Customer Story

CYFIRMA
DECODING THREATS

Large Pharmaceutical Company Secures Medical Goods Distribution with DeCYFIR™ Advanced Threat Intelligence

COMPANY

Large Pharmaceutical Company

INDUSTRY

Pharmaceutical & Manufacturing

HEADQUARTERS

Asia

SOLUTION

DeCYFIR – Advanced Threat Visibility and Intelligence Platform

CHALLENGES

- Increasingly aggressive threat landscape amid COVID-19
- Expanding attack surface
- APTs likely from deep-pocketed adversaries

BENEFITS

Mitigated
Nation-State Attack

>USD 100M
Financial Losses Averted

10X
Lower Incident Rates

8X
Faster Incident Remediation

Reclaimed
Control of Threat Landscape

ABOUT THE COMPANY

The large pharmaceutical company develops and distributes medical goods on a global scale. It has a manufacturing presence across many countries and a complex supply chain network, involving many different stakeholders – from its multiple manufacturing facilities, to third-party logistics and cold chain providers, as well as warehouses and distribution centers. With increasing digital transformation, the company has put in place a cybersecurity strategy to safeguard its digital assets and technology environment.

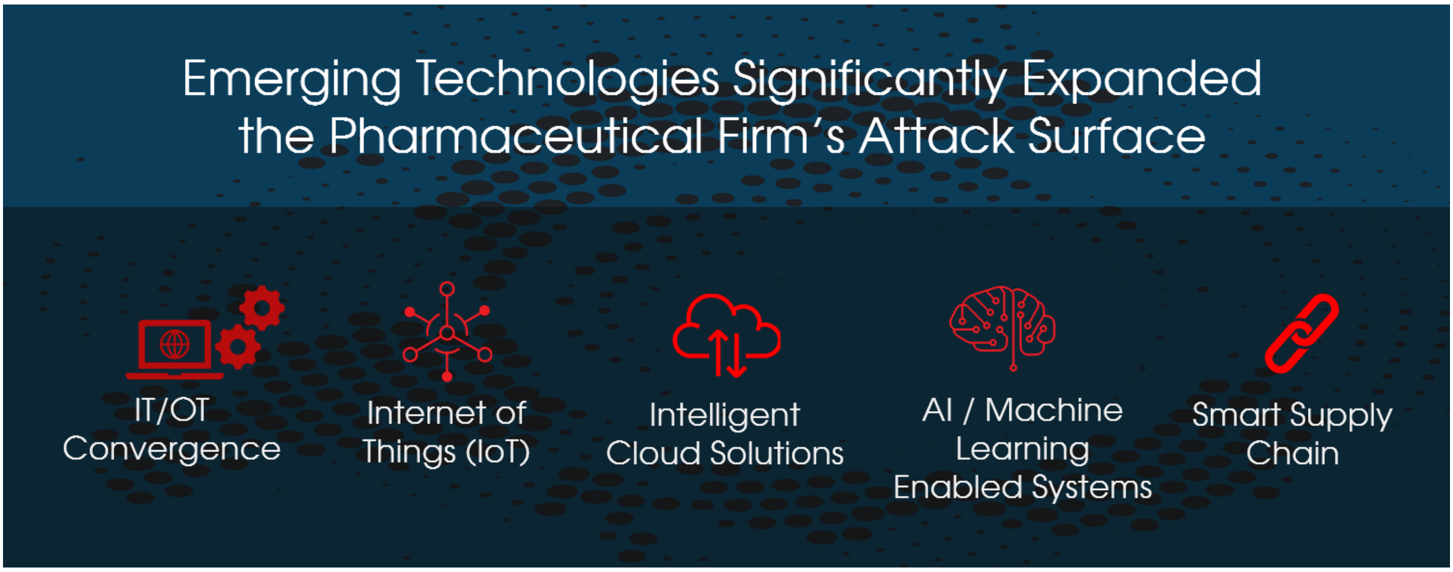
THE CHALLENGE

The COVID-19 pandemic thrusted the pharmaceutical industry into the global spotlight. Positive news on successful vaccine developments have been accompanied by grimmer updates that pharma companies are facing disproportionate levels of targeted malicious attacks.

With valuable vaccine research data and information on how key medical goods are being supplied across the world, pharma firms are viewed as lucrative targets by cybercriminals lurking in the dark web.

> "DeCYFIR™ helped us stop a nation-state sponsored attack."
>
> SOC Team Leader, Large Pharmaceutical Company

> "The DeCYFIR™ solution from CYFIRMA made a critical difference to us amid an increasingly aggressive threat landscape that was mounting due to COVID-19. "
>
> CTO, Large Pharmaceutical Company



Emerging Technologies Significantly Expanded the Pharmaceutical Firm's Attack Surface

IT/OT Convergence

Internet of Things (IoT)

Intelligent Cloud Solutions

AI / Machine Learning Enabled Systems

Smart Supply Chain

Mounting threats amid COVID-19

This large pharma manufacturer too found itself a growing target of malicious cyber adversaries. It encountered increasingly sophisticated campaigns, including brute force, ransomware, BEC and spear-phishing attacks, as well as credential harvesting attempts to access sensitive vaccine transport and distribution information.

The company also faced multiple attempts from hackers who tried to exfiltrate intellectual property, sensitive clinical trial information, customer information, and medical product information for geopolitical and financial gain.

Expanding attack surface countered system hardening

It did not help that the pharma company's attack surface was expanding due to the growing convergence of its IT and operational technology (OT) environments. In addition, more devices, industrial control systems (ICS) and SCADA systems were getting connected over the Industrial Internet of Things (IIoT) as well as Information sharing with third parties/supply chain broadens the attack surface and vector. This made it more challenging for its security operations center (SOC) team to detect attack vectors and secure weak points. It also reduced the effects of the team's system hardening efforts.

Intensifying attacks hint at deep-pocketed adversaries

As a result, the threat actors were able to leverage zero-day exploits, among other system vulnerabilities, as well as weak web and mail applications. They also tried to implant malware.

The SOC team suspected this was an advanced persistent threat (APT). This was highly alarming as APTs usually mean determined, capable and deep-pocketed adversaries.

Far-reaching repercussions if hackers succeeded

If successful, the malicious actors would cause extensive damage in stolen data and trade secrets, as well as hijacked medical supplies.

This had serious repercussions for the pharmaceutical company. Lost or damaged research data would mean the need to repeat entire clinical trials and absorb associated costs.

Seized medical goods could be sold in the dark web to traffickers who use the products in illicit drugs. Share prices could plummet. And the company's brand could be irreparably tarnished.

Over-stretched security operations team

To fend off the attacks, the pharmaceutical firm's security team was working overtime. This was despite having a competent and sizable team.

The company's senior management decided this was untenable.

They wanted to regain control of threats by gaining greater visibility of its cyber posture online. It was also critical that they find out if the pharmaceutical company was being specifically targeted by any threat actors and/or campaigns.

HOW CYFIRMA HELPED

The large pharmaceutical company looked to CYFIRMA to actively provide insights to its team and identify even unknown, signatureless threats – so that if anything malicious penetrates its defenses, the firm will have the right intelligence to rapidly remediate the situation.

Predictive threat intelligence uncovered nation-state espionage

DeCYFIR™, CYFIRMA's flagship product and the world's first predictive cyber-intelligence platform, quickly detected discussion in hacker forums, unveiling interest from well-resourced nation-state actors, including North Korea, that are mounting aggressive and focused campaigns.

These threat actors had interest in this pharmaceutical company as well as many others in the same sector globally. They planned to disrupt the supply chain and hijack physical logistics vehicles.

WHY IT MATTERS: With a clear understanding of the attack vectors, the pharmaceutical company was able to fortify its security posture to prevent the sophisticated state-sponsored attack from evolving into a breach.

Multi-layered intelligence delivered relevant insights for C-suite and SOC team

To ensure effective consumption of cyber threat intelligence, DeCYFIR™ delivers intelligence across multi-dimensional levels in the organization – namely strategic, management, and operational. This capability proved critical as it disclosed crucial information for the COO, CTO as well as the SOC teams.

The intel included the who, why, where aspects regarding the threat actors which helped the C-suite assess and decide on the overall defense approach.

DeCYFIR™ also answered the how and what elements, identifying critical gaps and vulnerabilities in the IT infrastructure and supply chain software, plus other weak services exposed to the internet which the SOC team could remediate at once.

WHY IT MATTERS: On a strategic level, it provided the C-suite with a better grasp of the threat profile, motive, and method to help them reach critical decision-points from a strategy, governance and policy perspective.

On a tactical level, it empowered the SOC team with immediate time horizon issues so they can update security controls (such as SIEM rules, and endpoint protection) against the latest threat vectors.

Personalized intelligence thwarted exploits

DeCYFIR™ also delivered customized insights to the pharmaceutical company based on its its geography, industry, technology. This allowed the firm to deploy its cybersecurity assets according to the severity of threats.

WHY IT MATTERS: Personalized threat intelligence enables organizations to focus on what matters and cut out irrelevant noise that muddles decision-making.

Contextualized insights into the making of cyberattacks

DeCYFIR™'s risk dossier with threat actor attribution, campaign and method details provided deep insights into cyberattack campaigns which are in the making and those currently underway.

This includes who malicious actors are, what they want, why are they interested, how they view their targets, the hackers' readiness to attack, and potential attack methods.

Based on that, the SOC team averted a supply chain cyberattack campaign targeted at 17 global pharma companies and hospitals working on COVID-19 research, as well as approving authorities across many countries including USA, UK, India, and Japan.

The hackers planned to exploit weaknesses in systems and lateral movement, implant ransomware, conduct targeted spear-phishing attacks on employees and exploit vulnerable systems running Citrix, RDP and SSHD.

WHY IT MATTERS: By fully understanding the attack surfaces, intent of malicious actors, and potential attack vectors, the pharma firm could harden its systems in the appropriate areas.

Risk ratings for every alert + full attack surface view = more assured decision-making

With risk and hackability scores that come with every alert from DeCYFIR™, the pharma company's SOC team was able to prioritize and remediate critical risks rapidly, and in order of severity.

A complete view of the company's attack surface also helped the firm better conduct attack surface analysis and work on reducing vulnerable areas.

WHY IT MATTERS: With millions of attack vectors, assessing the optimal next steps can be tricky.

By flagging the most critical risks and showing the full attack surface on a single platform, DeCYFIR™ helped the company make more confident decisions to bolster its defenses and contain risks.

At the same time, a holistic view of the complete attack surface helped the company understand its exposure level to work on lowering it.

SECURING MEDICAL GOODS DISTRIBUTION AMID AN AGGRESSIVE THREAT LANDSCAPE

Today, the large pharmaceutical company is using DeCYFIR™ daily within its SOC and at various levels across the organization for risk exposure assessment and attack surface evaluation.

With DeCYFIR™'s advanced threat intelligence that is designed to meet the most stringent demands of CISOs, Chief Risk Officers (CRO), and Security Operations teams, the company has been able to secure its supply chain to ensure its drugs and medical devices get to the right places and people, despite an aggressive threat landscape.

The company has also been able to better optimize its cybersecurity resources. Plus, enhance its security posture. This has given the firm a firmer foothold on its digital assets and technology environment.

The pharma's firm fortified defense capabilities include being able to:

Act early with relevant, personalized, and contextualized threat alerts

With tailored insights and early warnings of cyber criminals and other threat actors targeting the firm, the SOC teams has been able to take immediate remedial actions to mitigate risks.

Predict cyberattacks and prevent breaches

By proactively identifying threats at the planning stage of campaigns from known or unknown threat actors and vectors. DeCYFIR™ has allowed the pharma firm to strengthen its security posture to prevent malicious attacks before they happen.

Adapt based on emerging cyber adversaries and threat vectors

By connecting the dots between hacker, motive, campaign and method, DeCYFIR™ gives the pharma company a complete context of the threats. This helps the firm continuously adapt based on emerging threats, e.g., implement important security defenses such as securing open remote desktop access ports and phishing security.

To learn more about DeCYFIR™ and CYFIRMA, visit **WWW.CYFIRMA.COM**

About CYFIRMA

CYFIRMA is a threat discovery and cyber-intelligence platform company. We combine cyber intelligence with attack surface discovery and digital risk protection to deliver predictive, personalized, contextual, outside-in, and multi-layered cyber-intelligence. We harness our cloud-based AI and ML-powered analytics platform to help organizations proactively identify potential threats at the planning stage of cyberattacks. Our unique approach of providing the hacker's view and deep insights into the external cyber landscape has helped clients prepare for upcoming attacks.

CYFIRMA works with many Fortune 500 companies. The company has offices located in the USA, Japan, Singapore and India.

Visit https://www.cyfirma.com/ today

CYFIRMA

DECODINGTHREATS

twitter.com/cyfirma

facebook.com/Cyfirma/

linkedin.com/company/cyfirma

www.cyfirma.com