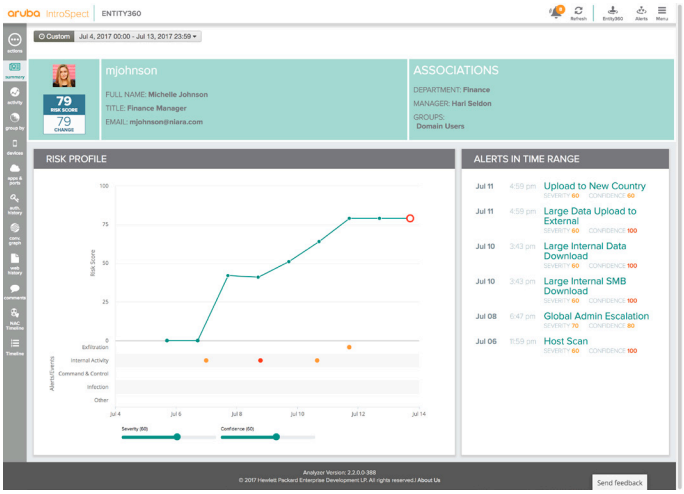
HOJA TÉCNICA

ARUBA INTROSPECT



ANALÍTICOS DE COMPORTAMIENTO DE USUARIOS Y ENTIDADES

La solución de Analíticos de Comportamiento de Usuarios y Entidades (UEBA por sus siglas en inglés) de Aruba, Aruba IntroSpect, detecta ataques identificando pequeños cambios en comportamiento que frecuentemente son indicativos de ataques que han evadido las defensas de seguridad tradicionales. Aruba IntroSpect integra aprendizaje de máquina (ML) avanzado basado en Inteligencia Artificial, visualizaciones puntuales y perspectiva forense instantánea en una sola solución, para que los ataques que involucran a usuarios, sistemas y dispositivos maliciosos, comprometidos, o negligentes se puedan encontrar y reparar antes de que puedan dañar las operaciones y reputación de la organización.

Con una plataforma Spark/Ha doop, IntroSpect integra en forma única la detección de ataques basada en comportamiento y la investigación forense de incidentes y respuesta a escala empresarial.

LO QUE DETECTAMOS: CASOS DE USO DE ANALÍTICOS DE SEGURIDAD

IntroSpect proporciona más de 100 modelos de aprendizaje de máquina supervisados y no supervisados enfocados en detectar ataques enfocados en cada etapa de la cadena:

- Abuso de Cuentas
- Toma de Control de Cuentas
- Comando y Control
- Exfiltración de Datos
- Movimiento Lateral
- Compartir Contraseñas
- Escalación de Privilegios
- Flight Risk
- Phishing
- Ransomware

BENEFICIOS CLAVE

Analíticos Avanzados

- Más de 100 modelos de aprendizaje de máquina supervisados y no supervisados
- Aprendizaje adaptativo
- Modelos extensibles (nuevos casos de uso, fuentes de datos)

El Rango Más Amplio de Fuentes de Datos

- Paquetes, flujos, logs, alertas
- Cualquier combinación, dependiendo de los casos de uso

Calificación de Riesgo Actualizada Continuamente

- Ponderada por severidad, secuencia, distribución y tiempo
- El contexto de negocio informa la calificación de riesgo

Investigaciones Aceleradas

- Reducción de 10x en tiempo y esfuerzo
- Registro histórico completo hasta el nivel de paquetes

Rápida Implementación

- En sitio o en la nube
- Plataforma autónoma o integrada
- Ingesta datos en forma nativa o del SIEM, administración de logs, packet broker
- Inicio optimizado vía IntroSpect Standard Edition

Escala Empresarial

- Plataforma Spark/Hadoop
- Billones de eventos por día
- Cientos de miles de usuarios y dispositivos

INVESTIGACIÓN Y RESPUESTA ACELERADA

De SysAdmins a Sistemas a Sensores — Proporcionando Visibilidad Instantánea

IntroSpect Entity360 es clave para reducir el tiempo y esfuerzo requerido para entender, diagnosticar y responder a un ataque. Entity360 proporciona un perfil de seguridad exhaustivo con calificación de riesgo continua e información de seguridad enriquecida – de otra forma, analistas invertirían horas o días buscando y compilando meses y años de datos de seguridad hasta el nivel de paquetes. Entity360 proporciona:

- Perfiles para usuarios, sistemas y dispositivos
- Acceso por SIEM, sistemas NAC, etc. vía una API abierta
- Playbooks de respuesta a incidentes pre empaquetados
- Ahorro de 30 horas/investigación medido por clientes
- Detección automática de otras entidades impactadas por el ataque

CACERÍA DE AMENAZAS

Cacería de amenazas proactiva se logra fácilmente con una interface de consulta poderosa, sin la carga de buscar, encontrar y sumarizar almacenes de datos aislados.

- Analíticos enriquecidos para probar hipótesis de amenazas en cualquier plazo de tiempo
- Búsqueda automatizada de datos históricos utilizando IOCs de STIX y feeds de amenazas personalizados
- Visualizaciones para resaltar anomalías e interacciones significativas
- Actividad significativa monitoreada y etiquetada para ayudar con la cacería y las investigaciones

FUENTES DE DATOS

La plataforma IntroSpect procesa el rango más amplio de fuentes de datos, incluyendo:

- VPN, FW, IPS/IDS, Web proxy, Email logs
- NetFlow, Bro logs
- Logs de protección EndPoint
- Logs de DLP
- Paquetes
- Logs de DNS
- Logs de Active Directory
- Logs de DHCP
- Feeds de amenazas externas
- Alertas de la infraestructura de seguridad de terceros

OPCIONES DE IMPLEMENTACIÓN

- Software o dispositivo en sitio
- Aplicación Hadoop en sitio
- AWS o Azure Virtual Private Cloud (VPC)

INTEGRACIONES CLAVE

- Aruba ClearPass
- HPE ArcSight
- IBM QRadar
- Splunk
- Intel McAfee Nitro
- Gigamon
- Carbon Black
- Microsoft
- Palo Alto Networks
- FireEye
- Cisco
- Symantec

INFORMACIÓN PARA PEDIDOS

Número de Parte	Descripción
Hardware	
JZ261A	Aruba IntroSpect 5Gbps Hybrid Packet Log and Flow Data Processor (with 1yr Support) FPC 2000 Appliance
JZ262A	Aruba IntroSpect 5Gbps Hybrid Packet Log and Flow Data Processor (with 1yr Support) PP 1000 Appliance
JZ263A	Aruba IntroSpect Analyzer 2000 (incluye 1 año de Soporte) Appliance
JZ264A	Aruba IntroSpect Analyzer 2500 (incluye 1 año de Soporte y SSD) Hardware
JZ265A	Aruba IntroSpect Analyzer 1000 Analyzer Node (incluye 1 año de Soporte y Copper Mgmt Port) Appliance
JZ266A	Aruba IntroSpect Analyzer 1000 Compute Node (incluye 1 año de Soporte y Copper Mgmt Port) Appliance
JZ267A	Aruba IntroSpect Analyzer 1050 Analyzer Node (incluye 1 año de Soporte y Fiber Mgmt Port) Appliance
JZ268A	Aruba IntroSpect Analyzer 1050 Compute Node (incluye 1 año de Soporte y Fiber Mgmt Port) Appliance
JZ269A	Aruba IntroSpect Analyzer 1500 Analyzer Node (con 1 año de Soporte y SSD y Copper Mgmt Port) Appliance
JZ270A	Aruba IntroSpect Analyzer 1500 Compute Node (con 1 año de Soporte y SSD y Copper Mgmt Port) Appliance
JZ271A	Aruba IntroSpect Analyzer 1550 Analyzer Node (con 1 año de Soporte y SSD y Fiber Mgmt Port) Appliance
JZ272A	Aruba IntroSpect Analyzer 1550 Compute Node (con 1 año de Soporte y SSD y Fiber Mgmt Port) Appliance
JZ273A	Aruba IntroSpect Switch 24-Port 10G (incluye 1 año de Soporte) Appliance
Software: Precios del Software para Procesamiento de Paquetes – Suscripción	
JZ231AAE	Aruba IntroSpect Packet Processor 100Mbps 1yr E-STU
JZ232AAE	Aruba IntroSpect Packet Processor 100Mbps 3yr E-STU
JZ233AAE	Aruba IntroSpect Packet Processor 100Mbps Perpetual E-LTU
Software: Precios del Software para Captura de Paquetes Completos – Suscripción	
JZ234AAE	Aruba IntroSpect Full Packet Capture 100Mbps 1yr E-STU
JZ235AAE	Aruba IntroSpect Full Packet Capture 100Mbps 3yr E-STU
JZ236AAE	Aruba IntroSpect Full Packet Capture 100Mbps Perpetual E-LTU
Software: Precios del Software Analyzer – Suscripción	
JZ237AAE	Aruba IntroSpect Security Analytics Standard Ed 1K Entities (Users and Servers and IoT) 1yr E-STU
JZ238AAE	Aruba IntroSpect Security Analytics Standard Ed 1K Entities (Users and Servers and IoT) 3yr E-STU
JZ239AAE	Aruba IntroSpect Security Analytics Std Ed 1K Entities (Users and Servers and IoT) Perpetual E-LTU
JZ240AAE	Aruba IntroSpect Security Analytics Advanced Ed 1K Entities (Users and Servers and IoT) 1yr E-STU
JZ241AAE	Aruba IntroSpect Security Analytics Advanced Ed 1K Entities (Users and Servers and IoT) 3yr E-STU
JZ242AAE	Aruba IntroSpect Security Analytics Advanced Ed 1K Entities (Users and Servers and IoT) Perp E-LTU
JZ243AAE	Aruba IntroSpect Security Analytics Standard to Advanced Upgrade 1K Entities 1yr E-STU
JZ244AAE	Aruba IntroSpect Security Analytics Standard to Advanced Upgrade 1K Entities 3yr E-STU
JZ245AAE	Aruba IntroSpect Security Analytics Standard to Advanced Upgrade 1K Entities Perp E-LTU

INFORMACIÓN PARA PEDIDOS

Número de Parte	Descripción
Software: Opciones de Licenciamiento Adicionales	
JZ246AAE	Aruba IntroSpect Analyzer HA Standard Ed 1K Entities (Users and Servers and IoT) 1yr E-STU
JZ247AAE	Aruba IntroSpect Analyzer HA Standard Ed 1K Entities (Users and Servers and IoT) 3yr E-STU
JZ248AAE	Aruba IntroSpect Analyzer HA Standard Ed 1K Entities (Users and Servers and IoT) Perpetual E-LTU
JZ249AAE	Aruba IntroSpect Analyzer HA Advanced Edition 1K Entities (Users and Servers and IoT) 1yr E-STU
JZ250AAE	Aruba IntroSpect Analyzer HA Advanced Edition 1K Entities (Users and Servers and IoT) 3yr E-STU
JZ251AAE	Aruba IntroSpect Analyzer HA Advanced Edition 1K Entities (Users and Servers and IoT) Perp E-LTU
JZ252AAE	Aruba IntroSpect Analyzer HA Standard to Advanced Upgrade 1K Entities 1yr E-STU
JZ253AAE	Aruba IntroSpect Analyzer HA Standard to Advanced Upgrade 1K Entities 3yr E-STU
JZ254AAE	Aruba IntroSpect Analyzer HA Standard to Advanced Upgrade 1K Entities Perp E-LTU
Licencias de Laboratorio	
JZ255AAE	Aruba IntroSpect Analyzer Lab License 1yr E-STU
JZ256AAE	Aruba IntroSpect Analyzer Lab License 3yr E-STU
JZ257AAE	Aruba IntroSpect Analyzer Lab License Perpetual E-LTU
JZ258AAE	Aruba IntroSpect Packet Processor Lab License 1yr E-STU
JZ259AAE	Aruba IntroSpect Packet Processor Lab License 3yr E-STU
JZ260AAE	Aruba IntroSpect Packet Processor Lab License Perpetual E-LTU
Mantenimiento – Software	
	Aruba IntroSpect Analyzer Standard Ed 1K Entities 1 yr Support E-STU
	Aruba IntroSpect Analyzer Advanced Edition 1K Entities 1yr Support E-STU
	Aruba IntroSpect Analyzer HA Standard Edition 1K Entities 1yr Support E-STU
	Aruba IntroSpect Analyzer HA Advanced Edition 1K Entities 1yr Support E-STU
	Aruba IntroSpect 100Mbps Packet Processing 1yr Support E-STU
	Aruba IntroSpect 100Mbps Full Packet Capture 1yr Support E-STU

ACERCA DE ARUBA, UNA COMPAÑÍA DE HEWLETT PACKARD ENTERPRISE

Aruba, una compañía de Hewlett Packard Enterprise, es un proveedor líder de soluciones de networking de siguiente generación para empresas de todos los tamaños a nivel mundial. La compañía entrega soluciones de TI que empoderan a las organizaciones para servir a la generación más reciente de usuarios conocedores de movilidad que dependen de aplicaciones de negocio basadas en nube para cada aspecto de sus vidas profesionales y personales. Para más información, visite www.arubanetworks.com. Para actualizaciones de noticias en tiempo real, siga a Aruba en Twitter y Facebook, y para las discusiones técnicas más recientes de movilidad y de productos de Aruba visite Airheads Community en http://community.arubanetworks.com.

aruba
a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com/latam