Omnis Cyber Intelligence Increases Network Visibility and Improves Threat Hunting Maturity Model

OVERVIEW

The Challenge

- Company had visibility gaps in the network and cloud
- Security Operations Center (SOC) Maturity Model for Threat Hunting was underdeveloped
- Not using previous Omnis® Cyber Intelligence (OCI) purchase and packet metadata to its full potential

The Solution

- Knowledge transfer to improve SOC analysts threat hunting capabilities and get more value out of original purchase
- Adding additional Cyber Adaptors to gain a more comprehensive visibility of their attack surface
- OCI bootcamps for ongoing SOC Analyst development

The Results

- Better visibility into their network and understanding of existing infrastructure
- Discovered Log4j vulnerability during onboarding and applied immediate remediation
- NETSCOUT® is a trusted advisor and continuously provides key insights into their visibility and threat hunting challenges
- OCI was able make their existing security technology stack stronger with easy integration and higher quality data

Company Background

This government agency has thousands of employees and supports millions of customers each year in multiple functions.

Challenge

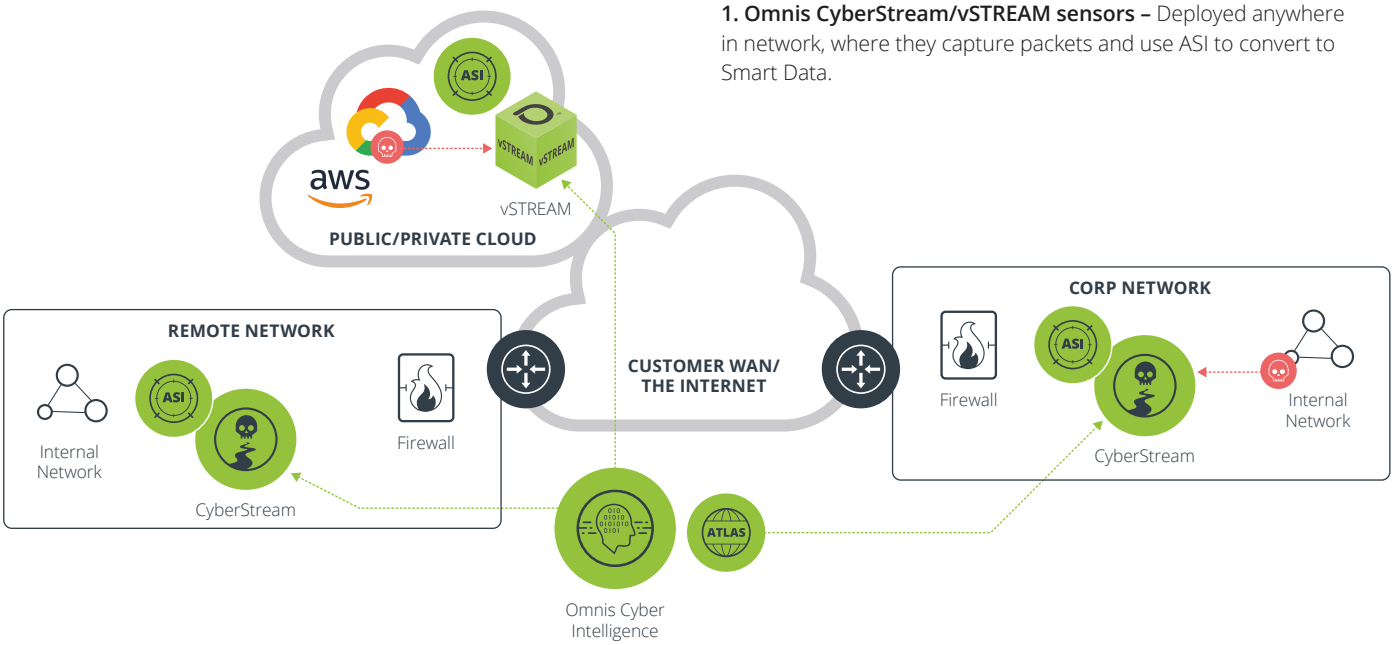
This client was in the process of building out their SOC and wanted to leverage any existing technologies they had for security purposes.

Last year this organization purchased a small order of OCI Cyber Adaptors for visibility into their 2 main datacenters that were on opposite sides of the country. The primary use by the SOC team for Omnis Cyber Intelligence was a packet capture and retrieval function related to an incident identified in their Splunk, Security information and event management (SIEM) platform.

During initial product training of their first purchase, they learned more about their current infrastructure and the visibility gaps that existed, so they purchased more cyber adaptors to fill those gaps.

With this ability to get a more comprehensive view of their attack surface, they were also able to look back in time, specifically to show the Log4j vulnerability.

1. Omnis CyberStream/vSTREAM sensors – Deployed anywhere in network, where they capture packets and use ASI to convert to Smart Data.



2. Omnis Cyber Intelligence – The central console that analyzes CyberStream/vSTREAM Smart Data; uses behavioral analysis and ATLAS/3rd party intelligence, for threat detection and highly contextual investigation.

Solution in Action

- **Knowledge Transfer** – Additional training for over 25 of their SOC analysts, the NETSCOUT team walked them through an interactive demonstration using their existing OCI solution on how to investigate and hunt for cyber threats through the user interface. During a live demonstration with the SOC analysts, we identified the Log4j vulnerability.
- **Cyber Adaptors** – By providing training on their existing solution, the organization realized they had more gaps in visibility and the value of adding more adaptors would increase their capabilities and reduce risks.
- **Back in Time Feature** – The tier 1 analyst was alerted to potential threats and easily able to package their findings for the tier 2 analyst to investigate and validate. The tier 2 analyst was able to use the back in time feature and discovered additional Log4j vulnerabilities that needed immediate remediation.
- **Easy Integration** – Their current workflow starts with Splunk; OCI's integration allows them to use OCI without drastic changes to their normal workflow.

The Results

With the improved partnership with NETSCOUT, the SOC team can now see firsthand how threats are identified, investigated, and remediated in hours or minutes through OCI versus the previous manual process of sifting through logs, which takes days, weeks, or even months.

OCI helped this organization build out the full picture of the entire attack chain, identify the gaps from the previous patch and validate the vulnerability was properly addressed and remediated.

LEARN MORE

For more information about NETSCOUT Omnis Cyber Intelligence:

www.netscout.com/product/cyber-intelligence

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

bako tech®

BAKOTECH is an international group of companies, a flagship in focused Value Added IT Distribution that represents solutions of leading IT vendors. Positioning itself as a True Value Added IT distributor BAKOTECH provides professional pre-sales, post-sales, marketing and technical support for partners and end-customers. BAKOTECH is the official distributor of Netscout in Ukraine, Georgia & CIS, Central Asia countries.

netscout@bakotech.com

+380 44 273 3333

www.netscout.bakotech.com

SECSB_001_EN-2201 02/2022