# Genetec

## Advancing security awareness and adoption with the BSIMM

**Company overview**

Since 1997, Genetec Inc. has delivered innovative technologies across a broad solutions portfolio encompassing security, intelligence, and operations. Its flagship product, Genetec™ Security Center, is a physical security platform that unifies IP-based video surveillance, access control, automatic license plate recognition, communications, and analytics. Genetec also develops cloud-based solutions and services designed to improve physical security and contribute new levels of operational intelligence for governments, enterprises, and the communities in which we live.

To learn more about Genetec, click here.

## The challenge: Build a software security program rooted in a security-first culture

Tasked with building a software security program nearly from the ground up, Mathieu Chevalier, lead security architect at Genetec, understood one thing to be true: his efforts to bolster and grow his organization's security program would require a trusted and proven strategy. Mathieu noted that the "main drivers [of his methodology] were to use a quantitative approach to establish a plan for what to focus on and to benefit from the experience of others that had already done so."

At the start of his security initiative journey, Mathieu quickly identified Genetec as being "early in [its] software security initiative… with no software security team." Understanding that the promotion of and adherence to a software security program would require more than policies and practices, Mathieu set out to promote an environment and culture in which security was prioritized.

The critical problem Mathieu faced was not only developing the program, but also finding a way to reinforce his strategy with proven methods and approaches. Essentially, he needed a way to validate his strategic decisions. He also understood the need to foster trust and belief in his software security initiative.

## The solution: A BSIMM assessment

Genetec elected to have a BSIMM assessment performed to help identify areas of potential growth and gain a clear picture of its software security stance. The Building Security In Maturity Model (BSIMM) from Black Duck® offers security executives a model and framework to test, measure, and benchmark their current AppSec activities. Based on the security programs of 130 organizations in many verticals, including financial services, independent software vendors, healthcare, and consumer electronics, BSIMM data offers a unique perspective on the state of AppSec and provides insight into the key activities, practices, and tools executives should consider implementing in their own organization.

Genetec began work with the BSIMM in December 2016 and has conducted two assessments in the past five years.

Mathieu's decision to perform a BSIMM assessment on his organization's fledgling security program provided crucial third-party insights. Use of BSIMM data helped with his plan "to find low-hanging fruit, build momentum, and use this to drive changes." Though he had a gut feeling of what needed to be done, Mathieu used the data provided by the BSIMM to assess "where they were, work on improving the situation, and then measure again." After looking at the best way to quantitatively approach this effort, Mathieu found that BSIMM would fill that need.

Use of a trusted third party lent credibility and support to his efforts, provided key guidance, and also validated his decisions and the direction for the program.

*"BSIMM helped us assess our product security initiative and guide us to where we should go. It is a valuable tool for anyone building a product security program."*

—Mathieu Chevalier, Lead Security Architect

## The results: Cross-team support of security activities

Understanding that implementation of policies alone is rarely sufficient to support and maintain a software security program, Mathieu invited a key BSIMM founder, Gary McGraw, to an internal event to build momentum around application security. By integrating the security activities he learned from the BSIMM as a culture and mindset as part of his program, Mathieu was able to secure both support and investment.

Development teams started asking Mathieu to work with them to secure their applications, perform threat modeling, review their vulnerabilities, and establish a plan with them. The BSIMM served as a validation of Mathieu's efforts. Use of a trusted and data-driven model, paired with custom security practices, helped teams build trust and reliance in the program. Through the use of the BSIMM's data-backed model, he succeeded in getting teams engaged with improving their posture over time. He then used those successes to convince other teams to start their journey with him.

Genetec recently conducted a second assessment in the hopes of gaining insight into its improvements and areas that continue to present pain points. Genetec presented the results to executives and development teams. This helped support new initiatives being put in place this year by demonstrating the benefits to the security team as well as to the organization as a whole.

In this use case, the BSIMM both united teams and validated ideas. It is through this pairing of data and credibility that BSIMM lends its greatest value; Mathieu was able to leverage the tool as part of his program to help reinforce a security-first program with top-down support.

## About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.

©2024 Black Duck Software, Inc. All rights reserved. Black Duck is a trademark of Black Duck Software, Inc. in the United States and other countries. All other names mentioned herein are trademarks or registered trademarks of their respective owners. September 2024