Qualys Indication of Compromise IOC 2.0 Now Provides Advanced Attack Detection, Investigation, and Response Capabilities

July 29, 2019

FOSTER CITY, Calif., July 29, 2019 /PRNewswire/ -- Qualys Inc. (NASDAQ: QLYS), a pioneer and leading provider of cloud-based security and compliance solutions, today announced a major update of its Indication of Compromise (IOC) solution, an integrated app delivered on the Qualys Cloud Platform.

"Qualys IOC now provides enhanced attack detection, investigation, and response for security analysts, incident responders, and managed security service providers. Leveraging the same Qualys Cloud Agent already deployed for an organization's asset inventory, vulnerability management, policy compliance, and patch management programs, Qualys consolidates functions and advanced capabilities to provide broad and deep security coverage," said Philippe Courtot, chairman and CEO, Qualys, Inc.

Qualys IOC 2.0 new detection, investigation, and response capabilities include:

- **Behavior-based Scoring Engine to Prioritize Response**
  Security analysts often waste valuable time chasing false alarms, ghost alerts, and non-impactful malware infections with solutions that have a single scoring dimension. Qualys IOC's new incident scoring engine factors in additional behavior attributes including file analysis, process state, and network connections to prioritize responses based on how the attack is behaving in the network. This enables security analysts to respond to the most critical attacks first.
- **Enhanced Attack Detection Using Comprehensive File Reputation Threat Feed**
  Qualys IOC extends the detection of malicious, suspicious, and fileless attacks that are often missed by anti-virus agents through the native integration of a leading file reputation threat feed provider. This enhances attack detection while eliminating the cost and complexity required by other solutions to correlate events in external SIEMs that cannot scale to handle the event volume associated with modern attacks.
- **Real-Time and Historical Views of Attack Patterns Speed Investigation and Response**
  Powered by Qualys' highly scalable Elasticsearch clusters, IOC now stores raw event telemetry and post-processed attack indicators across multiple dimensions: time-series and current state indexes. This enables security analysts to quickly answer and respond to the two most important questions to speed investigation and response: "Is the attack still live in my network?" and "At what point in the past did it happen?"
- **Real-Time Response Platform for Alerting and Actions**
  Analysts can create alerts and notifications, delivered by a new response platform microservice, to push the critical insights they need to investigate and remediate incidents as soon as they occur. Alerts are easy to manage using the same Qualys Query Language (QQL) already used by security analysts for two-second search for threat hunting, investigations, and dashboard widgets. Initial responses include email alerting, integration with ticketing systems, posting to Slack channels, and creating PagerDuty incidents. Additional responses will be released throughout the year.
- **API and Ecosystem Integration**
  Qualys IOC public API enables integration with third-party SIEM, threat intelligence platforms, incident handling/response systems, security orchestration and automated response platforms, and IT Ticketing systems to automate rapid sharing of threat information with security and IT operational platforms. Support for the Qualys Technology Add-on (TA) for Splunk will be available in September.

Availability and Pricing
Qualys' IOC Cloud App is immediately available. Pricing is based on the number Qualys Cloud Agent assets installed; annual subscriptions start at $2,995. To learn more, visit www.qualys.com/IOC or watch the video.

About Qualys
Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 12,200 customers and active users in more than 130 countries, including a majority of each of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and consolidate their security and compliance solutions in a single platform and build security into digital transformation initiatives for greater agility, better business outcomes, and substantial cost savings.

The Qualys Cloud Platform and its integrated cloud apps deliver businesses critical security intelligence continuously, enabling them to automate the full spectrum of auditing, compliance, and protection for IT systems and web applications on-premises, on endpoints and elastic clouds. Founded in 1999 as one of the first SaaS security companies, Qualys has established strategic partnerships with leading cloud providers like Amazon Web Services, Microsoft Azure and the Google Cloud Platform, and managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, DXC Technology, Fujitsu, HCL Technologies, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance. For more information, please visit www.qualys.com.

Media Contacts:
Tami Casey
Qualys
(650) 801-6196
tcasey@qualys.com

Mariah Gauthier
Highwire PR
(415) 963-4174
qualys@highwirepr.com

View original content:http://www.prnewswire.com/news-releases/qualys-indication-of-compromise-ioc-2-0-now-provides-advanced-attack-detection-investigation-and-response-capabilities-300892083.html

SOURCE Qualys, Inc.