banyax

PHARMACEUTICAL MANUFACTURING · EMPLOYEE-TARGETED PHISHING · MANAGED EXTERNAL THREAT INTELLIGENCE (M/ETI) + MANAGED EXTENDED DETECTION & RESPONSE (M/XDR) + MANAGED AWARENESS TRAINING (M/AT)

Stopped Before It Started:

Detecting Phishing Infrastructure Before the Campaign Launched

How Banyax's integrated M/ETI (Managed External Threat Intelligence) + M/XDR (Managed Extended Detection & Response)+ M/AT(Managed Awareness Training)service detected an active phishing infrastructure in preparation — stopping a credential theft campaign before any employee received a single message.

INDUSTRY Pharmaceutical Manufacturing · Mexico

01 · RESULTS AT A GLANCE

The value in this case is not what Banyax responded to — it is what Banyax prevented. Detection happened at the infrastructure preparation stage, before any campaign was launched against employees.

Threat Stage	Prior Visibility	Incident Cost	Services Activated
Pre-launch	**Zero**	**Avoided**	**3 of 3**
detected during infrastructure preparation, not execution	*client had no knowledge the domain existed*	*credential theft and initial access prevented before impact*	*M/ETI + M/XDR + M/AT coordinated around a single risk*

Before Banyax, the organization had limited visibility into external infrastructure being prepared for targeted attacks. Existing controls could detect threats once a campaign was already in motion and producing internal indicators — but not while an attacker was quietly building the tooling to launch one.

After this engagement, the security team had early warning of a threat they would never have discovered through internal monitoring alone. They acted before any employee saw a phishing message. The question changed from 'how do we respond to a credential compromise?' to 'how do we prevent one from happening?'

02 · THE BUSINESS PROBLEM

The pharmaceutical manufacturer's security team was well-equipped to detect threats once they reached internal systems. What they lacked was visibility into the stage that precedes an attack — when an adversary is preparing infrastructure, registering domains, and building the deception before launching it.

Controls that only detect, never anticipate

Traditional security controls are designed to identify threats that are already executing. When a phishing domain is registered but hasn't sent a single email, no alert fires. The organization was protected from known, active campaigns — not from the preparation phase that precedes them.

Employee-targeted deception at corporate scale

A well-constructed phishing campaign targeting a large employee base doesn't need to fool everyone; it only needs to fool a few. The attacker's goal was to replicate a trusted internal portal convincingly enough to harvest credentials from employees who would have no reason to question its legitimacy.

No visibility outside the perimeter

The threat was being built outside the organization's monitoring perimeter. Internal Security Information and Event Management (SIEM), endpoint, and network tools had nothing to detect because the malicious infrastructure hadn't interacted with the organization yet. External threat intelligence was the only layer that could have seen it.

What made it urgent

There was a clear trigger: Banyax identified a domain simulating an internal corporate information-sharing portal. No campaign was actively running at that moment — but the infrastructure existed, it was operational, and it was ready to be weaponized. That alone elevated the urgency from theoretical to immediate.

03 · THREE SERVICES, ONE RISK — THE INTEGRATED DEFENSE

This case is notable because it demonstrates how Managed External Threat Intelligence (M/ETI), Managed Extended Detection & Response (M/XDR), and Managed Awareness Training (M/AT) operate as an integrated defense — not as separate products sold to the same client, but as coordinated layers activated by a single threat signal, all orchestrated through Banyax Quest, our proprietary platform.

The detection the client didn't know to look for

Banyax identified a domain and interface that the client's internal team had not detected — and did so before any phishing campaign was activated at scale. The domain was impersonating a corporate environment: the kind of site employees interact with daily and have no reason to distrust. The AI-led correlation engine evaluated domain similarity, interface elements, brand references, and content signals together — what looked like a low-confidence coincidence in isolation resolved into a credible threat in preparation when viewed as a pattern. Analysts confirmed the context and escalated for action.

M/ETI (Managed External Threat Intelligence) — Detect

External threat intelligence continuously monitors for infrastructure being prepared to impersonate the organization's internal environment. It operates outside the perimeter — the only layer that can see a threat before it interacts with internal systems.

In this case: *Identified the fraudulent domain during the preparation phase, before any employee received a phishing communication.*

M/XDR (Managed Extended Detection & Response) — Prepare

Once the external threat was identified, Managed Extended Detection & Response (M/XDR) used the intelligence to reinforce internal detection coverage: updated detection rules, prepared response playbooks, and ensured that if the campaign launched, the Security Operations Center (SOC) would identify it immediately.

In this case: *The organization entered a state of readiness — not just awareness. Internal monitoring was aligned to the specific threat profile identified externally.*

M/AT (Managed Awareness Training)— Prevent

Managed Awareness Training (M/AT) was activated as a direct response to the phishing infrastructure finding. Employees were briefed on the specific social engineering pattern identified — not a generic security reminder, but targeted communication built around the actual threat.

In this case: *The human layer was reinforced at the exact moment it was most needed, using the specific context that made the deception credible.*

04 · HOW THE SERVICE OPERATES

From external signal to coordinated prevention in five steps — all three services working in parallel through Banyax Quest.

1	2	3	4	5
M/ETI (Managed External Threat Intelligence) DETECTS	**AI CORRELATES**	**M/XDR (Managed Extended Detection & Response) PREPARES**	**M/AT (Managed Awareness Training) ACTIVATES**	**GOVERNED**
External infrastructure monitoring triggers alert	*Domain signals scored and confirmed by analysts*	*Detection rules + playbooks updated for specific threat*	*Targeted employee awareness communication*	*Continuous monitoring maintains pre-launch visibility*

05 · WHY BANYAX — THE STRUCTURAL MOAT

Four differentiators that create prevention dependency, not contract dependency.

■ The only layer that sees pre-launch infrastructure.

Internal tools — SIEM, endpoint, network — have nothing to detect until a threat interacts with the organization. M/ETI operates outside the perimeter, continuously monitoring for preparation activity. No internal tool can replicate this visibility. This is not a feature comparison — it is a capability gap.

■ AI-led at scale, human-validated at every escalation.

Thousands of external signals are processed continuously. The AI-led correlation engine filters false positives and scores risk. Human analysts from Banyax validate every escalation before it reaches the client. The security team receives confirmed threats — not noise.

■ Integrated stack — value multiplies when services work together.

M/ETI + M/XDR + M/AT were already active when this incident occurred. What it demonstrated is that their combined value is greater than the sum of the parts: the external finding became internal readiness and human prevention in a single coordinated response.

■ Pharmaceutical-context detection — regulated environment expertise.

In a pharmaceutical manufacturing environment, internal access integrity is a compliance requirement. The stakes of a credential compromise go beyond operational disruption. Banyax's detection is calibrated to that risk profile — and the evidence packages are formatted for regulatory documentation.

06 · OUTCOMES — BEFORE AND AFTER

Before

Limited visibility into external threats in preparation. Controls activated only once campaigns were in motion and generating internal indicators. The team was reactive by design — there was no mechanism to detect what hadn't yet reached the organization.

Avoided cost

If the domain had been activated and reached employees, the potential impact included: credential theft across a large employee base, unauthorized initial access into internal systems, and operational disruption in a regulated manufacturing environment where the integrity of internal access is a compliance requirement.

After

Phishing infrastructure detected before campaign launch. Internal detection coverage reinforced. Employees briefed with targeted awareness communication. Security team shifted from reactive investigation to coordinated prevention.

Team efficiency

The internal security team stopped discovering threats late and responding under pressure. With the Banyax finding and evidence package, they coordinated preventive measures with full context — reducing reactive investigation time and improving the quality of the response.

INVESTOR SIGNALS

Retention Active — three services maintained

Integration M/ETI + M/XDR + M/AT proven as a combined stack

Value type Pre-incident prevention — highest ROI category

NPS signal Client acknowledged proactive detection value

Moat No internal tool can see pre-launch infrastructure

"The value was in avoiding the incident, not in responding to it. Banyax showed us a threat that was being prepared before we had any reason to know it existed."

— Information Security Lead, Major Mexican Pharmaceutical Manufacturer

Discontinuing Banyax means returning to the posture where the next phishing infrastructure would be discovered only after employees had already been targeted. That is not a risk the security team is willing to accept.

07 · IDEAL CLIENT PROFILE

Pharmaceutical manufacturers, regulated industrial companies, and organizations with large employee bases and corporate portals used as daily internal touchpoints — particularly those that rely on employee credential security for regulatory compliance, operate in environments where an internal access breach would trigger reporting obligations, or want to shift their security posture from reactive detection to proactive prevention.

08 · LEARN MORE & CONTACT

Learn more about Banyax M/ETI (Managed External Threat Intelligence)+ M/XDR (Managed Extended Detection & Response) + M/AT (Managed Awareness Training)

Discover how Banyax's integrated suite — M/ETI, M/XDR, and M/AT— detects threats before they reach your employees.

Visit: banyax.com

Want to learn more?

If this document was forwarded to you and you'd like to explore how Banyax can help your organization prevent threats before they launch — reach out directly.

Email: marketing@banyax.com

Website: banyax.com