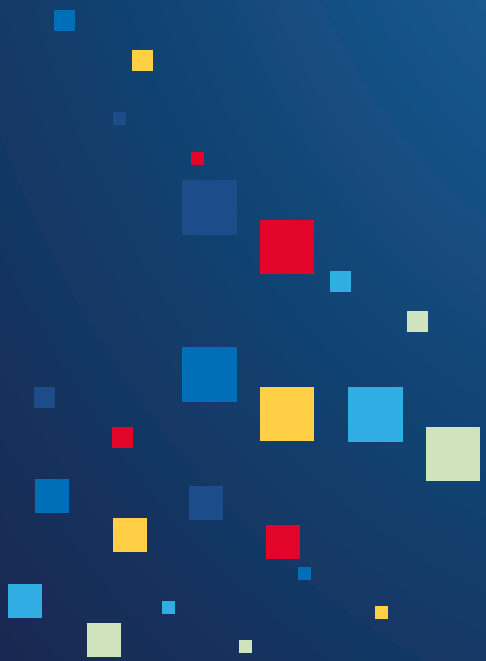
panaseer

Case study:

Schroders

Schroders retained Panaseer in June 2016, to enable, empower and automate the understanding, monitoring and reduction of its device vulnerabilities across the business.



PCS-016-2

Schroders

Company size

1,000 - 5,000

Headquarters

London, UK

Industry

Financial services

Challenges

To provide an automated, accurate, risk-based understanding of assets, controls, vulnerabilities and threats

Solution

Continuous Controls Monitoring (CCM) platform

Results

Automated reporting demonstrating impact, progress and action points to improve security posture

Schroders is a world-class asset manager operating from 32 countries across Europe, the Americas, Asia and the Middle East. Employing 5,000 people across six continents, as of January 2019 they are responsible for £421.4 billion (€469.5 billion/$536.7 billion) of assets created from a focus of bringing together people and data to spot the trends that will shape the future.

Schroders retained Panaseer in June 2016, to enable, empower and automate the understanding, monitoring and reduction of its device vulnerabilities across the business.

Challenges

Aware that the collation of security and IT data to drive visibility into its risk appetite was critical in delivering a security programme that could meet its requirements, Schroders has been consistently developing its own Management Information process.

Introduced to Panaseer at the 2016 FS-ISAC Conference in London, the platform was perfectly aligned with Schroders strategic requirements – providing an automated and accurate, risk-based understanding of assets, controls, vulnerabilities and threats. By pulling data from Schroders' security solutions and products, then cleaning, enriching, normalizing and unifying it into a single, scalable view of the truth, Panaseer has enabled Schroders to further improve its security controls.

Solution - the Panaseer Platform

Automating the ingestion and normalisation of business, IT and security data from existing sources into a single view, Panaseer's security metrics and associated dynamic dashboards have given the Schroders security and IT teams an effective and continual oversight of their security posture.

The initial focus of the platform was to generate visibility of device vulnerabilities, exploring the data to expose, highlight and diagnose problem areas, establish journeys and use cases to highlight next best actions targeted at reducing device vulnerabilities.

> **"Panaseer has allowed us to gain the insight we need into our security controls to always know whether they're adequately deployed and operating effectively."**
>
> **Rob Hyde, CISO**

Leveraging the campaign tool, Schroders security team has been able to take remedial action and track progress. Through dynamic dashboards cross functional teams worked against a single source of shared insight, and also tracked and reported on remedial progress.

For example:

- With the new ability to drill down into the data and gain insight, Schroders discovered that a device build was introducing new vulnerability detections into the environment. This visibility has allowed the team to further reduce any potential security risk.

- Devices with 'End of Life' software were identified and tracked through the Campaign feature, allowing infrastructure and security teams to collaborate on updating the software.

Outcomes

Panaseer delivers real actionable intelligence that enables measurably improved security and reduction in risk posture by reducing the number and severity of device vulnerabilities whilst decreasing the likelihood of an attack exploiting those vulnerabilities.

Recent instances include:

- Ability to identify areas of greatest risk: Providing the continuous identification of areas of concern.

- Ability to focus on areas of greatest return: Identifying the areas with the greatest potential improvement and the associated risk allowed Schroders to focus and prioritise.

As Panaseer automatically pulls and analyses data, it can ingest and update vulnerability and anti-malware data more frequently. It has empowered Schroders' Security team to get automated insight into potential vulnerabilities and remediation activities.

Together Schroders and Panaseer also agreed on metrics to summarize the effectiveness of vulnerability remediation actions in order to report to senior stakeholders, such as the Global Technology Risk Committee.

Previously this monthly report had been completed manually. The report is now automated, and demonstrates impact, progress and next step actions to improve security posture. Recent examples of this include the deployment and rollout of new critical endpoint protection software and focused patching efforts to upgrade certain software.

Also, by increasing the consistency of information, they can ensure that all users and stakeholders reference the same underlying trusted data.

This ability to work from an agreed single source of trusted data has improved team performance and cross functional engagement.

The future

Both Security and IT teams at Schroders are invested in continuing to evolve the depth of insight provided by Panaseer and are currently expanding out the use cases to also include Patch Management Analytics, Application Security, Access Management and other data-driven insights.

If you would like to know more about the benefits of Continuous Controls Monitoring, drop us a line at: **contact@panaseer.com**

We've got you covered

Continuous Controls Monitoring for enterprise security

Panaseer UK

CargoWorks
Unit 101
1-2 Hatfields
SE1 9PG
London, UK

Panaseer US

WeWork
315 W 36th Street
6th Floor
NY 10018
New York, USA

contact@panaseer.com