Customer story

expel®

Pharmaceutical company selects Expel for 24x7 monitoring, detection and response

Transparent managed security approach allows pharmaceutical company to detect and respond to incidents during the first 10 minutes of the "golden hour"

Pharmaceuticals

The company

This global pharmaceutical company develops life-changing therapies for patients and families affected by rare diseases. Soon after the company brought to market its best-known drug, a disease broke out in Europe and this drug proved to be an effective treatment. The company grew rapidly. Within a year, they'd been added to the NASDAQ-100, the 100 largest non-financial stocks traded on the NASDAQ.

> "With Expel, we know someone is looking out for us, which gives us time to focus on tactical gaps in our armor, and the luxury to be thoughtful and deliberate about them."

The situation

The company's rapid growth placed new demands on its IT infrastructure. According to the company's senior director of global security operations, "At the time, IT was completely *ad hoc*. It existed entirely to enable the business. Security wasn't top of mind."

But when the organization grew, it built out its IT infrastructure and security quickly came to the forefront. They hired a CIO and a chief information security officer (CISO). The CISO assumed responsibility for physical security *and* cybersecurity, with both managed from the company's global security operation center (SOC) in the northeastern United States.

The senior director of global security operations joined the organization as they were building the security team. When he came aboard, he was struck by how exposed he felt. The company was using a managed security service provider (MSSP) for detection and monitoring, but there were gaps. "Our MSSP was providing eight-by-five coverage, but it was entirely dependent on how they had configured Splunk," he recalled. As a result, the MSSP was blind to key parts of the company's infrastructure, and even when the MSSP generated alerts, it would just pass them back to the company's in-house security team. "They weren't doing any meaningful investigation," he said.

To better understand the problem (and, ultimately, what the solution would be), the customer rolled up his sleeves and sat down in the security analyst's chair. He triaged alerts, decided what needed to be escalated and got a front row view of the company's infrastructure and alert stream.

"That was a very sobering three-week period for us. It really solidified our thinking. We concluded we needed a partner who could focus on monitoring and detecting incidents and then investigating and handing them off to us," he said. "It also convinced us of the importance of immersion. Everyone associated with an incident response effort has to be immersed in it from beginning to end. It can't be a hot potato that's passed from a tier one analyst to a tier two analyst and so forth."

Armed with a clear vision of what the organization needed, the company prioritized finding a vendor who could provide 24x7 coverage and help them create a real and repeatable incident response capability.

> **"In the past, an incident would trigger a linear series of events, starting with an alert, progressing to escalation and eventually a ticket, at which point the security team would finally awaken to the danger. The swarming approach we've implemented with Expel eliminates that waiting. Waiting for a trigger, a ticket or for someone else to take action. All that waiting costs time during that critical first 10 minutes of an incident."**

Evaluating options

The customer evaluated seven different managed security service providers, including what the senior director calls "all the traditional and conventional providers." But he and his team believed that to turn their vision into reality, they also needed to include providers with new, innovative approaches.

His previous experience working in highly-targeted industries had led him to the conclusion that security operates within a "golden hour." It's akin to how trauma physicians and first responders approach medical emergencies, where the first 10 minutes spent stabilizing a patient for transport is critical to the ultimate outcome.

"In the incident response world now, with the threat environment, multi-stage attacks, things that get past initial defenses and exploit user privilege, we have about 10 minutes – and that's probably generous. Just 10 minutes right up front, to detect, recognize and contain."

Early in his tenure at the company, he was at an event where he encountered Expel's CEO, Dave Merkel (or "Merk" as he's been called since his first name went missing sometime in the late 90's). As the customer recalls, "Merk's presentation piqued our attention right away. Expel's approach aligned really well with our vision. The team's pedigree, attitude and Merk's ability to speak to lessons learned in the environment really made an impression."

After a rigorous evaluation process, which included an RFP, detailed technical evaluation and customer references, the pharmaceutical company ultimately selected Expel's 24x7 service with hunting.

How Expel helped

According to the customer, service onboarding went exactly as Expel had promised during the sales process. He could tell Expel had put a lot of engineering effort into keeping it simple. "From start to finish, it took about five days to get Expel up and running, including a day or so of upfront work," he said. "From there, it was a matter of tuning and iterating and ensuring the initial data flows were optimized."

With Expel running smoothly, the customer and his team finally had some space to think through the next steps of their security strategy. As he describes, "With Expel, we know someone is looking out for us, which gives us time to focus on tactical gaps in our armor, and the luxury to be thoughtful and deliberate about them."

Expel also helped the organization realize their vision of responding to incidents during the "golden hour". With Expel on board, he says they're now able to "swarm" an intrusion.

"In the past, an incident would trigger a linear series of events, starting with an alert, progressing to escalation and eventually a ticket, at which point the security team would finally awaken to the danger." Because of Expel's transparency, now everyone has visibility from the get-go. "The swarming approach we've implemented with Expel eliminates waiting. Waiting for a trigger, a ticket or for someone else to take action. All that waiting costs time during that critical first 10 minutes of an incident."

Now, he says, the company is able to embrace the idea of immersion. The dashboard in Expel Workbench is visible to the entire team. It's "perfectly configured" so everyone can observe investigations as they're unfolding, even as Expel's analysts are conducting investigative steps, documenting those steps and alerting our entire team.

Like most organizations, the pharmaceutical company has lots of potential attack surfaces – from research and development to manufacturing to its global network and its employees' personal devices which the company's "bring your own device" policy allows. "If you look at all of the attack surfaces, there's real exposure," says the customer. "All that risk – and the importance we place on serving the patients and families who rely on us -– drives the urgency of our immersion approach. We can't afford to have silos when it comes to security."

> **"The ultimate measure of effectiveness is when we can keep security events from materially degrading or disrupting our business. Every bit of the data that we're getting from Expel Workbench helps us to demonstrate the volume and velocity of things happening in our environment that have not resulted in a breach or hindered our ability to do business. Those are the kinds of numbers CFOs like to explore and understand."**

According to the customer, sometimes things are running so well that they feel like they might be missing something. He once had one of his analysts message Expel's analysts at midnight, just to see what would happen. Apparently, it had been awhile since anything graduated to an incident, and they got antsy (the analyst replied right away and let the team know everything was clear). The customer also knows his team members can reach the Expel crew in a variety of ways. They've got Slack on their mobile phones, and they get emailed alerts as well.

Benefits

The pharmaceutical company has experienced several tangible benefits from working with Expel, beyond a fundamentally better security operations workflow.

Reduced risk

All security organizations, including the customer's, reduce risk. While detecting and responding to incidents is one way to reduce risk, they'd prefer to prevent them from occurring in the first place. The proactive resilience recommendations that Expel provides have helped this company do that.

For example, after one investigation where Expel detected and stopped an attack, the Expel analysts provided a resilience recommendation that allowed the customer to prevent similar attacks in the future.

"There's no better scenario than that. With Expel, we detected it, we isolated it, we quarantined it and we did the postmortem. We understand the root cause and now we're making the changes so it can't happen again."

Benefits of partnering with Expel:

- ✓ Reduced risk
- ✓ Return on investment

Return on investment

Investigations like this also demonstrate the return on the organization's investment in Expel.

The customer uses data from Expel Workbench to communicate the benefits he's getting from the service and help justify continued security investments. "The ultimate measure of effectiveness is when we can keep security events from materially degrading or disrupting our business," he says. "Every bit of the data that we're getting from Expel Workbench helps us to demonstrate the volume and velocity of things happening in our environment that have not resulted in a breach or hindered our ability to do business. Those are the kinds of numbers CFOs like to explore and understand."

The customer's relationship with Expel is very interactive. "There's a continuous feedback cycle," he says. "We're learning over time about how the alerts are being processed, what the sensors are telling us, and it's clear that Expel's systems and analysts are learning about us and our environment."

A look ahead

This pharmaceutical company has a big vision for security. “We want to share our experience with our community, so we can all improve. We also want to learn from others.”

Ultimately, they want to converge all of their security functions to the point where they can live in that 10-minute window, the golden hour of incident response.

“All security professionals say you have to keep the lights on, right? We’ve got to keep the business running. I can’t leave that out of it. Ultimately, we’re here to enable a business to develop and deliver life-changing drug therapy. We’re committed to that, absolutely. And we also want to be a leader in how we secure that.”

Expel provides transparent managed security. It’s the antidote for companies trapped in failed relationships with their managed security service provider (MSSP) and those looking to avoid the frustration of working with one in the first place. To learn more, check us out at www.expel.io