


A photograph of a lighthouse on a rocky island at sunset. The sky is a mix of purple, blue, and orange. The lighthouse is illuminated from within, casting a warm glow. The sea is calm, reflecting the light from the lighthouse.

AMPEG Security Level Management

Keep the attack surface small 

 Schott AG

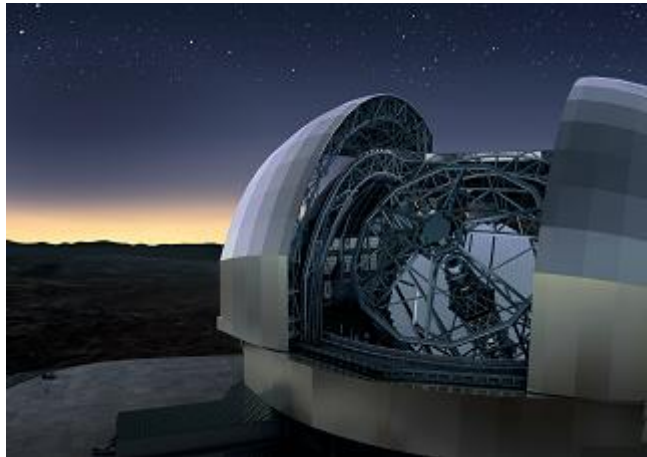
Security through
transparency - for a
universe of glass

A Security Lighthouse Case Study

▶ Security through transparency - for a universe of glass

As an innovator of specialty glass with manufacturing and distribution on almost every continent, SCHOTT AG places both comprehensive and complex demands on IT security. AMPEG Security Lighthouse watches over the international office IT systems of this long-established company and global corporation like an eye of Argus. With its comprehensive analyses, the monitoring system supports the company's requirement for maximum transparency.

CERAN® cooking surfaces are a byword worldwide. A lesser known fact is that this revolutionary glass-ceramic was developed by SCHOTT as early as 1971. SCHOTT also stands for outstanding pioneering achievements in numerous other fields. When Neil Armstrong became the first person to walk on the moon in 1969, his legendary footprint was recorded with lenses made of optical glass from SCHOTT. Even today, people are reaching for the stars with materials from the company: The largest and most modern telescopes in the world rely on ZERODUR® glass-ceramics to explore the mystery of dark matter or to detect evidence of extra-terrestrial life.



*Four of the five mirrors of the Extremely Large Telescope are made from ZERODUR® Glass Ceramics by SCHOTT.
Source: SCHOTT*

More than 130 years after the company was founded, SCHOTT represents a portfolio that covers nearly all spheres of life. The "Hidden Champion" is a global innovation partner for the domestic appliance industry, pharmaceuticals, electronics, optics, life sciences, automotive and aviation. In the 2017/18 financial year, sales of more than 2 billion euros worldwide were booked, of which 86% were from outside of Germany. Its manufacturing and distribution sites in 34 countries employ around 15,500 people. The parent company's headquarters are in Mainz and it is wholly owned by the Carl Zeiss Foundation.

Protecting the "Crown Jewels" is not everything

Such a high-tech company has numerous patents and a tremendous amount of specialised knowledge that must be guarded in all circumstances. Protecting this treasure was also the first step in expanding IT security at SCHOTT. "When I started at SCHOTT, our focus was basically: How do we protect our crown jewels?" explains Dirk Ossenbrueggen, Head of Information Governance and Security at SCHOTT. "The whole big rest went down a bit in IT operations. But then the awareness has grown that there are other things to protect besides the crown jewels and that you need to spend some money to do so. Above all, we had too little transparency at that time. We didn't have a deeper insight into our network, didn't know what we were up against, or what the security level was at all. To solve this

▶ Security through transparency - for a universe of glass

problem, I was searching for tools that would give me a quick overview of the security level of our IT."

After Dirk Ossenbrueggen had initially come across another tool, further research led him to AMPEG's Security Lighthouse. After comparing both tools with SCHOTT's specific requirements, the decision was made to use Security Lighthouse. Dirk Ossenbrueggen and his team were guided by the following requirements: "We wanted to know what we're doing in the way of update management, How up-to-date are our Patches? In addition, there was also the question of endpoint protection, i.e. antivirus protection. Which systems are covered and how current are the signatures? The third area was hard drive encryption. We felt that AMPEG could give us the necessary insights into each of these issues with Security Lighthouse. As well as the collectors for the target systems already mentioned, we also had an eye on those for the Active Directory, and that was also the initial setup we started with."



SCHOTT relies on augmented reality applications and offers special optical glasses for the corresponding spectacles.

Source: SCHOTT

Rollout in just 10 days

The Proof of Concept (PoC) quickly confirmed that AMPEG was able to provide the collectors required by SCHOTT for patch management, virus protection, encryption and software inventory as interfaces "out of the box". "The collectors tested in the PoC fulfilled their function as desired, such that SCHOTT commissioned the installation of our Security Lighthouse system immediately after the test phase," emphasises Michael Hänsel, Project Manager at AMPEG. "Our system currently monitors all clients and servers in the SCHOTT AG global office network and maps the security status on a world map almost in real time. The installation was very quick. All in all, including the PoC and the basic training of the staff, the rollout of the full monitoring system took only ten days. A really quick process, given the size and scope of the project."

The ability to discuss possible solutions openly has proven to be effective. "AMPEG has proven to be a flexible partner, open to innovation and improvement. If we, as a customer, have an idea and say that we can imagine this or that as a new feature, then that will be picked up. This gives us the opportunity to help shape certain details of the product itself and the project roadmap," summarises Dirk Ossenbrueggen.

▶ Security through transparency - for a universe of glass

Valuable findings

The findings that SCHOTT was able to draw from the data detected by Security Lighthouse were significant. "The control system clearly showed us where we stand," emphasises Ossenbrueggen. "In a way, the data was sobering because we had thought that we were further ahead with our IT security. But that was not the case. However, and that was the positive thing about it, we now knew what deficits we had. We have seen this very clearly, for example, in our IP address management. It was quickly discovered that our data quality was still in need of much improvement in some places. This is indeed a major advantage of the tool: It makes it unmistakably clear which construction sites need to be worked on."

The group of people actively using Security Lighthouse at SCHOTT has meanwhile expanded considerably: "Until recently, the tool from AMPEG was used exclusively by our five-member security team," said Ossenbrueggen. "We had collected the monitoring data and then instructed the respective IT managers accordingly. In the meantime, we have moved on to the fact that the IT managers in the locations themselves are actively working with the tool. The Security Lighthouse serves exactly that purpose. On the one hand, employees are trained in the use of the system, and on the other hand, the system is so comfortably constructed and user-friendly per se, that the employees can handle it on their own. It's also a bit motivational when people realise, 'hey look, I can actively help increase IT security and thus improve the situation'. In addition, we hope to arouse an element of competitive ambition in terms of IT security, accordingly to the motto: Why is the other location green and mine not?"

Wanted transparency

Security Lighthouse is designed for maximum transparency. At SCHOTT, it maps the security status throughout the global office network, down to the individual locations via the Security Information Map. The system uses a traffic light circuit with the usual red, amber and green colours. Even the smallest deficiencies and weak points are systematically revealed and visualised by the monitoring system. The IT department lays the cards out on the table for the management of the company. For Dirk Ossenbrueggen as Head of Information Governance and Security, this "ruthless" transparency is absolutely desired and part of the company's growth culture. What's more: it is the core element of the system for him. "If I don't have that transparency and do not



*At SCHOTT, Security Lighthouse maps the security status down to the individual locations via the Security Information Map.
Source: AMPEG*

▶ Security through transparency - for a universe of glass

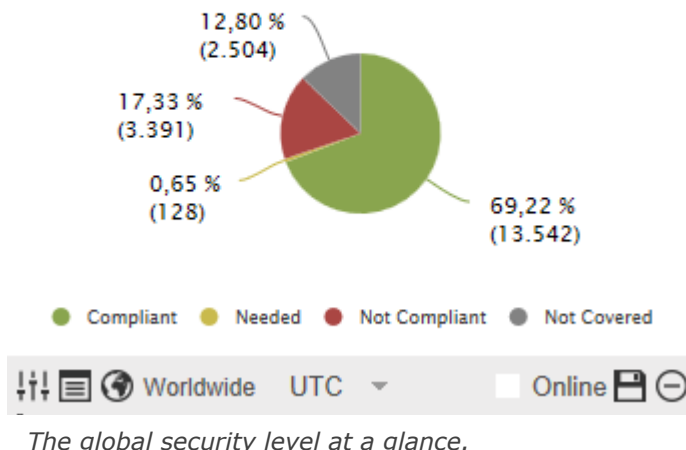
want it either, then I have a mentality to want to sweep everything under the carpet. And when things do come up, I would have to ask myself why I didn't know about it. My way is the way of transparency. The system shows me the areas needing improvement and I can work on the concrete plans. Even if resolving an issue takes some time - it is crucial that we are aware of the issue. This is a thousand times better than being surprised by something and being told by other people: 'watch out, you don't have your business under control'. So it's better to be proactive and use the transparency of the system constructively. Anything else would be a pseudo-solution in my eyes."

OT Security as a future issue

Following the collectors installed during the start-up phase, additional collectors were commissioned in the further course of the cooperation, including a CMDB collector (Configuration Management Database) to collect information about all systems known in the service management. At SCHOTT, the experience in the global office network leads to the consideration of extending the monitoring with Security Lighthouse to the company's Operational Technology (OT).

"At the moment we only have Security Lighthouse in the office IT. However, we already see a part of the manufacturing IT, namely where, for example, an endpoint protection solution is in place that is in fact behind the firewall, but is just on the phone with the head office. And then we also see systems that are not actually in the office network, but instead behind them," explains Dirk Ossenbrueggen. "Our thinking is to include the production potentially more in-depth in the monitoring. But we have to see how practicable it is in this sector. It will not be possibly to want to prescribe the same rules to the systems in production as those in the office network. Because when I say to production, 'you have to patch your machines every four weeks', of course that means machine downtime, which is by nature simply not feasible. One solution for the Security Lighthouse could be that you can differentiate between the assets, whether it is IT or OT. Then I would have two categories that could be treated differently. It could go in such a direction in the future."

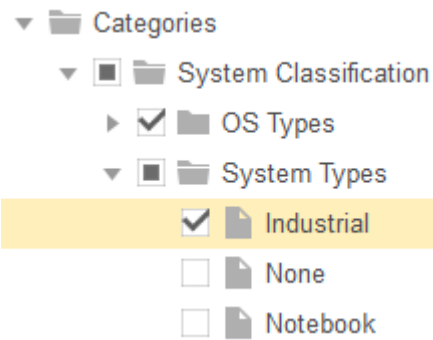
Updates Compliance Overview with need...



The global security level at a glance.
Source: AMPEG

▶ Security through transparency - for a universe of glass

At this point it remains to be added that AMPEG is now developing and providing special collectors for the OT sector. In this respect, the vision for the future outlined here by SCHOTT, of integrating the OT sector into monitoring in addition to IT, could well become a reality.



*Categorisation for analysing manufacturing systems.
Source: AMPEG*

This solution was implemented at:

Schott AG
Hattenbergstraße 10
55122 Mainz, Germany
<https://www.schott.com>

With support from:

AMPEG GmbH
Stavendamm 22
28195 Bremen, Germany
<https://www.ampeg.de/>