Vulnerability Management at Diebold: Automation, Prioritization, Remediation

Success Story

Challenge: Diebold needed an effective threat exposure management solution that would offer scalability and visibility.

Solution: Nexpose helps align risk with what matters most to the business; automated scan and prioritized remediation saves time

The name Diebold has long been synonymous with innovative technology and security systems. Headquartered in Canton, Ohio, the company has approximately 16,000 employees worldwide and boasts a service team that's one of the largest in the industry, with more than 7,000 field professionals serving 600 locations.

Due to the company's global footprint, somewhere in the world the sun is always shining on Diebold. Ryan Elkins, Senior Manager of Information Security at Diebold, calls it a "follow-the-sun" model in terms of support, which is provided 24/7. And if the data is always flowing, then the security team needs to be on their A-game.

Effective Vulnerability Management

"Those of us who are on the Diebold security team look at part of our role as being advocates and consultants to the business, and encouraging security throughout," Ryan says. That also means having a general awareness of what's going on, from a security standpoint, and what needs to be remediated. "Vulnerability management offers an end-to-end approach to ensuring that the security posture at Diebold remains consistent with our requirements. That starts at a tactical level, where we identify issues, and it extends all the way up to governance, risk and compliance where we compare policy scans to industry baselines."

Given the pivotal role vulnerability management plays at Diebold, selecting a vulnerability management solution was an important task which the team did not undertake lightly. "A main priority for us is the effectiveness of the vulnerability scanner," says Ryan. "Diebold needs accurate, up-to-date, real-time data. Scalability is also an important factor; we're a global company and we need the ability to reach around the world without adding administrative overhead. Which is why Rapid7 Nexpose Enterprise fits the bill – it offers a centralized console and scan engines, so our vulnerability administrators can get the right visibility and global coverage. Using Nexpose, we regularly scan every IP on the network."

> "The automated asset classification, risk prioritization, and remediation assignment in Nexpose are a big value add."
>
> ~Ryan Elkins, Senior Manager of Information Security, Diebold

Prioritizing and Managing Risk

Ensuring that security aligns with business needs is a key goal for any security professional, most of whom know firsthand the challenges of communicating effectively with other business units like IT and management. That holds especially true for a company of Diebold's size.

> "Diebold needs accurate, up-to-date, real-time data. Scalability is also an important factor... Which is why Rapid7 Nexpose Enterprise fits the bill."
>
> ~Ryan Elkins, Senior Manager of Information Security, Diebold

So how does a senior infosec manager at a global company measure success? Ryan says there are several ways – from a vulnerability management perspective, Nexpose allows him to compare trends from different geographic locations on a month-by-month basis, and allows him to focus on the highest risks that matter most to the business. Rapid7 RealContext™ allows risk to be aligned with business priority, ensuring that resources are used effectively to mitigate risk that matters; risk asset context is automatically completed, saving valuable time for security professionals. "We want to make sure everything is aligned, from a data protection perspective as well as with the needs of the business," he says. "The automated asset classification, risk prioritization, and remediation assignment in Nexpose are a big value-add in that respect."

Automation is also an integral component of quantifying risk. "It's a huge factor in being able to scale, and be effective," says Ryan. "There are never going to be enough hours in the day to tackle everything on your to-do list – you need prioritized remediation. We really try to automate what we can, which includes distributing reports automatically to corresponding groups and internal security teams for even better alignment."

Be Selective

Ryan is careful when navigating and choosing from the slew of security offerings in today's marketplace. Rapid7 passed the test, and he advises all organizations to apply thorough criteria during the qualification process before making a final purchase decision.

"Whether for compliance, an audit check, or some other reason, companies will often go out and buy technologies that cover vulnerability management, data loss prevention, etc. They grab tools, implement them, and then find themselves with a huge mass of data they can't strategically leverage – or that they need more resources to manage. My advice is this: When it comes to risk management, always think about the underlying process so you know what technology you need. Understand your locations, your assets, your critical networks, and where sensitive data is housed. Dedicate scans to your most critical assets and networks segments, and have a solid patch management process."