NETWITNESS

CASE STUDY

How Does a Defense Contractor Get Their Ideal Security Environment?

A security incident prompts a SIEM replacement, but Professional Services sets a course for the future

Defense contractors play a vital role in the United States government: supplying departments and agencies with the tools they require to protect the country's citizens, borders, critical infrastructure—and more. The important role that these contractors play makes them attractive targets for cyber threats, from small-scale threat actors looking to exploit vulnerabilities to coordinated hacking organizations from enemy nation-states out to cause nationwide havoc.

One prominent defense contractor is used to repelling these kinds of attacks. "We know that we're targeted often. As a part of the defense industrial base, it's normal for us. We see ransomware and other advanced persistent threats (APTs), but we're also on the lookout for insider threats. These threats are both in terms of people not exercising proper security practices as well as malicious insiders who might be trying to steal our intellectual property," said the company's information security manager.

A Successful Attack Prompts a Change in its SIEM

Unfortunately, this organization experienced a cyberattack which its legacy SIEM (security information and event management) product was unable to detect. The result was an effective infiltration. To avoid similar outcomes from future attacks, the company knew that it must modernize its sceurity capabilities to gain better visibility into its environment.

After evaluating multiple SIEM solutions, the IT team determined that the NetWitness Platform would provide the threat detection and response capabilities the company required. What the organization didn't realize at the time, however, was that its decision would deliver two-fold success: not only replacing the SIEM, but also setting the course to optimize its entire cybersecurity game plan.

"The first goal for implementing the NetWitness Platform was to get our security infrastructure to a more stable place. We needed to understand what we could see and what we needed to see. We came to the realization that we could go far beyond simply monitoring logs. We determined we could optimize and tune the NetWitness solution to our specific requirements, and its capabilities would scale right along with our needs," says the IS manager.

That legacy SIEM was not providing true monitoring; the NetWitness Platform opened new possibilities for faster and more comprehensive threat detection. NetWitness also provided the organization with the ability to correlate data and deliver more advanced threat intelligence than previously achieved.

"If the security doesn't provide that data correlation, you have to do it in your head, which I always say is using analog speed for digital data—it's doomed to fail," notes the IS manager.

NetWitness Professional Services Takes the Mission to the Next Level

But adjusting the strategy is easier said than done. This team already had its hands full with its day-to-day tasks of protecting the organization's infrastructure and data. "We needed more hands than we had, so we turned to NetWitness' Professional Services team," the manager explains. "That was the boost we needed, both to help with optimizing the solution for our environment, and for ad hoc things like incident response. For any company out there considering whether to add NetWitness Professional Services, do it. The engagement is worth the time and budget. When you're in a high-stress situation, you don't want to be looking through your contacts to find someone to call."

The successful combination of the NetWitness Platform and Professional Services has prompted this defense contractor to elevate its cybersecurity capabilities even more. Case in point: it's currently looking to replace several of its point solutions for endpoint detection and response with NetWitness.

"We're working on getting as much data as possible onto the platform in the next few years. We love the efficiency of the solution and are really happy with the gained visibility we have. It only makes sense to tie NetWitness into more of our infrastructure," says the IS manager.

About NetWitness

NetWitness, an RSA® Business, provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats. For more information, go to **netwitness.com**.

The Industry

Defense contractor

The Challenge

When a breach happens—is it too late? Not always, as this company's cyberattack served as a successful wake-up call to examine its legacy systems and improve security ops.

The Solution

- NetWitness Platform
- NetWitness Professional Services

Why It's Working

The combination of the NetWitness Platform and Professional Services provides defense contractors with critical visibility; visibility that empowers any size team to stay vigilant against continuing threats to data and infrastructure.

NETWITNESS
An RSA Business