Business challenge

This international dairy products company wanted to improve its security posture but lacked the internal resources to build and run its own security operations center.

Transformation

With locations in Ireland, the UK, Spain, Germany and China, Ireland's largest farmer-owned dairy company must protect its large and diverse network environment. Engaging IBM Business Partner Smarttech247 to help implement IBM® QRadar® SIEM and IBM BigFix® endpoint management plus provide alert oversight significantly improves its security posture.

Results

90 days
from signed contract to operational SOC

4 million
events reduced to 17 actionable incidents with QRadar SIEM

One
source of information for determining asset inventory with BigFix

Dairygold

Leveraging IBM QRadar out-of-box use cases and IBM BigFix ease of use to improve security posture

Located in the heart of Ireland's most green and fertile milk production region, Dairygold Co-Operative Society Ltd. processes 1.3 billion litres of milk annually (17 percent of the Irish milk pool) from its 3,000 milk suppliers. Headquartered in Mitchelstown, County Cork, Dairygold currently employs over 1,100 people and generates a turnover of about 850 million euros from its worldwide sales. It is Ireland's largest farmer-owned dairy business and the country's second largest dairy processor.

"Our approach was to first do a product search so we could choose a SIEM platform that we as a technology team were happy with."

—Brian Padden, Group IT Director, Dairygold

Smarttech
YOUR 24/7 SECURITY PARTNER

Share this

Making security a business priority

Ireland's largest farmer-owned dairy business, Dairygold Co-Operative Society Limited processes 1.3 billion litres of milk annually, turning it into butter, award-winning cheeses and other milk products for sale within the UK, across Europe and in China. The company has factories in Ireland and the UK that process milk from more than 3,000 suppliers and sales offices in Germany, Spain and China.

Over the past five years, Dairygold has followed a well-planned strategy and roadmap for significantly improving its security posture. The effort started with reducing the number of security vendors providing solutions in areas such as client and email protection. Then came filling in gaps, such as building out an intrusion protection solution and adding data loss protection.

Each of these solution areas produces massive volumes of information, which on its own wasn't helping Dairygold understand what was happening across the network. That's why the next stage in the company's security evolution was to consolidate security data and increase global visibility with a security information and event management (SIEM) solution to provide real-time insights, threat analysis and detection.

"We knew from the beginning that we wanted to partner with someone to run the security operations for us," says Brian Padden, Group IT Director. "Our approach was to first do a product search so we could choose a SIEM platform that we as a technology team were happy with. From there we did a similar search to find the right partner."

Gaining visibility across the enterprise with QRadar and BigFix

After spending time with a number of vendors and getting advice from analysts, Dairygold selected the IBM QRadar SIEM platform along with IBM BigFix for endpoint discovery and management.

"The goal of the SIEM is to integrate all the different security information feeds and give you a view of what's going on in your environment. QRadar had a lot of our use cases already mapped out. During the selection process, if we mentioned a particular use case, generally there would already be a solution for it out of the box," says Brian Padden.

"As part of the demos we got to see some of the integration between QRadar and BigFix. Although we didn't set out to buy a patching and remediation platform at the same time, it just evolved to be the right thing to do—and emboldened the case for using QRadar as our SIEM platform."

A similar search process resulted in selecting IBM Gold Business Partner Smarttech247 as Dairygold's partner for architecting and implementing the QRadar SIEM solution and providing SOC services. Smarttech endorsed the QRadar and BigFix combination and added the IBM X-Force Exchange threat intelligence service to its solution.

"BigFix helps Dairygold understand what its vulnerability posture looks like across a large and disparate network environment with a lot of assets," says Ronan Murphy, CEO of Smarttech. "And, should there be any type of global incidents like Petya or WannaCry, we could very quickly help them to remediate those vulnerabilities in real time."

Smarttech's architecture for the QRadar SIEM implementation addressed technical issues including low bandwidth connectivity from some sites and the wide array of technologies in place across the Dairygold environment. The solution places processors and collectors across all sites to feed security data back to the centralized QRadar console operated by Smarttech.

Long term, Dairygold aims to integrate the operational technology in its factories, including ICS

> ***"BigFix helps Dairygold understand what its vulnerability posture looks like across a large and disparate network environment with a lot of assets."***
>
> —Ronan Murphy, CEO, Smarttech247

(industrial control system) and SCADA (supervisory control and data acquisition) environments as well as devices attached to the corporate LAN. Dairygold has begun investigations into who owns what and what's there in the factory systems and has brought one plant into the monitoring environment already.

"BigFix can help us with this effort because we can tell the system owners in the plants what we are seeing," says Brian Padden of the ongoing factory integration project. QRadar can accept feeds from many of the industrial control systems and help identify anomalous behavior within the factory environment or on the factory floor. Devices that pose a security risk because, for example, they are legacy components that cannot be patched can be identified and isolated from the corporate network.

Rapid implementation and reduced complexity

Within 90 days of signing the contract with Smarttech, Dairygold had an operational security monitoring environment consolidating and analyzing information feeds from the main elements of its network, including main controllers, Windows alert logs, anti-virus software, and its email security platform.

"The key element of our partnership agreement with Smarttech is that we get a piece of information that tells us what the problem is, where it is occurring and what we need to do to remediate it," says Brian Padden. According to a recent monthly report, the Smarttech SOC processed 4 million events, filtering those down to 122 items that required investigation. Out of those, Dairygold received 17 priority 3 or priority 4 incidents that the IT team needed to act on, most of which were relatively quick fixes.

"With BigFix, the big win is around reducing complexity," says Brian Padden, adding that after a side-by-side trial, Dairygold decided to drop its previous patching solution in favor of BigFix, which is "way easier to use and has a better technology engine. Deploying patches is much easier than it used to be." Moreover, instead of correlating three different data sources to derive an asset inventory, the company now relies on BigFix to provide the definitive record of its entire estate, including Windows and non-Windows devices.

Overall, Brian Padden characterizes the company's experience with Smarttech and the IBM Security products as very positive. "Like most good things in the technology field, if it does what it says 'on the tin,' then you're happy," he notes. "That's what's happening here."

> ***"The key element of our partnership agreement with Smarttech is that we get a piece of information that tells us what the problem is, where it is occurring and what we need to do to remediate it."***
>
> —Brian Padden, Group IT Director, Dairygold

Solution component

- Bigfix Endpt Security
- ISC Threat Intelligence Insights
- QRADAR

Take the next step

Smarttech247 is an award-winning cyber security organization that provides innovative solutions to global companies. The Smarttech247 SOCs are ISO9001/ISO27001 NSAI certified and they deliver a wide range of cybersecurity solutions, including cognitive security services using IBM Watson® for Cybersecurity as well as SIEM, compliance and governance, and penetration testing. To learn more about Smarttech visit: www.smarttech.ie

To learn more about IBM BigFix, visit: ibm.com/security/endpoint-security/bigfix

To learn more about IBM QRadar SIEM, visit: ibm.com/security/security-intelligence/qradar

For more information on IBM Security solutions and services, visit: ibm.com/security. Follow us on Twitter at @IBMSecurity

For more client stories, access the IBM case study home page.

Please Recycle

63029563-USEN-00