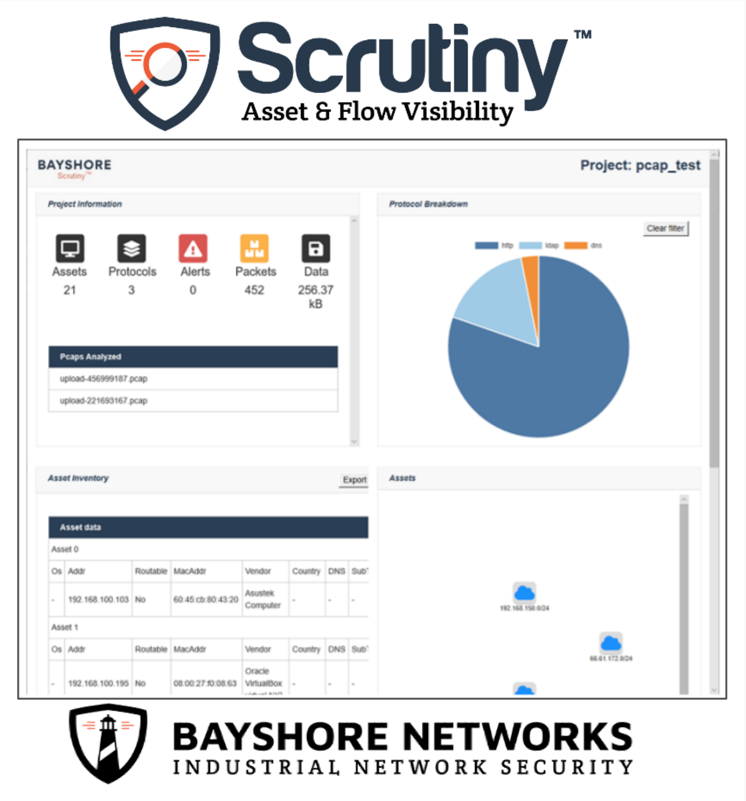
EIN PRESSWIRE

Bayshore Networks Announces Scrutiny™: Free Tool for Identifying Cyber Risks to Plant Networks

New Bayshore tool provides security visibility into OT networks, ICS assets and communications

DURHAM, NORTH CAROLINA, USA, May 12, 2020 /EINPresswire.com/ -- Bayshore Networks, a leading provider of industrial cybersecurity protection, policy, and enforcement today announced the release of Scrutiny™ – a new free tool for operational technology (OT) and IT teams to see and understand the assets and flow of communications in industrial networks.

Many industrial organizations don't have the staff skills or resources required to manage comprehensive visibility products, but they still need to know what is going on with their plant networks and assets to identify cyber risks and that could disrupt production. Plant personnel and IT teams need an easy-to-use tool that can give them a first snapshot of what is going on in their plant networks. There may be unexpected assets, external IPs in play, and systems that should not be talking to other specific systems. Any of these circumstances could be indicators of cyber risk gaps that could potentially impact production if not caught early and appropriate action taken.



Pcaps Analyzed
upload-456999187.pcap
upload-221693167.pcap

Asset data

Asset 0

Os	Addr	Routable	MacAddr	Vendor	Country	DNS	Sub
-	192.168.100.103	No	60:45:cb:80:43:20	Asustek Computer	-	-	-

Asset 1

Os	Addr	Routable	MacAddr	Vendor	Country	DNS	Sub
-	192.168.100.195	No	08:00:27:f0:08:63	Oracle VirtualBox	-	-	-

Scrutiny provides an HTML report after analyzing industrial traffic. If desired, users can export to a spreadsheet and create trending and tracking for their networks and assets.

Scrutiny is a free asset and communications flow detection tool from Bayshore that can run as a Windows application on a desktop or laptop. The software is built for industrial settings and understands OT assets and protocol communications activity. Scrutiny can work from a live packet capture (PCAP), or with offline PCAP files. With even a few minutes of traffic, Scrutiny delivers a basic security report of assets, protocol activity, and network communication flows – essentially what's there, what's it talking to, and how - all of which can be beneficial to determining safety, security and production risks.

"Scrutiny is like a camera, it's basically a snapshot of the traffic. Many small and mid-sized asset owners find they cannot afford high-cost, comprehensive visibility tools which perform more like video by providing a continuous readout of network activity," said Toby Weir-Jones, Chief Product Officer for Bayshore Networks. "Scrutiny provides OT and IT teams with a practical solution that can identify OT equipment IP addresses, operating systems, MAC addresses and vendors, country, public Domain Name Service (DNS), OT protocols, and communications topologies. This information can be very valuable as building blocks when beginning the process of identifying risks that could affect safety and security of production.”

Common Scrutiny findings include:
•Identifying Outside IP Addresses – Catching communications from plant assets flowing to routable external IP addresses. When such addresses are detected, Scrutiny performs an IP Reputation security check to confirm no known botnet or other malware sites are active on the customer network.
•Indications of Policy Violation – Pinpoint communications that indicate security risks due to weak or missing policies, or overly permissive access which can be corrected once identified.
•Asset Discovery – Industrial Control Systems (ICS) and other plant assets can be detected through information contained in OT protocols and communication patterns.
•Communication Flow Analysis – Identifying two systems that shouldn’t be communicating together, or unauthorized protocols in use can sometimes put assets or processes at risk.

For a list of supported protocols see www.bayshorenetworks/scrutiny for the datasheet and details on how to get started, or email us at info@bayshorenetworks.com.

About Bayshore Networks
Bayshore Networks was founded in 2012 and is a leading provider of patented and award-winning industrial cybersecurity protection, policy and enforcement specifically designed for OT environments, automation engineers, and plant operators. The company created SCADAfuse®, SCADAwall™ and OTaccess™ to address the digital and physical security risks which can compromise the safety and availability of OT environments. Bayshore actively and securely protects ICS systems, SCADA, industrial applications, networks, machines, and workers from cyber threats.

Bayshore Networks is backed by ForgePoint Capital and Benhamou Global Ventures and Bayshore technology is in use by many world-leading industrial automation operators, including GE, Kimberly Clark, AT&T, Yokogawa and water districts and wastewater treatment sites around the globe. For more information, email us at contact@bayshorenetworks.com or visit us at www.bayshorenetworks.com.

Jannica Morton
Mind Shift Agency
+1 817-372-2250
email us here
Visit us on social media:
LinkedIn

This press release can be viewed online at: http://www.einpresswire.com

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.
© 1995-2020 IPD Group, Inc. All Right Reserved.