NETSCOUT Omnis Intrusion Detection System

Smart Security and Visibility

HIGHLIGHTS

- High performance IDS solution using Suricata open source technology
- Omnis® Cyber Intelligence (OCI) for centralized management via intuitive Web UI
- Identifies lateral movement, brute-force attacks, privilege escalation, ransomware, and command & control exploits
- Uses Suricata and supports open source, commercial, private, and customized rulesets technology for detection
- Quickly assesses threats with automated alert prioritization
- Sends contextually rich alerts and metadata to Omnis Cyber Intelligence, and/or SIEM, including Splunk

NETSCOUT's Omnis® Intrusion Detection System (IDS), a vital part of the NETSCOUT® Omnis Security solution, provides network intrusion detection for enterprises of all sizes. With seamless integration into open security stack, Omnis IDS delivers preconfigured and customizable rule configuration that will bring scalability, visibility, and efficiency to your security program. Based on the leading IDS platform, Suricata and supporting open source, commercial, private, and customized rulesets, Omnis IDS offers a comprehensive, high-performance, cost-effective intrusion detection software-based solution.

Omnis IDS incorporates the Omnis IDS Sensor, and Omnis Cyber Intelligence components described below.

Omnis IDS Sensor

Omnis IDS Sensors are high-performance software appliances strategically deployed throughout the enterprise environment for collecting and analyzing network packet traffic to detect intrusions. Omnis IDS Sensor uses Suricata and supports open source, commercial, private, and customized rulesets to detect security threat events and initiate alerts.

Omnis Cyber Intelligence

Omnis IDS Explorer in the Omnis Cyber Intelligence is a powerful analytics and centralized management system. Multiple Omnis IDS Sensors forward security threat events to the Omnis IDS Explorer to apply further analysis and initiate alert triggers. It can also be configured to forward security threat events and alarms to third-party security information and event management (SIEM) systems for consolidated security event management.

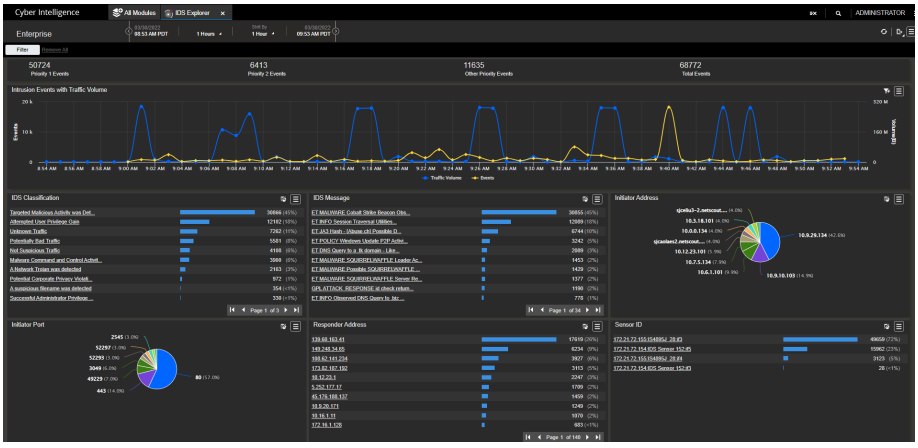

Figure 1: Omnis Cyber Intelligence event analysis.

Key Features

Omnis IDS Sensor

- **Visibility** – As part of a comprehensive visibility plan, Omnis IDS Sensors can be easily deployed to provide packet visibility for insights into the areas of the network deemed critical.
- **Rule Signature Comparison** – Uses Suricata and supports open source, commercial, private, and customized rulesets for the ability to add or remove rules with no disruption of service.
- **Alerting** – Reduces alert fatigue, with the ability to refine tuning to meet the most important, unique needs of the business.

Omnis Cyber Intelligence

- **Centralized Management** – Simplifies and streamlines the deployment and management of the IDS sensors with ability to configure, edit, and customize sensors from a single pane of glass for consistent, reproducible, and predictable deployment of 1 or many IDS Sensors.
- **Centralized Reporting** – Aggregates metadata into a flexible interface for simple visualization and customized prioritization. Provides this information in a consistent view, which gives Security Operations Center (SOC) teams the information they need to understand the attack and respond faster.
- **Central Analysis** – Provides complete visibility into the entire attack chain, and risks associated with it, to alert the Omnis IDS Explorer and/or a 3rd party SIEM export (Splunk) for correlation, collaboration, and refinement of response efforts.

Omnis Cyber Intelligence

Product Type	SKU	Description
Software	91D10L	Omnis Cyber Intelligence – Entry (5) – Software – (Linux)
Appliance	51D41L	Omnis Cyber Intelligence – Workgroup (10) – Standard Appliance
Appliance	51DH1L	Omnis Cyber Intelligence – Intermediate (25) – Standard Appliance
Appliance	51D51L	Omnis Cyber Intelligence – Full (50) – Standard Appliance
Appliance	51D21L	Omnis Cyber Intelligence – Full (50) – Standby Appliance
Software	91D40L	Omnis Cyber Intelligence – Workgroup (10) – Software – (Linux)
Software	91DH0L	Omnis Cyber Intelligence – Intermediate (25) – Software – (Linux)
Software	91D700	Omnis Cyber Intelligence – Incremental (50) – Software – (Linux)
Software	91D20L	Omnis Cyber Intelligence – Full (50) – Standby Software – (Linux)
Software	91D50L	Omnis Cyber Intelligence – Full (50) – Software – (Linux)
Software	91DK00	Omnis Cyber Intelligence – Intermediate (25) License Upgrade to Full (50)
Software	91DU00	Omnis Cyber Intelligence – Workgroup (10) License Upgrade to Full (50)
Software	91D50L-E	Omnis Cyber Intelligence – Full (50) – Software – (Linux) – Evaluation
Software	51DD1L	Omnis Cyber Intelligence – Dedicated Global Manager – Appliance
Software	91DD0L	Omnis Cyber Intelligence – Dedicated Global Manager – Software – (Linux)

Omnis IDS Sensor

Product Type	SKU	Description
Software	Q-02795-010-1	Certified Omnis IDS Sensor software, 10G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+), for use with C-02700 certified appliance hardware.
Software	Q-04895-020-2	Certified Omnis IDS Sensor software, 20G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+), for use with C-04800 certified appliance hardware.
Software	Q-04895-030-2	Certified Omnis IDS Sensor software, 30G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+), for use with C-04800 certified appliance hardware.
Software	Q-04895-040-2	Certified Omnis IDS Sensor software, 40G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+), for use with C-04800 certified appliance hardware.
Software	Q-04807-040-2	Certified Omnis IDS Sensor software, 40G license, includes NETSCOUT 2-Port 40G ASI Accelerator NIC (QSFP+), for use with C-04800 certified appliance hardware.
Software	Q-05095-010-X	Qualified Omnis IDS Sensor software, 10G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+), for use with qualified servers.
Software	Q-05095-020-X	Qualified Omnis IDS Sensor software, 20G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+), for use with qualified servers.
Software	Q-05095-030-X	Qualified Omnis IDS Sensor software, 30G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+), for use with qualified servers.
Software	Q-05095-040-X	Qualified Omnis IDS Sensor software, 40G license, includes NETSCOUT 4-Port 10G ASI Accelerator NIC (SFP+), for use with qualified servers.
Software	Q-05007-040-X	Qualified Omnis IDS Sensor software, 40G license, includes NETSCOUT 2-Port 40G ASI Accelerator NIC (QSFP+), for use with qualified servers.
Software	C-02700-XSJA1	Certified InfiniStreamNG server, 1U, Single 22-Core CPU, 192GB, 32TB (4x 8TB, Not Expandable), AC.
Software	C-02700-XSJD1	Certified InfiniStreamNG server, 1U, Single 22-Core CPU, 192GB, 32TB (4x 8TB, Not Expandable), DC.
Software	C-04800-XSJA2	Certified InfiniStreamNG server, 1U, Dual Intel 6152 22-core 2.1GHz CPUs, 384GB RAM, 32TB (4x 8TB), AC Power.
Software	C-04800-XSJD2	Certified InfiniStreamNG server, 1U, Dual Intel 6152 22-core 2.1GHz CPUs, 384GB RAM, 32TB (4x 8TB), DC Power.

SPECIFICATIONS

Characteristic	C-02700-XSJA1 C-02700-XSJD1	C-04800-XSJA2 C-04800-XSJD2
Management Port	2 RJ-45 1/10GBASE-T 1 IPMI 1000BASE-T	
CPU	Single 22-core	Dual 22-core
Memory	192GB	384GB
Storage	32TB HDD in RAID 5	32TB HDD in RAID 5
Embedded OS	Solid State Drive (SSD) dedicated to Linux® OS	
Rack Unit	1 Rack Unit (1RU)	
Dimensions	Height: 1.7 in (4.3 cm) Width: 17.2 in (43.7 cm) Depth: 25.6 in (65 cm)	
Weight (Maximum Configuration)	38 lbs (17.24 kg)	
Vibration (Operating)	0.25 G from 5-200 Hz for 15 minutes	
Mechanical Shock (Operating)	1 shock pulse of 20G for up to 2.5 ms	
Altitude	-50 to 10,000 ft (-16 to 3,048 m)	
Temperature (Storage)	-40°F to 149°F (-40°C to 65°C)	
Temperature (Operating)	50°F to 95°F (10°C to 35°C) at altitudes less than 2953 ft or 950 m with no direct sunlight on the equipment	
Maximum Temperature Gradient (Storage and Operating)	36°F in an hour (20°C/h) and 9°F in 15 minutes (5°C/15 min)	
Operating Altitude De-rating	Maximum operating temperature is reduced by 1.8°F/984 ft (1°C/300 m) above 2953 ft (900 m)	
Humidity (Storage)	5% to 95% RH with 91°F (33°C) maximum dew point. Atmosphere must be non-condensing at all times	
Humidity (Operating)	10% to 80% relative humidity with 84.2°F (29°C) maximum dew point (non-condensing)	
Power Rating (AC)	Dual auto-ranging hot-swappable, redundant supplies: 700W: 100-140 VAC, 50-60 Hz, 8.0-6.0 Amp 750W: 200-240 VAC, 50-60 Hz, 4.5-3.8 Amp	
Maximum Power Consumption (AC)	6.5A, 655W, 2235 BTU/Hr	
Power Rating (DC)	Dual hot-swappable, redundant supplies: -48VDC, 650W, 20A	
Maximum Power Consumption (DC)	13.7A. 658W, 2245BTU/Hr	
Regulatory Approvals	Regulatory Model Number: NV51U, FCC Part 15 Class A, CE Mark (EN55032 Class A, EN 55024, EN 61000-3-2, EN 61000-3-3), VCCI (Japan) Class A, RRA (Korea) KC Cert #: R-R-NSZ-NV51U, CCC Class A (China), EAC (Russia), BIS (India), CM (Morocco), UL-C of C (Mexico), BSMI (Taiwan), LoA (South Africa), UL 60950-1/62368- 1, CAN/CSA C22.2 No. 60950/62368-1, IEC 60950-1/62368-1, EN 60950-1/62368-1, CB Report	

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)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

EPDS_042_EN-2201 07/2022