ONUG Collaborative Maps Fortinet FortiGate Log Messages to CSNF's Canonical Data Model for Cloud Security Notifications

Project team planning Cloud Security Notification Framework enhancements that will extend the power of CSNF to simplify multi-cloud security analytics.

BOSTON, MA, USA, May 2, 2024 /EINPresswire.com/ -- ONUG Collaborative Project Maps Fortinet FortiGate Log Messages into CSNF's Canonical Data Model for Cloud Security Notifications

Project team plans additional Cloud Security Notification Framework enhancements that will extend the power of CSNF to simplify multi-cloud security analytics.

ONUG, the leading advocate for the Global 2000 community of IT professionals, today announced that

ONUG The Voice of the Large Enterprise

the ONUG Collaborative Cloud Security Notification Framework (CSNF) project team has mapped Fortinet FortiGate VM next-generation firewall (NGFW) log messages into CSNF's canonical data model for cloud security notifications. This is the first in a series of planned enhancements that will extend the power of CSNF to reduce the complexity of multi-cloud security analytics by integrating many more log message mappings for widely deployed cloud security products and public cloud services.

"Fortinet reviewed the log messages output by its FortiGate NGFW and mapped all relevant message fields into the critical fields specified in CSNF's canonical data model," said Josh Hammer, CSNF Project Co-Leader and Field Chief Cloud Security Architect at Oracle. "CSNF's common model for security log messages frees SOC analysts from needing to understand the syntax and semantics of each message type, simplifying threat analytics and reducing the time-

to-resolution for security incidents."

"Fortinet is thrilled to be contributing to the Cloud Security Notifications Framework," said Vincent Hwang, Senior Director, Cloud Security at Fortinet. "This new standardized mapping of cloud security log messages from Fortinet's FortiGate NGFW has the potential to decrease confusion and increase SOC effectiveness, reducing a persistent barrier to cloud adoption. CSNF furthers Fortinet's effort to drive better customer outcomes through broad ecosystem support within the Fortinet Security Fabric."

"Cloud security notifications are a Tower of Babel of different languages and varying message formats which are often semantically equivalent but syntactically different from each other," said Richard Julian, CSNF Project Co-Leader and security consultant at ThatCloudGroup. The value of CSNF for SOC analysts increases as we incorporate as many log message mappings as possible from leading cloud services and security products, and we anticipate that the FortiGate integration is the first of many in 2024 and beyond.

About CSNF
For more information about the ONUG Collaborative CSNF Project:
https://onug.net/project-teams/csnf

For information about CSNF canonical data model message mappings:
https://github.com/onug/csnf/blob/main/mappings/README.md.

SOC analysts who are interested in gaining hands-on experience with CSNF and the opportunity to test their threat surveillance skills are welcome to register for the https://onug.net/capture-the-flag-spring-2024/ at ONUG Spring 2024.

About ONUG
ONUG is the only organization composed of senior-level IT executives from the Global 2000 that represent the interests and initiatives of the Enterprise Community. Through its global event series, working groups, training academies and webinars, ONUG plays a central role in the creation of new and improved tools to develop, manage and secure the digital enterprise. The ONUG Community is made up of IT leaders from Bank of America, RTX, Cigna, Citigroup, UBS/Credit Suisse, eBay, FedEx, Fidelity Investments, Gap Inc., GE, Intuit, JP Morgan Chase, Kaiser Permanente, Morgan Stanley, Pfizer, State Street Bank, TD Ameritrade, Oath, and hundreds more. For more on ONUG, go to onug.net or follow on Twitter @ONUG.

Register here for ONUG Spring 2024, hosted by FedEx, which will be held in Dallas, May 15-16, 2024.

William Sell
ONUG LLC
+1 508-596-6118

bill@onug.net
Visit us on social media:
Facebook
Twitter
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/708373223