we didn't need a fully hands-on services like MSSPs offer. Critical Start had all the features we were looking for.** The promise of a high level of customer service and transparent communications also made Critical Start a compelling choice.**

> **- Ean Meacham,**
> **IT Security Analyst**

The Critical Start Solution

First and foremost, Moffatt & Nichol sought a vendor that could accelerate and simplify vulnerability scanning and prioritization. Additionally, they wanted to partner with a firm that could supplement their existing team without completely taking over security monitoring and management. Moffatt & Nichol wanted to have granular control over how their service was configured, implemented, and executed. They also needed to know that their provider's Security Operations Center (**SOC**) would respond quickly, especially during alert investigations.

After evaluating a few vulnerability management vendors, Managed Detection and Response (**MDR**) services, and MSSPs, Moffatt & Nichol decided to partner with Critical Start. Ean Meacham, IT Analyst for Moffatt & Nichol said, "We have a full IT staff, so we didn't need a hands-on services like MSSPs offer. Critical Start had all the features we were looking for. The promise of a high level of customer service and transparent communications also made Critical Start a compelling choice."

Moffatt & Nichol implemented Critical Start Vulnerability Management Service (**VMS**) with Qualys VMDR, MDR services, with SentinelOne EDR, and XDR with Sumo Logic as their SIEM. Additionally, they integrated the Critical Start Cyber Operations Risk & Response™ (**CORR**) platform with Intune for comprehensive asset visibility, creating a one-stop shop for their security needs.

"We were excited to partner with a firm that allowed us to continue using the tools we already have in place. We did not want to have to rip-and-replace, and we also wanted to use best-in-class solutions," said Jewett.

The integration of Qualys VMDR, a key component in Critical Start's VMS, was the only new component in the Moffatt & Nichol security stack. However, the VMS team at Critical Start provided extensive support, ensuring that Moffatt & Nichol could fully utilize the prescriptive patch lists and prioritized vulnerability reports provided through CORR.

> **Critical Start has helped us streamline our security operations by reducing the need for manual analysis. It gives us what we need to make real progress in risk reduction across our environment.**
>
> **- Ean Meacham,
>   IT Security Analyst**

Critical Start Checked all the Boxes:

- Direct integration with incumbent security tools, including SentinelOne, Sumo Logic, and Microsoft Intune
- Simplified vulnerability management with turnkey patch lists
- Easy-to-use dashboard for tracking vulnerability management and alert escalations
- Staff augmentation
- Custom configuration of playbooks, response actions, and Response Authorizations
- Rapid response, with contractual SLAs
- Transparent operations and open communications

The Critical Start Solution

- Vulnerability Management for Qualys VMDR
- MDR with SentinelOne EDR
- Managed XDR with Sumo Logic SIEM
- Intune integration for Asset Visibility

Results

"Onboarding was quick," said Meacham, "which is awesome, because we were on a timetable to get everything switched over." Ninety percent of the onboarding process was completed in one month. During that time, Moffatt & Nichol reassessed much of their environment and realized where they had risks of potential exposure. They also found some misconfigurations, which helped the onboarding team tune detection rules and sensors to reduce alert noise.

From the start of operations with Critical Start, Moffatt & Nichol has experienced significant improvements in their security posture, especially around vulnerability management. Instead of receiving unmanageable spreadsheets, they now rely on a clean, concise dashboard with clear prioritization and prescriptive patch lists that help them make an immediate impact. "We were barely keeping our heads above water when it came to vulnerability management," Meacham said. "Critical Start has helped us streamline our security operations by reducing the need for manual analysis. It gives us what we need to make real progress in risk reduction across our environment."

Within the first three months, Critical Start:

Helped identify assets that were vulnerable to ransomware attacks, and those that had endpoint security coverage gaps.

Provided prescriptive patch recommendations that allowed Moffat & Nichol to patch over 78% of open vulnerabilities.

Saved Moffatt & Nichols valuable time and work effort by suggesting just 5 patches that could be used to remediate over 6,700 vulnerabilities.

"

After an alert comes in, we can quickly review it within the CORR platform, see what was written, and give our approval to create a block, add to the exclusion list, or whatever – and it just gets done. It's not two weeks down the road. It's within a few hours.

- Ean Meacham,
  IT Security Analyst

"

The Moffatt & Nichol team have also been impressed with the level of communication and competency they have experienced since choosing Critical Start. "Our weekly cadence calls provide significant value, as well," Jewett said. "We often skipped those calls with our previous provider. Now, my team looks forward to those check-ins, because they're actionable. We use the recommendations provided to continually improve our security posture."

Additionally, the team has noted a marked improvement in MDR support over their previous firm. Meacham said, "After an alert comes in, we can quickly review it within the CORR platform, see what was written, and give our approval to create a block, add to the exclusion list, or whatever – and it just gets done. It's not two weeks down the road. It's within a few hours."

With customizable playbooks and rules, contractual response SLAs, and transparent communications, Moffatt & Nichol has come to trust the alerts coming from the Critical Start team. They also use the MOBILE**SOC®** app to further accelerate response, remediation, and communication during alert escalations.

Moffatt & Nichol appreciate how the Critical Start SOC feels like an extension of their organization, providing experienced care, complete transparency, and human ingenuity that has helped them improve their security posture and has given them the time back they need to achieve their organization's goals. "The comprehensive support from the Critical Start team has enabled us to leverage the full potential of our security solutions, leading to enhanced security and operational efficiency," said Meacham.

> **The comprehensive support from the VMS team has enabled Moffatt & Nichol to leverage the full potential of the solutions, leading to enhanced security and operational efficiency.**
>
> - Ean Meacham,
>   IT Security Analyst

CRITICALSTART ®

For more information, contact us at:
https://www.criticalstart.com/contact/