SecureWorks

BIG BIOTECH FIRM KEEPS INTELLECTUAL PROPERTY SAFE

A fast-growing, global biotech company needs protection, especially for its intellectual property, so it engaged SecureWorks for managed services and staff support

Company: Biotechnology firm | **Industry:** Healthcare | **Country:** U.S.

BUSINESS NEED

With nearly 8,000 employees and a small IT security staff, this global this global biotech firm was concerned not only about protecting its data and networks but intellectual property, too.

SOLUTION

The company improved its security posture with managed firewalls and intrusion protection from SecureWorks, backstopped by threat intelligence, forensics services and SecureWorks resident staff support.

BENEFITS

- Improved intellectual property security
- Extended transnational firewall protection
- Enhanced intrusion response capabilities
- Reinforced staff expertise and experience
- Improved awareness of vulnerabilities
- Achieved much more mature security levels

PRODUCTS | Advanced Endpoint Threat Prevention | Digital Forensics Services and Malware Analysis | Managed Firewall | Managed iSensor Intrusion Protection System | Managed Security Services Integration | Security Residency and Implementation | Targeted Threat Intelligence Services

In the life sciences and biotechnology industries, intellectual property — especially patents, trade secrets and trademarks — are foundational assets that can be worth billions of dollars to the companies that own them. And they can be worth millions to anyone stealing and reselling them to interested third parties. Small wonder that so-called "IP" can be inviting targets for threat actors and competitors focused on industrial espionage. This adds even greater urgency to the importance of securing the networks and data of companies in these industries.

Such was the case for one fast-growing, global biotech company that has steadily growing over the past several years to a multi-billon dollar company. With the successful launch of several medicines in its portfolio. Its success and industry fame made it a ripe target for attack. And its dated firewalls and security practices made it extremely vulnerable to one.

EXPLOSIVE GROWTH EXPANDS ATTACK SURFACE AND VULNERABILITIES

By that time, the company had grown to 5,000 employees employees and contractors with overseas manufacturing and sales offices. The company's attack surface had expanded dramatically yet its cyber safeguards had barely kept pace. Typical was manual monitoring of the company's anti-virus console and ad hoc reporting. A 24x7 incident response protocol was non-existent. When an attack might occur, the company was not prepared to deal with it.

Fortunately, a newly hired CISO realized this after looking into the biotech firm's risk posture. To start strengthening security, the CISO contacted SecureWorks. He had come to know SecureWorks and its capabilities based on his prior experience with the company at his previous employer, a Global 500 firm.

The initial engagement involved SecureWorks Managed Firewall services supported by a Managed iSensor Intrusion Prevention System (IPS). To install and commission this infrastructure, SecureWorks Managed Security Services Integration was called in. The company started with two iSensors in their headquarters and another major location, but within two years, expanded that coverage to two more large corporate competency centers plus their manufacturing site in the European Union.

MANAGED SECURITY SERVICES BOOST SAFEGUARDS IMMEDIATELY

With the iSensor IPS, the biotech firm gained an immediate and quantum leap in its cyber defenses. While the iSensor devices perform in-line, deep-packet inspections of all inbound and outbound network traffic, they are monitored continually 24x7 by SecureWorks Security Operations Centers (SOCs). All upgrades and patches are automatically applied, with performance and availability are also closely watched.

In addition, the iSensor units stay fully updated with proprietary intelligence from the SecureWorks Counter Threat Unit (CTU) research team. It evaluates billions of security events from across the SecureWorks global client base and information from thousands of sources worldwide to discover new attack techniques and threats as they emerge. This intelligence keeps the iSensors fine-tuned to provide the best protection possible.

ACTIONABLE ADVANCED THREAT INTELLIGENCE FOR STRATEGIC INSIGHTS

To further enhance its security posture, the company also retained SecureWorks Targeted Threat Intelligence. This service complements the CTU intelligence that keeps the iSensors updated day-to-day by providing more strategic insights to threats, including those specific to industrial espionage, intellectual property theft and sources of threats that may target the firm. In effect, it provides the IT staff with go-to, expert resources to understand and proactively take counter-measures against threats beyond the company's networks.

Should an attack occur, the company has added a critical component to its incident response (IR) readiness: SecureWorks Digital Forensics Services and Malware Analysis. For enterprises like this one, with billions of dollars of IP to protect, it's not enough to isolate and clean infected devices and network domains, which is a typical IR protocol. They also need to determine the full extent of a breach and know how far their systems have been penetrated and what, if any, IP has been exfiltrated.

ON-SITE STAFF AUGMENTATION WITH EXPERTS

Several years ago, as the biotech firm was growing explosively, it was determined to keep its cost curve behind its revenue growth to ensure profitability. One way to do that is to contain labor costs. That's one reason it decided to take advantage of the SecureWorks Residency and Implementation service. This provides full-time, onsite security experts to augment IT staff expertise.

The company started with one SecureWorks staff member and eventually added another, bringing its total IT security staff, including managers, to eight. Aside from the firm's caution about adding headcount, it has found several other benefits to having two SecureWorks resident employees on its IT security team.

One, of course, is having security experts onsite every day to work should-to-shoulder with the company's own staff. Another is help with education and awareness of employees at large, especially in areas of behavioral concern, such as phishing. A third is the customer advocacy the residents provide inside SecureWorks — knowing who to talk to about what and how to escalate and expedite issues for resolution.

SECUREWORKS PORTAL KEEPS STAFF INFORMED

The IT security team uses the SecureWorks Portal extensively for updates on security news and information, alerts on critical events and a variety of reports. One example is the timely analysis on Microsoft's monthly patches that the CTU provides. This helps the patching team make its decisions on priorities following what's known as "Patch Tuesday" and its evil twin "Exploit Wednesday" — when new threats start emerging to take advantage of what Microsoft has revealed the previous day.

In all, SecureWorks has helped the biotech firm achieve a maturity level in its security defense model that it lacked before. Its vastly improved security posture has lowered its risk profile and vulnerability exposure. Today, all its stakeholders — shareholders, employees and customers — can rest assured that not only are its data and networks well-protected but also its intellectual property.