baseVISION

Augment internal resources with baseVISION's Managed Extended Detection and Response service

Case Study MCH Group

Who is MCH Group?

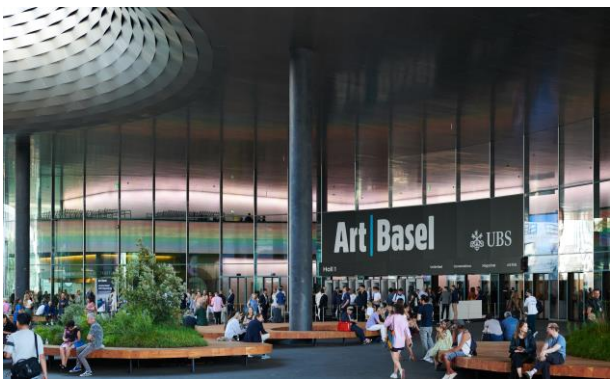
MCH Group, with its head office in Basel, Switzerland, is an internationally active experience marketing company with a comprehensive service network. It organises around 30 community platforms in Switzerland and abroad, including Art Basel, Swissbau, and Giardina. The Live Marketing Solutions division, with the brands MCH Global, MC2 and Expomobilia, offers comprehensive experiential marketing solutions ranging from strategy and creation to implementation. MCH Group also operates the Messe and Congress Center Basel and Messe Zurich.

The Vision

- 24/7 Security Monitoring
- Enhancing Detection Coverage
- Benefit from focused Security Expertise

Initial situation

MCH Group conducted a plan to enhance its internal security incident monitoring, detection and respond capabilities. This involved the integration of a professional Security Operation Center that will provide external support around the clock, ensuring a robust and responsive security infrastructure. There was also a need to expand security coverage to include additional cloud and on-premises resources. These issues highlighted the importance of addressing resource constraints and enhancing security measures to meet evolving threats.



«As we have to constantly develop and improve the IT security of MCH Group, we were faced with the need to monitor our infrastructure in the cloud and on-premises 24/7 and to be able to react quickly to incidents. The very high professionalism and expertise of baseVISION, as well as our requirement to stay on the Microsoft product line, convinced us to select baseVISION..»

Rachid Dahjaoui
Head of Information Security – MCH Group AG

About baseVISION AG

baseVISION is ISO27001 certified and is member of the Microsoft Intelligent Security Association.

ISO/IEC 27001:2013
BUREAU VERITAS Certification
UKAS MANAGEMENT SYSTEMS 0008

Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Simple baseVISION MXDR Premium Onboarding process

baseVISION leverages a simple onboarding process to start Security Operations services within weeks.

1. Preparation
The initial step in SOC onboarding involves thorough preparation. It encompasses resource allocation and planning for the upcoming security operations. A crucial part of this phase is the kick-off meeting, where roles, expectations, and timelines are discussed and clarified. The customer questionnaire is utilized to collect vital information about the organization's specific security requirements. Additionally, a review of prerequisites ensures that the client's environment is ready for the onboarding process.

2. Onboarding
During the onboarding phase, the focus shifts to technical aspects. Coordination of technical setup requirements takes place between the SOC team and the client. The technical onboarding implementation involves the deployment of security tools and configurations tailored to protect the client's environment effectively.

3. Communication
Effective communication is fundamental for a successful partnership. This phase is dedicated to aligning secure communication channels and reporting requirements. Regular status reports are generated to keep both parties informed about the progress of the onboarding process. Furthermore, this stage includes discussions and alignment regarding any optimization opportunities identified.

4. Optimization
Optimization efforts are aimed at fine-tuning security operations for efficiency. The focus here is on addressing known false positives and negatives. Validated optimization and automation activities are implemented to enhance threat detection and response capabilities. Specific response activities are set up in accordance with the client's preferences and approved optimization actions.

5. Start Operation
Transitioning into the SOC live operation phase, security services officially commence, and Service Level Agreements (SLAs) become effective. Regular SOC reporting and security incident review meetings are scheduled to ensure transparency and alignment between both parties. Continuous improvement activities are initiated to adapt to evolving threats and challenges, ensuring ongoing security effectiveness.

These five steps collectively form a structured SOC onboarding process and helped to bolstering the security posture of MCH Group.

«We are convinced of the solution! The cooperation with baseVISION was smooth and exceeded our expectations. We were particularly impressed by the outstanding quality and the high level of commitment during the onboarding process and during ongoing operations. The cooperation with baseVISION was undoubtedly beneficial for us.»

Christian Boos
Head Corporate IT – MCH Group AG

Efficient 24/7 Protection

24/7 operations is mandatory as attacks take place at any time and a timely response is required in most cases. Our MXDR Premium service has taken this burden from the MCH Group security team and continuously monitor their environment. The baseVISION team can analyze, process and close up to 99% of the incidents on their own without customer interaction.

«The open-minded and transparent communication during onboarding facilitated efficient collaboration, leading to an increase in security incident visibility. Witnessing the strong commitment of all experts is inspiring, as they continually strive to improve detection, protection, and response to both current and new threats.»

Jürg Meier
Lead SOC at baseVISION AG

One objective of MCH Group was to enhance detection coverage by leveraging the comprehensive capabilities of the Microsoft 365 Defender Platform, with the added flexibility of expanding data sources in the future. The baseVISION MXDR Premium package also provides access to the baseVISION Detection repository, incorporating over 100 additional detections into customers' environments. This repository is maintained by baseVISION Security experts and continuously expanded to detect current threats.

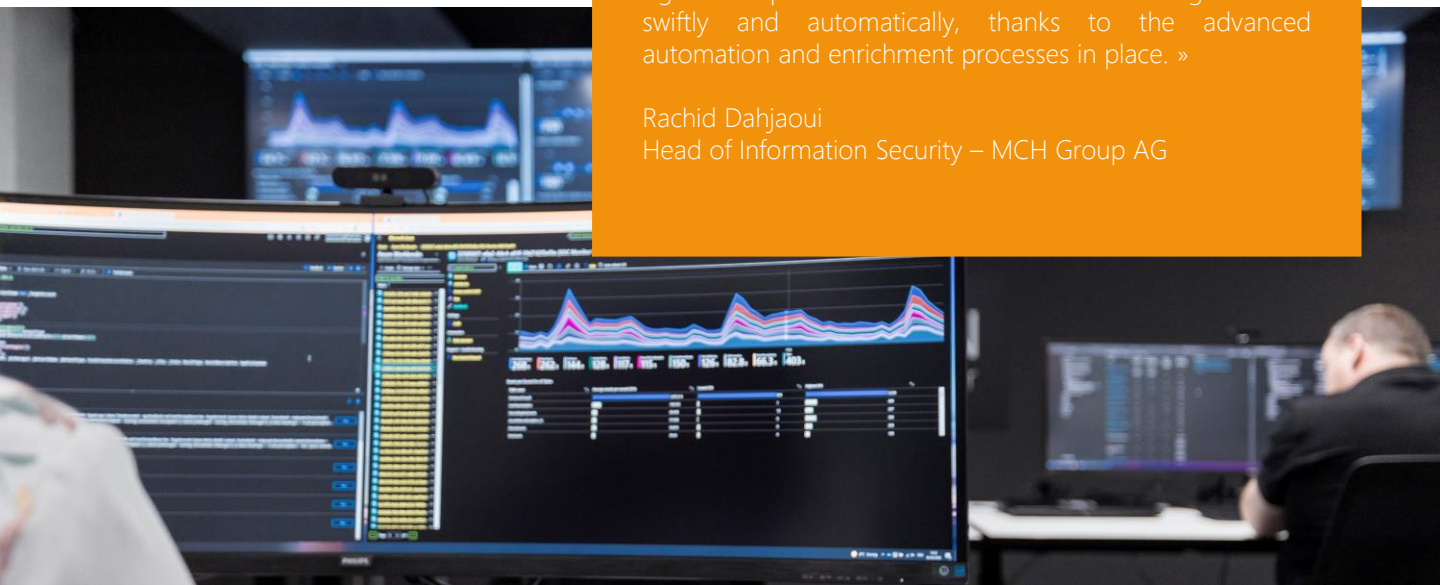
Besides extending detection capabilities, it is important to continuously tune and automate Security Operation tasks. This is fully included in the baseVISION offering, and we continually review security incident automation to increase processing efficiency through automation and enrichment. With that, more than 60% of the detected incidents are handled automatically within minutes.

Most beneficial Microsoft technologies used

- ✓ Microsoft 365 Defender
- ✓ Microsoft Entra ID Protection
- ✓ Microsoft Sentinel

«We are immensely satisfied with the efficient onboarding process provided by baseVISION AG. The integration has significantly lifted the burden off our shoulders, allowing us to focus on other activities with the assurance that our detection capabilities are robust, and our security operations are being continuously optimized. The professional and fast approach of basevision has notably enhanced our ability to counter current threats, making us feel well-supported and secure. It's a relief to know that a significant portion of incidents are now being handled swiftly and automatically, thanks to the advanced automation and enrichment processes in place. »

Rachid Dahjaoui
Head of Information Security – MCH Group AG



Summary

The SOC Onboarding process for MCH Group was driven by their objectives of achieving 24/7 Security Monitoring, enhancing Detection Coverage, and benefiting from specialized Security Expertise. These goals were successfully met through the implementation of the "baseVISION MXDR Premium" managed service, ensuring round-the-clock security monitoring. Detection coverage was significantly improved by introducing additional signals to Microsoft Sentinel and deploying detections from the baseVISION Detection repository. Moreover, MCH Group now benefits from the expertise of baseVISION's security professionals who actively analyze incidents, reducing the need for customer interaction and enhancing overall security effectiveness.

baseVISION AG
Unterführungsstrasse 25
4600 Olten

info@basevision.ch

+41 62 291 30 00

Contact us

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT

We make your IT workplace ready for the future – modern, flexible and secure.

We are able to combine expert knowledge with practical experience due to our focused company strategy. You can rely on our expertise as consultants, integrators and coaches on your way to modern IT workplaces and the simple and secure operation of your end devices. Our young company is proud that we already won four times the Microsoft Partner of the Year Award for our innovative and successful projects.