Bricata Delivers Network Protection with Enhanced Customization Features

Users can Tailor their Experience with New Metadata Filters, Dashboard Customization and Smart Alerts Grouping

COLUMBIA, Md. (PRWEB) October 10, 2019 -- Bricata, Inc., a leading provider of comprehensive network protection, today released a new version of its network security platform with a range of customization and personalization options. The enhancements provide security teams with the flexibility to precisely control the network metadata they want to capture – from among hundreds of possible fields – to better match the needs of their unique environment. Just as importantly, the new version also provides options for analysts to design how they view the data, which allows them to personalize dashboards to meet their individual preferences.

“Our goal is to simplify network security and this round of enhancements to the Bricata platform is largely a result of implementing requests customers have made of us,” said Bricata CEO John Trauth. “This software release is about enabling security teams and analysts to work how they want to work and in turn, improving the efficacy of protecting, detecting and hunting threats.”

Bricata simplifies network protection with a combination of unparalleled network visibility through “smart” packet capture (SmartPCAP) and rich network metadata generation; full-spectrum threat detection that simultaneously applies deep packet inspection, behavioral anomaly, IOC matching, and AI-based binary conviction to network traffic; true threat hunting through an all-in-one, self-managing and workflow-driven investigation environment; and post-detection actions that enable security operations center (SOC) teams to take action on detected threats.

New enhancements in this release include:

- Network metadata filters. These new filters enable users to fine-tune the specific network logs (generated by Zeek) that are streamed to the Bricata Central Management Console (CMC) repository and to other third-party forensic repositories and SIEMs. This helps security teams use their resources more efficiently by removing nonessential data that consumes storage and repository space.

- Customizable CMC dashboards. Network visibility dashboards can be custom designed through a palate of drag-and-drop widgets. This permits users to create unique CMC dashboards that align exactly with their network situational awareness requirements.

- Smart alerts grouping. Alerts grouping consolidates similar or related alerts together. This reduces alert fatigue that sometimes results from a single threat that is detected in multiple ways and therefore triggers multiple alerts. Bricata enables grouping in three ways by a) geographic location, b) 3-tuple hash (client-server), and c) the 5-tuple Community ID hash. The Community ID is part of the open-source Zeek project that will ensure interoperability with other cybersecurity solutions that are also adopting this up-and-coming standard.

- Support for external sandbox file inspection. Sandboxing provides another level of file behavioral observation performed within external sandbox – over and above the file-based binary conviction that Bricata already provides. Bricata provides seamless bi-directional integration with external instances of the Cuckoo open source sandbox.
- SNMP support. SNMP allows IT operations to monitor the health of Bricata – along with the health of their other enterprise applications – through consolidated SNMP-based monitoring and management platforms.

- Upgrade scheduling. The scheduling feature permits systems administrators to schedule the date and time that a Bricata system update will be performed. This allows administrators to perform updates at a convenient time of their choosing to avoid disruption to the organization.

- Section 508 compliance assurance. With this software update, Bricata reviewed the product and product documentation to ensure its compliance with Section 508.

Since Bricata was founded in 2014, the company has set itself apart with a continuous focus on improving threat detection. This past year the company has been recognized by security technology research analysts for its innovation in intrusion detection and prevention systems (IDPS). In addition, Bricata has teamed up with a network tap solution provider to develop network flyaway kits for incident response and has strengthened its relationships with partners in digital forensics and incident response (DFIR).

Last year, Bricata was recognized as a business driving technology innovation in the Greater Washington metropolitan region when it was selected for the inaugural list of NVTC Tech 100 companies. In addition, the security trade publication CSO Online named Bricata to its list of best security software solutions based on an independent review of the product: Bricata adds threat hunting to traditional IPS/IDS.

About Bricata
Bricata is the leader in comprehensive network protection. The Bricata solution provides unparalleled network visibility, full-spectrum threat detection, true threat hunting, and post-detection capabilities in an intuitive, tightly integrated and self-managing system. Its automated detection, productive GUIs, and expert system workflows make it easy-to-use for novices; while granular control of its engines, access to rich network metadata and PCAPs, and true threat hunting capabilities give experts the power and control they demand. Bricata has been proven to speed incident resolution by eight times by reliably detecting threats and providing the context necessary to get to the truth quickly and act. For more information visit www.bricata.com.
Contact Information
Frank Strong
for Bricata
http://www.bricata.com
202-352-5920

Online Web 2.0 Version
You can read the online version of this press release here.