PACKETVIPER®

PRODUCT BRIEF

OT360™

OT Security and visibility without unplanned downtime

The Challenge

Critical operational technology (OT) and industrial control systems (ICS) are being exposed to new and evolving cybersecurity threats. As information technology (IT) converges with OT we see air gaps disappearing and attack vectors increasing. Increased vulnerabilities resulting from these interconnected systems require a new approach.
Simply extending legacy IT security solutions and practices into OT environments will not result in better OT security.

The Solution – PacketViper OT360™

OT360 supports unique OT security needs while reducing the risk of unplanned downtime. OT360 is an adaptive network security solution that passively monitors the OT network without scanning and offers capabilities to respond to threats without complex orchestrations.

The solution improves asset and communications visibility while gathering intelligence on network threats performing reconnaissance and moving laterally. Threats are detected without false positives and security teams have the option to respond at wire speeds, both within a segment or across an enterprise.

How it works

- PacketViper and the customer populate the network with lightweight, sensors and highly believable decoys.
- Threats performing reconnaissance scans, moving laterally on the network and seeking unauthorized access are identified when they interact with the OT360 deception artifacts.
- Once detected, an alert is sent to the security team with threat context.
- If security teams choose to do so, OT360 policies can initiate threat response without complex orchestrations. Response options include alerting, quarantining and slowing the activity or outright blocking/preventing the threatening act.

Features and Benefits

Lightweight.

Agentless sensors and decoys are easily configured and blend into the fabric of network segments without any destabilizing influence.

Passive and active capabilities.

Older ICS and OT systems might stop working when unexpectedly scanned. With OT360 passive observation of traffic can actively identify assets and threats on the network.

Vendor risk management.

Third-party vendors may connect to ICS and OT systems for diagnostics and maintenance. OT360 can detect and prevent anomalous vendor behavior on the network.

Mirror mode and in-line capabilities.

Once operational and security professionals gain trust with the solution, OT360 can evolve from a passive, detection-only configuration to active prevention mode.

Automated adaptive responses.

When operating in-line, the solution provides graduated response capabilities. These include alerting, throttling communications speed, and active blocking of unwanted and potentially malicious activity.

Aligned IT and OT.

Eventual attacks on the OT network frequently start on the connected IT network. PacketViper's OT360 and Deception360 can work across both the OT and IT infrastructure environments.

Supports compliance.

OT 360 is well aligned with FERC/NERC CIP controls, specifically satisfying several CIP-007 (Systems Security Management) requirements and enabling several measures to be met.

About PacketViper

PacketViper is a cybersecurity deception technology company featuring a lightweight deception that produces heavyweight, practical results including dynamic network defense, relief of security related operational costs and burdens, and 3rd party risk monitoring with real-time policy enforcement.

Contact Us Today

Call: 855-758-4737

Email: info@packetviper.com