CASE STUDY

AFG TURNS THE TABLES ON THE HACKERS WITH **LMNTRIX**

INDUSTRY: FINANCIAL SERVICES

As a mid-tier financial services firm, Alliance Funding Group (AFG) knew falling victim to a cyber breach was not a matter of 'if', but 'when'. Matt Kraus, IT Manager at AFG, said after reading the steady stream of headlines describing successful attacks against the Finance sector's juggernauts, he knew he had to call on external experts to bolster the firm's security posture.

"I'd see the larger firms with multi-million-dollar preventative mechanisms like internal SOC teams, SIEM implementations and external MSSPs still getting breached," Kraus said. "If they failed against attackers, we wouldn't stand a chance."

Founded in 1998, AFG finances small and medium sized businesses across the US. To date, it has originated more than $1.5 billion in equipment leases and unsecured business loans to support American firms secure inventory and equipment, increase cash flow, or pursue expansion. Given the sensitive nature of financial data, Kraus said his main concern in bolstering AFG's security capability was to protect the Personally Identifiable Information (PII) of the firm's customers.

"We'd done a good job of setting up our perimeter defenses – firewalls, intrusion prevention systems, email security, web security and WAF – but these were all signature-based defenses, we needed more sophistication. We needed visibility into our network to catch anything that had bypassed our controls and a way to detect signature-less attacks."

Running a lean IT team, already 100 per cent utilized, Kraus began searching for a solution that would provide AFG not only the products and services needed to thwart all manner of attackers, but also the human expertise needed to properly use the technology.

PROBLEM:

- AFG's small IT team, already at full capacity, was looking to improve its security posture
- Limited internal cyber security capability and limited budget complicated efforts
- Cyber skills shortage made finding and affording experienced analysts difficult

CASE STUDY

PROBLEM

Kraus' IT team already had their hands full. With a small team dealing with everything from enterprise app-level assets down to configuring desktop images for new users, the team's focus was on enabling client interactions and supporting the sales team. Although security was always a priority, there was a lack of capacity and expertise to extend AFG's security framework with current internal resources.

"We're not in the business of security," Kraus said. "We investigated point solutions and SIEM implementations, but they were not only cost-prohibitive, we'd then need to find the right talent to make sense of it all. These are skills that are in high-demand and low supply."

After briefly considering a SIEM implementation, Kraus was initially drawn to LMNTRIX as the platform was a 100 per cent cloud service and promised zero false positives – something that haunted other solutions tested.

A cloud solution would enable Kraus and his team to focus on AFG's day-to-day business needs, while allowing the security experts to handle cyber defense.

"If we'd gone the SIEM route, we'd still need to make sense of the logs – which threats are real, which are false positives, and then we'd need to develop a response to those threats. We didn't have the capability, or the budget, to develop that capacity."

Kraus said he was initially skeptical of LMNTRIX's claims and thought the platform's depth of capability was too good to be true.

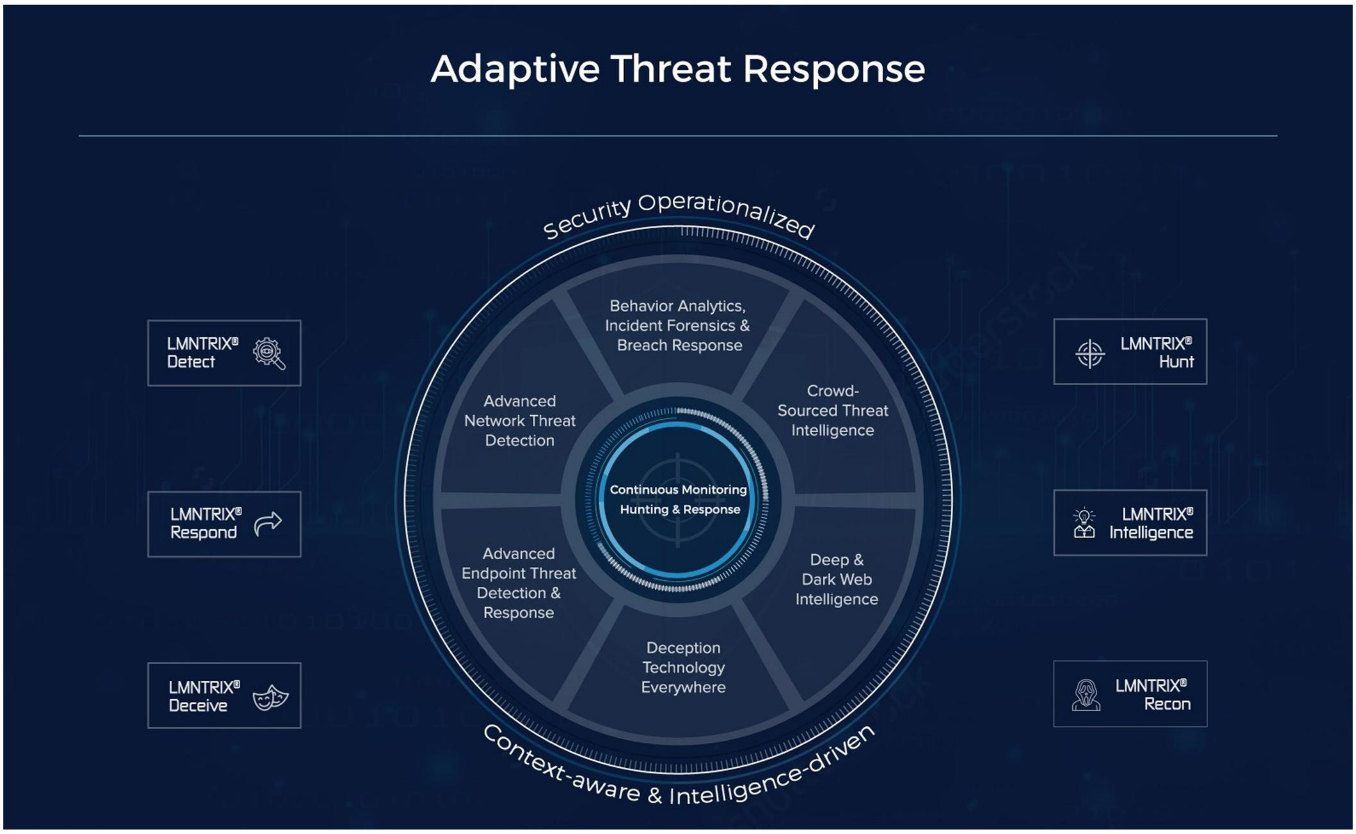
"The Proof-of-Concept quickly put any doubts to rest – we saw LMNTRIX's Adaptive Threat Response (ATR) approach bait, trap and hunt down attackers already hidden in our networks. All our previous solutions missed these threats entirely."

SOLUTION:

- LMNTRIX Adaptive Threat Response platform

CASE STUDY

SOLUTION



Adaptive Threat Response

Security Operationalized
Behavior Analytics, Incident Forensics & Breach Response
Crowd-Sourced Threat Intelligence
Deep & Dark Web Intelligence
Deception Technology Everywhere
Advanced Endpoint Threat Detection & Response
Advanced Network Threat Detection
Continuous Monitoring Hunting & Response
Context-aware & Intelligence-driven
LMNTRIX® Detect
LMNTRIX® Respond
LMNTRIX® Deceive
LMNTRIX® Hunt
LMNTRIX® Intelligence
LMNTRIX® Recon

After testing LMNTRIX's full ATR platform against traditional MSSPs, Kraus decided to implement a next-generation security solution built on key elements of the ATR platform.

"I couldn't believe the level of detail during testing. In real-time, LMNTRIX analysts were baiting attackers and actively pursuing them through our environment – it was like something out of a movie."

Ultimately, Kraus said the comprehensiveness of the LMNTRIX platform made the decision a no-brainer.

"They didn't just do one thing, they covered all the bases – endpoint protection, network monitoring, reconnaissance, adversary deception, and proactive threat hunting.

To build this ourselves, we'd need 50 different products and then we'd need to find the security analysts capable of managing it all.

The multi-dimensional and holistic approach that LMNTRIX takes is a real game changer in my opinion"

CASE STUDY

BENEFIT

Krauss said LMNTRIX's value was clear as soon as the sensors were installed during the initial Proof of Value.

"LMNTRIX gave us eyes we didn't have before. Almost straight away, they discovered multiple issues that had gone completely undetected by our previous security infrastructure. "It wasn't just external threats – LMNTRIX discovered internal gaps in how some of our users were using various applications and services. We simply didn't have the visibility beforehand to uncover these things. What became obvious for me and our management was that until that point we simply had a false sense of security."

For Krauss and his team, the most valuable part of the LMNTRIX platform is the knowledge that experienced security analysts are now monitoring AFG's environment.

"When a breach is validated, the instruction LMNTRIX provides from a remediation standpoint is something we desperately needed. We didn't have the capability to do the required research, or the security talent to reverse engineer malware and understand the different threat-level components.

Critically for us, the intelligence we receive is cross-correlated across all our various platforms – there's no way we could have achieved this in house.

"We realized that before LMNTRIX, we had placed too much dependence on the promises of point-product vendors and protective controls that were letting us down."

Beyond bolstering AFG's current defensive posture, Kraus said LMNTRIX also enables the firm to prepare for the future.

"It's inevitable that there'll be more regulations surrounding cyber security. In Europe, we're witnessing the rollout of GDPR and, while the US isn't at that stage yet, it's safe to assume a similar scheme isn't too far off."

"When we undertook this project, we took our time and thought strategically so when the regulations do come, we're already prepared and well on that path rather than playing catch up."

BENEFIT:

- Multiple issues – previously undetected – were immediately discovered and mitigated
- Experienced LMNTRIX threat analysts now monitor AFG's environment 24/7
- AFG has future-proofed its IT security, in line with more stringent international regulations
- False Positives: Reduced by 95%
- Threat Detection Time: Reduced from Months to Minutes
- Incident Response Time: Reduced from Days to Minutes
- Breaches Validated: In less than 2hrs
- PC Wipe & Reimaging: Reduced by 98%

LMNTRIX US.
333 City Blvd West, Suite 1805,
Orange, CA 92868 USA
+1.888.958.4555

LMNTRIX UK.
Kemp House, 152 - 160 City Road,
London, EC1V 2 NX
+44.808.164.9442

LMNTRIX SINGAPORE.
60 KAKI BUKIT PLACE#05-19
EUNOS TECHPARK
+65.3159.0639

LMNTRIX Hong Kong.
Room 1102, 11/F, Kenbo Commercial Building,
335-339 Queen's Road West, Sai Ying Pun,
Hong Kong
+852.580.885.33

LMNTRIX Australia.
Level 5, 155 Clarence St
Sydney, NSW,
+61.288.805.198

LMNTRIX India.
#811,10th A Main Road, Suite 110,
Indira Nagar, 1st Stage,
Bangalore, Karnataka,India, 560038