Case Study

Bricata Protects Federal Data with SafeLogic's FIPS 140-2 Validated Encryption

The Background

Networks are the nervous systems of modern enterprises and government. Interactions with customers, constituents, employees, suppliers, contractors, and regulators all take place over the network. Items of value, such as digital currency, intellectual property, procurement data, and intelligence are stored on the network. Protected data — sensitive personally-identifiable information (S-PII), healthcare data (HIPAA), credit card (PCI), Europe's General Data Protection Regulation (GDPR) — must be secured on the network. The failure to do so can result in the inability to conduct business, legal fees and fines, a tarnished brand/reputation, and loss of public trust.

Bricata provides comprehensive network protection — simplified. It combines unparalleled network visibility, full-spectrum threat detection, true network threat hunting, and post-detection actions into a single, tightly-integrated system that is easy-to-deploy, easy-to-use, and easy-to-manage. Bricata prevents threats from infiltrating networks and moving laterally within them with a combination of signature, behavioral anomaly, hash, and zero-day artificial intelligence threat detection methods. It then gives you high-fidelity metadata and network-truth PCAPs with which to investigate and resolve them. Bricata protects networks so that business can proceed with confidence.

The Challenge

Bricata operates on the basis of network traffic. It stores network traffic (PCAPs), it generates metadata on network traffic (Zeek Logs), and it transmits network traffic (both) throughout its system. Bricata understood that the data it collects and outputs contains real value and sensitive information, and set out to protect it. The U.S. Federal government provides the reference standard for the cryptographic protection of data in the National Institute of Standards and Technology (NIST) publication FIPS 140-2. This standard articulates the specific encryption measures to be used, how to conduct operational testing, and even how it will be validated. In fact, Federal government departments are prohibited from deploying information technologies that store and transmit data without FIPS 140-2 certification.

Bricata set out to protect its customers' data and to ensure that its own system wasn't a point of vulnerability by incorporating FIPS 140-2 validated encryption into its system and achieving NIST certification.

SafeLogic's Tandem Solution

In Bricata's due diligence on FIPS 140-2, they identified ease of deployment and speed of validation as priorities. SafeLogic was perfectly positioned to fulfill both needs with CryptoComply software and the RapidCert service. The two are bundled together to achieve streamlined, accelerated results and in this case, the whole is truly greater than the sum of its parts!

Completed Ahead of Schedule

Once the validation process was underway, the RapidCert took less than two months. Bricata was counting on SafeLogic to beat the traditional timeline of 12+ months, but this was even faster than anticipated. The Cryptographic Module Validation Program (CMVP) issued FIPS 140-2 validation certificate #3325 on November 10, 2018.

The Solution

To speed the process, Bricata licensed SafeLogic's pre-validated encryption libraries, CryptoComply, and was able to integrate quickly into the Bricata product. This particular version of CryptoComply was selected for compatibility and ease of installation, and required very little developer time, as promised. It delivers reference-standard encryption, ensures compliance with FIPS 140-2 requirements, and therefore sped Bricata through the process. The FIPS 140-2 validation was granted after an independently accredited lab put the Bricata encryption module through a rigorous NIST-specified series of tests, also managed by SafeLogic.

"Offering FIPS 140-2 validated encryption is another major milestone for Bricata's comprehensive network security product, and we are deploying it significantly ahead of schedule thanks to our strategic partnership with SafeLogic," said Bricata CEO John Trauth. "Our advanced threat protection and threat hunting capabilities solve some of the most pressing challenges in network security and earning NIST certification helps provide assurance to our government customers that we are dedicated to meeting the standards they need in their environments."

Since SafeLogic's CryptoComply module had already been validated to meet the FIPS 140-2 standard, Bricata's cryptographic test report was expedited and sent to the Cryptographic Module Validation Program (CMVP), operated by the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) of Canada. Their joint office confirmed compliance and issued certificate #3325. From beginning to end, Bricata achieved FIPS 140-2 validated encryption within two months with a minimum of effort on its part, a far cry from the traditional 12+ months of stressful work and coordination.

The result is that Bricata is available for use by both commercial and Federal government customers, and both can rest assured that their data is protected to the highest standard of cryptographic data protection in the industry.

"We are deploying FIPS 140-2 validated encryption significantly ahead of schedule thanks to our strategic partnership with SafeLogic!"

John Trauth
CEO, Bricata

BRICATA

About Bricata

Bricata's comprehensive network protection provides unparalleled network visibility, full-spectrum threat detection, true threat hunting, and post-detection response capabilities in an intuitive, tightly-integrated and self-managing system. Automated detection, productive GUIs and workflows make it easy-to-use for novices; while granular control and rich network metadata and PCAPs for threat hunting give experts the power they demand. Bricata speeds incident resolution by up to eight times by quickly detecting threats and providing the context necessary to act.

Bricata was founded in 2014 and is headquartered in Columbia, MD.

SafeLogic

About SafeLogic

SafeLogic Inc. was established in 2012 to reduce the time and complexity of integrating and validating world class encryption. Spun out from Apex Assurance Group, which has provided FIPS 140 consulting services to top companies for nearly a decade, SafeLogic delivers innovative security, encryption, and FIPS validation to applications for mobile, wearable, server, appliance, and constrained device environments.

SafeLogic is privately held and is headquartered in Palo Alto, CA.

SafeLogic Inc.
530 Lytton Ave, Suite 200
Palo Alto, CA 94301
(844) 4-ENCRYPTION
@SafeLogic
info@SafeLogic.com
www.SafeLogic.com

You needed SafeLogic six months ago.