NOPALCYBER

GLOBAL PHARMA GIANT CASE STUDY

Can Incident Response Actually Defeat Cyber-Attacks?

NopalCyber Found the Answer for One Pharma Giant

The Challenge:

Ensuring They Were Prepared for an Incident

Cyber-attacks are now a certainty for all companies. In some highly sensitive industries, they are a near-constant threat and potentially cause deep and lasting disruption. Incident response plans are designed to help companies prepare for attacks in advance, so they know precisely how to react when alarm bells go off.

Having a plan must be considered mandatory… but that's just the start.

In an atmosphere of dynamic cyber risk, where attacks evolve and emerge non-stop, incident response plans can lose their effectiveness. Plans developed yesterday aren't necessarily equipped to handle the incidents of tomorrow. Worst of all, that deficiency might only become apparent once the attack is underway, and the response plans are inadequate.

Our client, a global pharmaceutical company, understood the risks and had a plan in place. Given their highly regulated industry and to be better prepared for any potential attacks, they decided to test for their strengths and weaknesses.

Enlisting Experts for Incident Response Assessment

Who better to assess incident response than a team of cybersecurity experts with decades of collective experience fighting cyber-attacks and with hard-won insights about what a good (and bad) incident response (IR) plan looks like?

NopalCyber offered such expertise, along with the specialty and scalability to serve a large enterprise client in the high-risk and regulated pharmaceutical industry.

Nopal was brought on board to conduct a complete incident response assessment and detail actionable improvements.

Nopal's scope was wide-ranging, but the goal was to create a real-world, successful incident response plan.

Nopal's analysis covered at a minimum:

- Conducting stakeholder interviews to understand how IR performs on the ground, in the heat of the moment.
- Reviewing all plans and policy documents to identify strengths and opportunities and develop a maturity score for each IR lifecycle phase.
- Hunting for and isolating existing threats such as low or slow ransomware, hidden across attack vectors.
- Performing recovery testing on applications in critical departments.
- Testing for resiliency against the most prevalent ransomware strains.
- Assessing past performance, current roles/responsibilities, organizational design, patching operations, logging capabilities, and other critical KPIs.

First Assessment, Then Improvement

All incident response plans were assessed against NIST SP 800-61 Rev. 2, which outlines best practices for incident response—practices now required, in whole or in part, by many regulatory frameworks. This allowed Nopal to identify gaps, quantify deficiencies, and expedite compliance.

After an extensive analysis and review, Nopal:

- Presented a comprehensive report of data, findings, and recommendations, and shared critical actionable details with senior security, IT and operational leadership stakeholders.
- Developed maturity scores for IR activities and prioritizing improvement areas.
- Created detailed road maps to improve each issue that was identified.

The Assurance of Being Prepared

Nopal made 42 specific recommendations on how the client could improve detection, response, communication, recovery, and incident response. Each recommendation resolved a specific issue that was identified during the assessment. With these enhancements the client is now in the best possible position to be prepared for any potential attack.

About NopalCyber

NopalCyber makes cybersecurity manageable, affordable and reliable. Managed extended detection and response (MXDR), attack surface management (ASM), breach and attack simulation (BAS), and advisory services fortify your cybersecurity position across both offense and defense. AI-driven intelligence in its Nopal360° platform, NopalGo application, and its proprietary Cyber Intelligence Quotient (CIQ) lets anyone quantify, track, and visualize their cybersecurity posture in real-time. NopalCyber's offensive and defensive services and external threat analysis are tailored to each client's need and budget, NopalCyber democratizes cybersecurity by making enterprise-grade security available to organizations of all sizes.