PACKETVIPER®

PRODUCT BRIEF

OT360™

Enhanced OT /ICS cybersecurity 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 and ICS 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 that are either performing reconnaissance and moving laterally, or simply lurking and listening.

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

OT360 has two primary deception features: decoys and OT Sirens™ and they each serve two different purposes.

OT Sirens are intended to lure threats passively listening to a network looking for systems and services to potentially exploit or attack. An OT Siren will be discovered because it is designed to independently emit network traffic as if it was a fully functioning system.

Decoys are highly believable targets for threats actively scanning a network looking for systems and services to potentially exploit or attack. A decoy will be discovered because it is designed to respond to various service requests as if it was a fully functioning system.

In either case, once discovered, the attacker will focus efforts on the respective OT Siren or decoy, enabling countermeasures to be taken.

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.

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.

Vendor agnostic.

Decoys and sirens on a network easily can be configured to exactly match the model, version and configuration of devices in actual use regardless of manufacturer.

Automated adaptive responses.

When operating in-line, the solution provides graduated response capabilities including 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.

OT360 is well aligned with the July, 2020 joint alert from US NSA and CISA, as well as various 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 lightweight, active cybersecurity deception solution for both IT and OT using lightweight, agentless internal and external deception artifacts to prevent, detect and respond to threats automatically without complex orchestrations.

Contact Us Today

Call: 855-758-4737

Email: info@packetviper.com