Industry: Telecommunications
Founded: 1998
Headquarters: Bern, Switzerland
Website: Swisscom.ch

CASE STUDY

Swisscom AG

Swisscom Frees Up Limited Resources by Embedding Better Data

Every security team knows that resources are finite, and there aren't enough hours in the day to manage and mitigate every risk that arises within an organization. This is especially true for a large, complex organization like Swisscom.

The telecommunications giant is the dominant service provider in Switzerland, where they develop and maintain the wireless and wireline network infrastructure, and boast a market share of 53% for broadband internet, 59% for mobile and 36% for digital TV. Along with its subsidiaries, Swisscom is also active in the banking, energy, entertainment, advertising and healthcare sectors, and is a growing provider of digitization and IT services.

That is the operational challenge faced by Stéphane Grundschober, Vulnerability Manager at Swisscom. He is a member of the group security team, with responsibilities including securing the organization by monitoring the workplace, identifying APT, lateral movement, reacting to new threats, as well as defining security governance and ensuring security requirements are applied consistently throughout the organization. To achieve this, Stéphane knew that each operational team within the organization would need to be self-sufficient in securing their own processes and technologies, under his coordination.

> "Just knowing we have VulnDB inspires confidence. This is a great feed. The quality is great. When you are exposed to this information you know that this is quality information. You can just see it"

Stéphane Grundschober
Vulnerability Manager at Swisscom

Limited Access to Limited Data

Stéphane knew that inadequate data, and inadequate access to that data, were preventing him from attaining his goal. For example, security teams within Swisscom were spending much of their time performing CVSS rating assessments instead of focusing their limited resources on managing and remediating the actual risk.

Security teams would be flooded with vulnerability notifications in major applications like Windows, or when vulnerabilities like SPECTRE/Meltdown were disclosed, but the disclosure information lacked the level of detail they needed to effectively help prioritize remediation. Many hours were lost searching for actionable details. The CVSS rating process proved to be a major friction point for the entire security framework. Teams had different interpretations of the CVSS scoring specifications, and a lot of time was consumed managing the overall process. A change needed to be made.

CVE is Not Enough

CVE fails to report over 93,000 confirmed vulnerabilities.

The vulnerabilities CVE does report are often late and limited in detail.

> “We knew we had a gap, we were investing a lot of time. We wanted to devote our scarce resources in actually doing something instead of just rating CVSS scores for vulnerabilities.

Introducing Better Data

Stéphane’s solution was to implement the comprehensive, timely and actionable data from VulnDB. With the powerful features of VulnDB, his team is now able to perform a centralized governance role, monitoring vulnerabilities impacting the whole organization and distributing prioritized information to the right people.

Using VulnDB’s search features, Stéphane’s team is able to filter for remotely exploitable vulnerabilities with high confidence. He gets real-time alerts for new vulnerabilities impacting the many software assets used within Swisscom, straight to his inbox. And once relevant vulnerabilities are identified, he can disseminate the right information to the appropriate teams so that they have the details they need to mitigate them effectively.

Comprehensive, Consistent Analysis

Stéphane’s team also benefits from data that is classified consistently and accurately, eliminating the need for his own team to perform CVSS ratings. Additional analysis of advisories, performed by Flashpoint's research team, gives Swisscom access to critical, actionable intelligence and metadata that would not otherwise be available.

The VulnDB database contains detailed metadata within each applicable entry to ensure proper prioritization and remediation. As well as vendor disclosures, it includes actionable resources like relevant articles and blogs, hackers breaking down exploits and more to spare organizations time that would otherwise be spent on research. Where classifications for a product are not clear, RBS works with vendors directly for clarification.

Inspiring Confidence by Embedding Up-to-Date Data

Swisscom is able to operationalize VulnDB using the powerful API provided. By consuming the data every three hours, their teams are always armed with the most up-to-date information, and Stéphane is informed on the latest exploitable vulnerabilities that might affect the systems within his organization. As well as being able to effectively guide risk mitigation, he can keep his operational teams accountable and provide an acknowledgement and timeline to his internal and external customers.

According to Swisscom, using VulnDB inspires confidence. All of their teams, from CIRT to DevOps know they can trust the feed powering their security. Swisscom have been able to reduce friction and increase overall operational efficiency by integrating vulnerability intelligence from VulnDB into their risk management process.

> “
> A Swisscom colleague asked me, ‘Where do you get this stuff? It’s always great and interesting.’ He asked what websites and forums I was looking at to find this juicy information, and how I had time. I said, ‘No, no, no... it comes straight to my inbox every day.

VulnDB Drives Informed Decisions

- ✓ Includes vulnerabilities in COTS and 3rd Party Code, Vendor Risk Ratings, and more
- ✓ Provides timely vulnerability alerts without scanning
- ✓ Trusted by leading brands including Adobe and Northrup Grumman
- ✓ Integrates with leading tools and ticketing systems

Experience the Comprehensive Intelligence and Powerful Features of VulnDB for Yourself

https://flashpoint.io/ignite/vulnerability-intelligence/

About Flashpoint

Flashpoint is the leader in threat data and intelligence. We empower mission-critical businesses and governments worldwide to decisively confront complex security challenges, reduce risk, and improve operational resilience amid fast-evolving threats. Through the Flashpoint Ignite platform, we deliver unparalleled depth, breadth and speed of data from highly relevant sources, enriched by human insights. Our solutions span cyber threat intelligence, vulnerability intelligence, geopolitical risk, physical security, fraud and brand protection. The result: our customers safeguard critical assets, avoid financial loss, and protect lives.

Discover more at flashpoint.io

Get a Demo