Print Post Approved PP100003227

AUSTRALIAN SECURITY MAGAZINE

THE COUNTRY'S LEADING GOVERNMENT AND CORPORATE SECURITY MAGAZINE | www.australiansecuritymagazine.com.au

June/July 2018

Top tax tips for security employees

Much more to do in locking down

This is cyber – So what is cyber?

The AV system done it!

Hostile vehicle attacks: Smart city planning

IoT – Securing the connected world

A cyber week in London – Part 1

Digital Forensics 101

Encryption Headaches

The State of the Security Union

AVIATION SECURITY

READY FOR TAKE OFF

$8.95 INC. GST

9 772201 460013 >

Cyber Security Weekly Podcast

PLUS Techtime

Jask expands platform beyond SIEM to transform how soc operators visualize cyber attacks

JASK the provider of the industry's first Autonomous Security Operations Center (ASOC) platform, is capturing industry demand with new features centered around enterprise-wide alert linkages and analyst workflow efficiency. Major enhancements include the JASK Navigator, a visually-driven, contextually-rich investigation console that provides SOC analysts a one-click path to situational attack awareness, multi-asset data ingestion; query flexibility and analyst team workflow support.

"Through our discussions with both partners and customers one thing has become crystal clear, the SOC of the future will not rely heavily on legacy SIEM technologies," said V.Jay LaRosa, VP Global Security Architecture, Chief Security Architect at ADP. "There are a lot of cybersecurity solutions and technologies promising ways to get more out of technology investments, and JASK is maniacally focused on truly addressing enterprise-wide alert prioritization, context and visibility by focusing on analyst workflows."

JASK ASOC Built to Streamline Analyst Jobs

Since launching the platform in July 2017, JASK's vision is delivering an asset-independent, open platform that enables an autonomous workflow of what, where, why and how analysts should take action. Using artificial intelligence (AI) and machine learning as its base engine, the platform is built for broad and smarter data ingestion to reduce costs and bandwidth without losing context. With its latest enhancements, the JASK ASOC platform improves visibility through unique mapping of data to records linked across devices, users, networks, applications and almost any third-party data source.

"JASK understands the urgency CISOs have placed on consolidating and integrating security operations technologies," said Jon Oltsik, Distinguished Analyst and Fellow at Enterprise Strategy Group. "By seamlessly fitting into existing environments, offering an intuitive user interface and reducing the overwhelming volume of alerts, JASK is addressing the top concerns SOC teams report."

JASK Navigator Console and Enhanced Team Workflow

JASK Navigator is an elegantly simple, visually-driven investigation console that equips analysts with an actionable view of JASK Insights, prioritized notifications of data that indicate a combination of events or activities that should be investigated, with all the associated signals and alert information that led to its delivery. Investigations are streamlined and logical, offering SOC teams one-click access to better prioritized insights and faster paths to resolution.

To further support enterprise analyst workflows, JASK is also developing team support via customizable workflow queues within the ASOC platform. This allows customers to represent user groups or teams in order to assign the triage of JASK Insights. The enhanced workflows allow teams to easily adjust the Insights stage, providing improved visibility into the overall status of all assigned tasks. JASK also allows analysts to assign and visualize alerts from existing security solutions by user, team and status.

"The attacker is winning in today's constantly changing threat landscape. The SOC is no longer human-scalable," said J.J Guy, CTO of Jask. "A flexible platform that focuses on analyst workflows to improve efficiency is a critical step forward in offering SOC teams immediate visibility and context. We must stop building our teams to support technology, and build technology to support our teams."

Off to a strong start in 2018, JASK doubled its customer base in the first quarter of 2018, adding enterprises spanning higher education, financial services, healthcare and retail. Additionally, the company continues to support existing security operations workflows through partnerships and specific integrations with leading solutions in cybersecurity, including Cylance, Demisto, Carbon Black, Microsoft Active Directory, Splunk, ArcSight, among many more.

For more information on the JASK ASOC platform, please visit https://jask.ai/solutions/product/.

About JASK

JASK is modernizing security operations to reduce organizational risk and improve human efficiency. Through technology consolidation, enhanced AI and machine learning, the JASK Autonomous Security Operations Center (ASOC) platform automates the correlation and analysis of threat alerts, helping SOC analysts focus on the highest-priority threats, streamlining investigations and delivering faster response times. www.jask.ai

Apstra deployed with Dell EMC and OPX by Awnix in open IaaS network infrastructure in Tier 1 service provider cloud

Apstra has announced that Awnix, a leading provider of cloud services and products, has deployed the first AOS® supported deployment of OpenSwitch (OPX) on Dell Z9100-ON switches in a Tier 1 service provider production network. The telecom service provider deployment includes a combined solution as part of a hybrid cloud for OpenStack Deployments and is part of an open IaaS network infrastructure offering.

The Awnix, Dell EMC, Apstra solution provides a cloud platform that meets the needs of both internal and external users at the telecom provider. The solution includes the features and ease of use desired by the service provider, while increasing control, auditability, security, and ease of management. The outcome is lower cost—beyond what is available from public cloud service providers or proprietary on-premise alternatives.

"The Z9100s are amazing. In fact, the entire line of Open Networking switches from Dell EMC is phenomenal – and Apstra's AOS software is the best management and monitoring tool I've seen for networking in decades," said Rick Kundiger, Awnix CEO. "100Gb is the new 10Gb; big brands are the past; cost effective devices and tools, security, and reduced lock-in are in now. In today's highly competitive cloud and IoT space, companies that can iterate faster for less will win. By combining our cloud with Dell EMC's switches and Apstra AOS for management, we can help

customers achieve that desired win."

"Dell EMC's Open Networking initiative is about choice and flexibility, without a compromise on technology," said Drew Schulke, Vice President Dell EMC Networking. "With OpenSwitch, Dell EMC Networking expands its Open Networking strategy to Open Source Networking enabling Awnix to combine OPX with Apstra's AOS to give unparalleled value and flexibility to the customer."

"Apstra's AOS provides scalable vendor-independent intent-based automation of the entire life cycle of network services – from day zero, to day one, to day two and beyond – including change operations, as well as advanced intent-based analytics for unmatched reliability, visibility, and troubleshooting ability," said Mansour Karam, CEO and Founder at Apstra. "As new products become available, they can be incorporated seamlessly without having to change operating procedures. Apstra is pleased to collaborate with Dell EMC and Awnix to deliver the first AOS support for an OPX cloud deployment in a Tier 1 service provider production network, providing greatly enhanced agility, reliability and reduced cost."

The Dell EMC Open Networking strategy helps customers innovate network operations for greater business agility. Dell EMC Open Networking allows customers to choose from a rich set of open network operating systems and software applications for greater automation, security, analytics, and ultimately greater flexibility. With Dell EMC Networking, customers can break vendor lock-in and embrace innovation that drives out complexity and can lower the total cost of ownership.

About OPX

The OpenSwitch platform is an open source, Linux-based network operating system (NOS) for disaggregated switches built around OCP-compliant hardware, utilizing an open network installation environment (ONIE) boot loader. Developers can build on reliable and modern architecture to create unique networking features and applications using an agile development approach for faster development and more stable applications with fewer post-release defects.

About AOS

AOS® delivers a turnkey Intent-Based distributed operating system and a data center application suite that offer game-changing network service agility, increased uptime and dramatically improved infrastructure TCO. AOS automatically prevents and repairs network outages for dramatically improved infrastructure uptime. It operates a network as one system, massively improving infrastructure agility while reducing operational expenses. AOS' distributed data store is a repository of all intent, configuration, and telemetry state, and hence acts as a single source of truth for your network. Its self-documenting nature streamlines compliance tasks. AOS is hardware-independent and works across all major vendors as well as open alternatives.

Awnix

Awnix is a leading provider of cloud services and products that provide organizations with a fast and easy way to transition away from expensive legacy virtualization platforms, and towards a secure private cloud to run their virtual servers, containers, and virtualized network functions. Awnix's products and services include the Advanced Rival Cloud (ARC), a turnkey cloud platform customized to meet each organization's unique needs and budgets, ARChive Restore, Backup, and Disaster Recovery software for OpenStack, ARCmon for cloud alerting and monitoring, and 24×7 support and cloud management services. Awnix has been delivering secure private cloud products and services since 2014 and its main offices are in Austin, Texas and Kansas City, Missouri.

About Apstra, Inc.

Apstra® pioneered Intent-Based Networking and Intent-Based Analytics™ to simplify how data center networks are built and operated. AOS® increases business agility through an autonomous or Self-Operating Network™ that delivers log-scale improvements in CapEx, OpEx and capacity. AOS is a hardware-inclusive, closed-loop intent-based distributed operating system that automates the full lifecycle of network operations and enables the network to configure itself, fix itself and defend itself. Apstra is based in Menlo Park, California and is privately funded.