Attivo Networks Deception Platform Integrates with Cisco pxGrid Simplifying Detection and Incident Response

Attivo Networks has partnered with Cisco to deliver a simplified solution for the real-time detection, analysis, and automated blocking of cyberattacks. the joint solution allows customers to create policies to automatically block and quarantine endpoints based on suspicious activity. Customers benefit from the reduction of time and resources required to detect threats, analyze attacks, and to remediate infected endpoints, ultimately reducing the organization's risk of breaches and data loss.

Highlights

- Real-time Threat Detection
- Attack Analysis and Forensics
- Automated Quarantine and Blocking
- Expedite Incident Response
- Cross-platform Information Sharing

Joint Solution Brief

The Challenge

To keep IT environments secure and running smoothly, businesses have had to use a wide range of tools and platforms from different vendors. These include identity and access management (IAM) platforms, policy platforms, security information and event management (SIEM) systems, threat defense systems, and many others. All of these tools are critical to protect the business and safeguard their operations. But they might not all talk to each other, creating multiple "silos" of information and a huge operational challenge.

Swiveling from one tool to another adds a lot of complexity and cost to security operations effort. It also reduces the overall effectiveness of IT security because it can take a long time, and a great deal of manual effort, to get the information needed from each of these tools to take the appropriate security action or respond to a threat. That is time that businesses can not afford when an advanced attack is seeking to burrow deeper into the environment or exfiltrate sensitive data.

Changing the Game

A modern day approach to today's security infrastructure requires a blend of prevention and detection for an adaptive defense. By integrating through a common platform for collaboration, attack context sharing can occur, enabling the automation to block attackers, therefore dramatically improving incident response and a company's overall cyber defense. This new approach is based on first preventing what you can, but then adding detection to identify threats that are mounting their attack within the network. Real-time detection is effective for identifying the known and unknown attacker. Not reliant on data base look up, deception and decoy techniques are used to entice engagement with Robots (BOTs) and Advanced Persistent Threats (APTs) that have made their way inside the network. Through engagement, attackers are detected early and attacks analyzed based upon engagement.

Attacks are then analyzed with detailed attack forensics generated to be shared through common information sharing platforms. This information can be used to then automatically block the exfiltration of data or lateral movement of the

"Two thirds of respondents said most cyber threat information is not timely enough by the time it's shared"

Ponemon Second Annual Study on Exchanging

Cyber Threat Intelligence: There Has to Be a Better Way

attacker, which would be used to infect additional systems. The benefit to security operations teams comes with the ability to gather relevant threat information faster and to be able to take responsive action immediately.

The Joint Solution

The integration of Cisco ISE pxGrid cross collaboration platform with the Attivo Networks ThreatDefend™ Deception Platform can be set up in a matter of minutes, empowering organizations with an integrated adaptive security platform that provides effective prevention, real-time detection of cyber attackers, and the ability to automatically block attacks so that data is not exfiltrated or additional endpoints infected.

The Attivo BOTsink solution seamlessly integrates with the Cisco ISE and WSA as well as all other pxGrid ecosystem partners to provide the needed intelligence to quarantine and block the infected nodes from infecting other systems on the corporate network or gaining Internet access and exfiltrating valuable company data.

The solution starts with the BOTsink platform identifying the infected device and CNC address. The IP address is then shared through pxGrid for policy enforcement; quarantining the device, stopping any communication with the Command and Control (CNC), and preventing any data exfiltration.

Combined, the integrated solution provides a real-time, non-disruptive way of detecting and blocking BOTs and APTs inside the network, eliminating the opportunity for an attacker to exfiltrate valuable company assets and information.

Attivo Deception Platform

As a critical part of an adaptive security defense system, the Attivo Networks Deception Platform provides the inside-the-network threat detection designed to deceive and misdirect attackers trying to reach or compromise valuable assets or company infrastructure.

The deception platform, comprised of BOTsink Engagement Servers, an End-Point Deception Suite, and analysis engine, will detect threats from all threat vectors including targeted, stolen credentials, ransomware, phishing, and insider attacks and is highly efficient for threat detection within user networks, data centers, clouds, IoT, and ICS- SCADA environments. Detection can start at the point of initial reconnaissance or scanning of the network through to detecting the lateral infection phase of an attacker as they look to escalate privileges and find the targeted asset. Once the attacker is engaged, the platform collects and correlates the full Techniques Tactics and Procedures (TTP) with associated forensics and reports via IOC, STIX, CSV and PCAP file formats for fast remediation. This information can be manually or automatically shared with security prevention systems, empowering organizations the notice and attack information required to deflect and stop the attack.

About Attivo Networks

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response. www.attivonetworks.com

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. For ongoing news, please go to http://thenetwork.cisco.com.

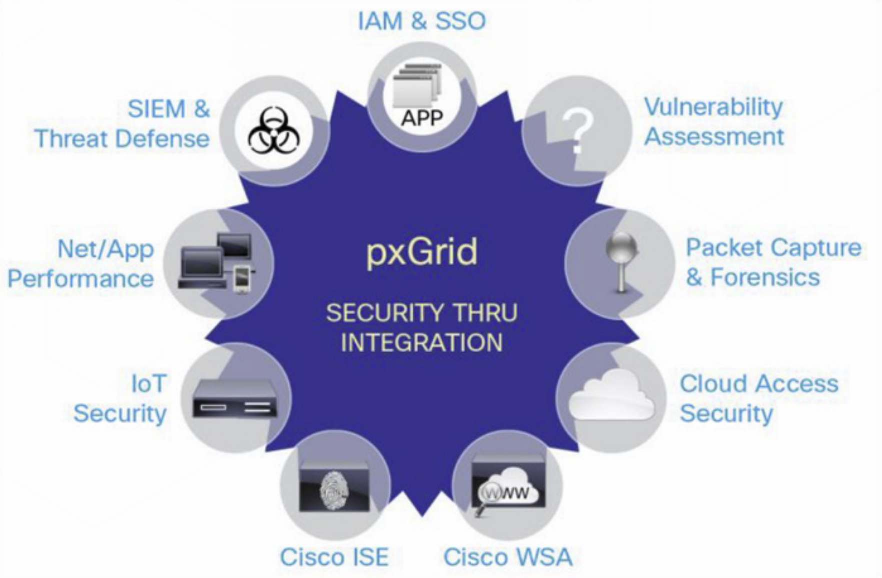
Joint Solution Brief

Cisco pxGrid

pxGrid provides a common transport language between the various network and security systems in the IT environment. Eliminating the need for each system to rely on single purpose APIs, they can all be integrated with pxGrid to share contextual information with each other. Intersystem communications can then happen automatically and immediately with no manual intervention required. pxGrid enables multivendor, cross-platform network system collaboration among multiple parts of the IT infrastructure enabling IT and security vendors to use pxGrid to share context with Cisco platforms that use pxGrid, as well as with systems from any other pxGrid ecosystem partner.

Summary

Information sharing and the automation of incident response, for blocking and quarantining an active attack, can dramatically reduce the risk and impact of a potential breach. Attivo Networks deception technology allows for the real-time detection and identification of reconnaissance activities and early lateral movement infections that are often the first step in a sophisticated breach strategy. Configuring BOTSink engagement servers to integrate with the Cisco pxGrid delivers an effective and efficient solution for early threat detection, prompt incident response, and the effective derailing of cyberattacks.



pxGrid Ecosystem Partners

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners.