



SIEM (Security Information & Event Management)

1

Ing. Lucas Lagrave

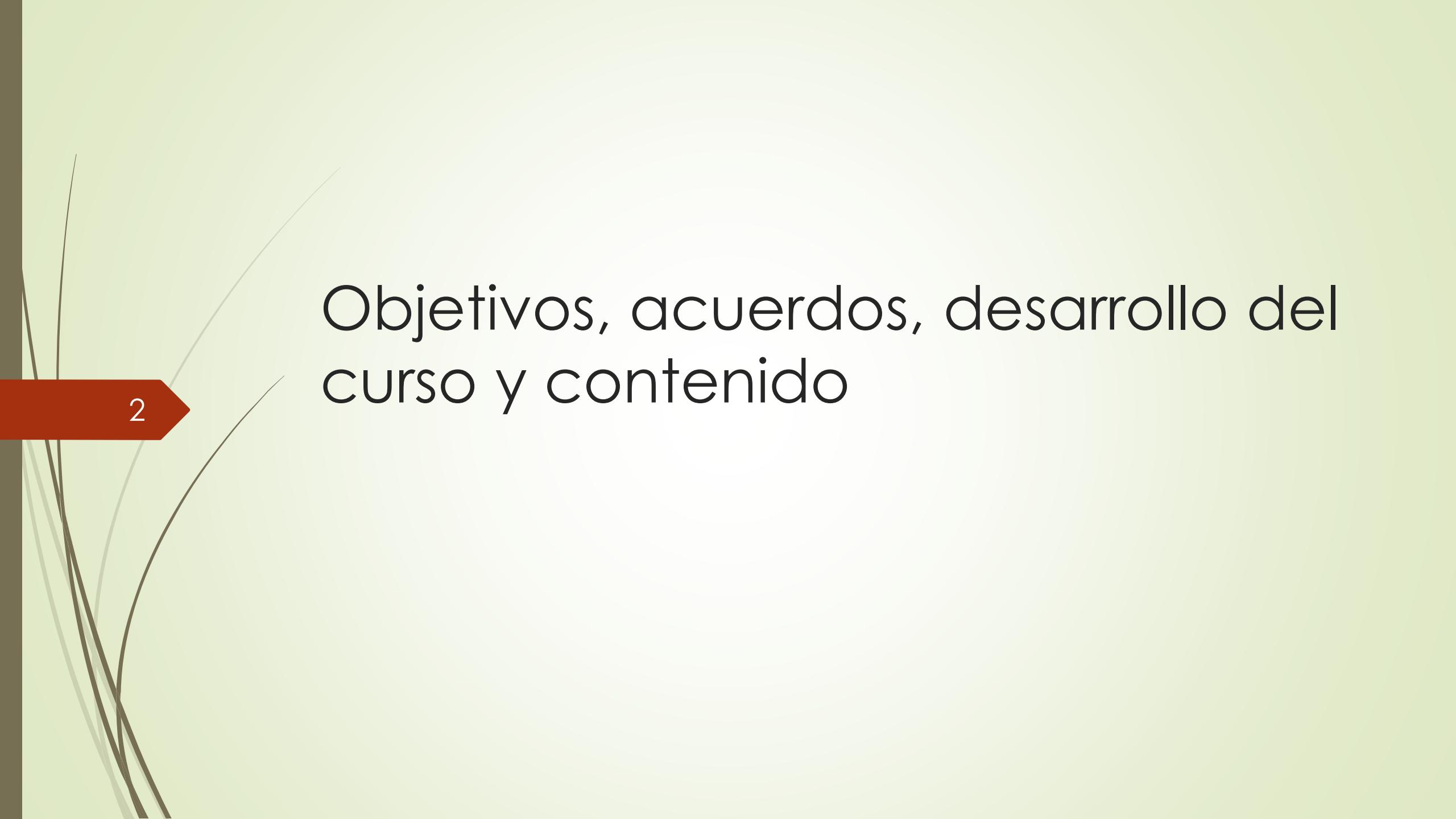
MBA, CISA, CISM, CAMS, OpRM

lucas.lagrave@itau.com.py

Banco Itaú Paraguay SA

lucaslagrave 

lucaslagrave@gmail.com 

The background features a minimalist design with thin, light-colored lines of varying lengths. A prominent element is a thick, reddish-orange arrow pointing to the right, which contains the white number '2'.

2

Objetivos, acuerdos, desarrollo del curso y contenido

Objetivos

3

- Comprender el funcionamiento de un SIEM
- Transmitir la importancia de un SIEM y cómo agrega valor
- Identificar en qué escenarios es útil
- Percibir la importancia de la diversidad de los orígenes de datos
- Conocer el funcionamiento de la tecnología
- Reconocer la importancia de definir adecuadamente el alcance

Acuerdos

- Turnos/horario de las clases
- Dinámica en clase
- Uso de celulares (llamadas, mensajes, emails, etc.)
- Igualdad de condiciones

Desarrollo del curso

5

- Nivelación de conocimientos
- Compartir experiencias
- Desarrollo conceptual
- Independiente al producto / agnóstico a la solución
- Comprender funcionamiento y utilidad
- Trabajo práctico al final

Contenido

6

1. Introducción
2. Funcionamiento
3. Principales características
4. Qué monitorear
5. Orígenes de datos
6. Aseguramiento
7. Monitoreo del SIEM
8. Comparativo de soluciones
9. Resumen
10. Bibliografía
11. Trabajo práctico

Introducción

Introducción

Contenido

8

Introducción

1. Qué es un SIEM?
2. Origen
3. SEM / SIM
4. Capacidades
5. Beneficios
6. Razones para utilizar un SIEM
7. Importancia de un SIEM
8. Es indispensable tener un SIEM?
9. Qué hay antes y después del SIEM?
10. Similitudes y diferencias básicas: Colector de log / Administrador de logs / Correlacionador / SIEM
11. Cuál es el fin de un SIEM?

Introducción

Qué es un SIEM?

9

Un sistema de **gestión de información y eventos de seguridad** (en inglés, security information and event management, SIEM) es un sistema que **centraliza el almacenamiento y la interpretación de los datos** relevantes de seguridad. De esta forma, **permite un análisis de la situación** en múltiples ubicaciones **desde un punto de vista unificado** que **facilita la detección de tendencias y patrones** no habituales. La mayoría de los sistemas SIEM funcionan desplegando múltiples agentes de recopilación que recopilan eventos relacionados con la seguridad.

Introducción

Qué es un SIEM?

Conjunto de herramientas que **ayuda a identificar** e **interpretar** de **forma eficiente** la **información relevante para el negocio** respecto a eventos de seguridad, **agregando valor** y ayudando a los equipos en la **respuesta** a los mismos **de forma tempestiva**.

Introducción

Origen

11

Un sistema **SIEM** combina funciones de un sistema de gestión de información de seguridad (*security information management*, **SIM**), encargado del **almacenamiento** a largo plazo, el **análisis** y la **comunicación de los datos** de seguridad, y un sistema de gestión de eventos de seguridad (*security event management*, **SEM**), encargado del **monitoreo en tiempo real**, **correlación de eventos**, **notificaciones** y **vistas de la consola** de la información de seguridad.

Introducción

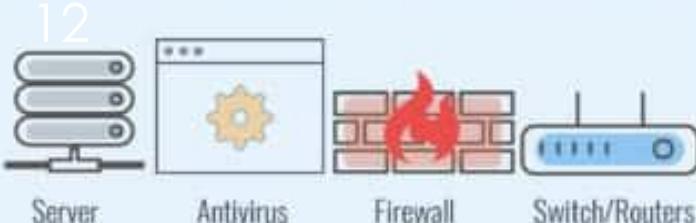
SEM / SIM

SIM VS SEM VS SIEM

SECURITY INFORMATION MANAGEMENT



SOFTWARE THAT AUTOMATES THE COLLECTION OF EVENT LOG DATA



Server Antivirus Firewall Switch/Routers

DATA GENERATED FROM NUMEROUS SOURCES



STRONG LOG MANAGEMENT CAPABILITIES

SECURITY EVENT MANAGEMENT



STRONG EVENT MANAGEMENT, REAL-TIME THREAT ANALYSIS,
VISUALISATION, TICKETING, INCIDENT RESPONSE, AND
SECURITY OPERATIONS



Oracle Database

DATA GENERATED FROM SQL/ORACLE DATABASES



POOR LOG MANAGEMENT CAPABILITIES

SECURITY INFORMATION AND EVENT MANAGEMENT

COMBINES SIM AND SEM CAPABILITIES



Introducción

SEM / SIM

	Security Information Management (SIM)	Security Event Management (SEM)	Security Information and Event Management (SIEM)
Overview 13	Collection and analysis of security-related data from computer logs.	Real-time threat analysis, visualization and incident response.	SIEM, as the name suggests, combines SIM and SEM capabilities.
Features	Easy to deploy, strong log management capabilities.	More complex to deploy, superior at real-time monitoring.	More complex to deploy, complete functionality.
Example Tools	OSSIM	NetIQ Sentinel	SolarWinds Log & Event Manager

Introducción

Capacidades

14

Las capacidades **básicas** y **más comunes** de un SIEM son :

- **Colecta de logs:** recolección de eventos de distintas fuentes y formatos
- **Normalización de datos:** unifica en un formato estándar, limpiando los datos para luego almacenarlos
- **Notificaciones y alertas:** gestión de avisos por distintos medios sobre configuraciones parametrizables
- **Detección de incidentes:** provee cierto grado de inteligencia para identificar amenazas de seguridad y su respectiva criticidad
- **Workflow:** facilita el seguimiento de eventos de seguridad que necesitan ser tratados



Introducción

Beneficios

Las herramientas SIEM proporcionan:

- Otorgan **visibilidad** en tiempo real
- Gestión unificada de **eventos de diversas fuentes**
- **Correlaciona eventos** recolectado de distintos orígenes
- Proporciona distintos tipos de **notificaciones, reportes y visualizaciones**

15



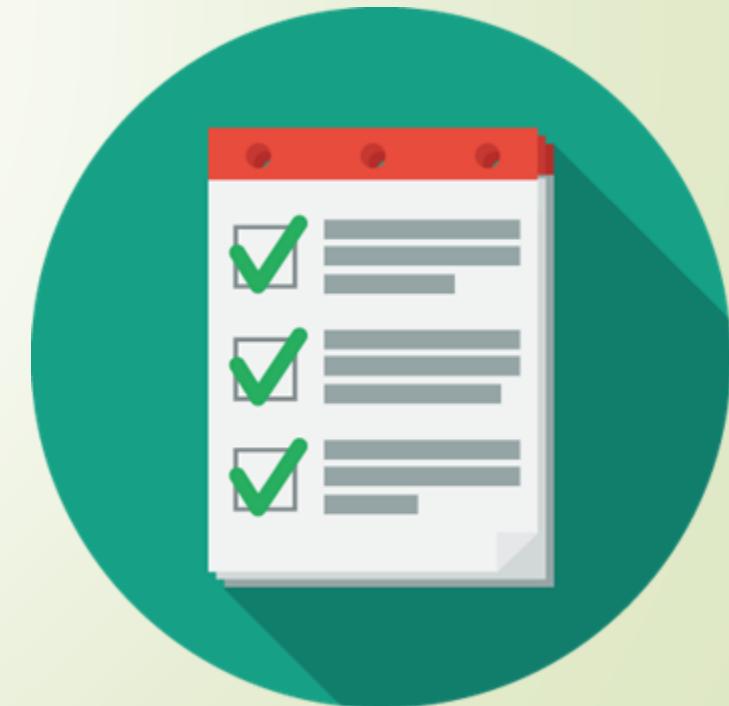
Introducción

Razones para utilizar un SIEM

16

Las razones pueden variar, las más comunes son:

- **Infraestructura heterogénea**
- Diversos **puntos de falla**
- Amplia **superficie de exposición**
- Elevada **exposición al riesgo**
- **Criticidad del negocio**
- Atendimiento **regulatorio**



Introducción

Importancia de un SIEM

17

- **Identificación temprana** de un **comportamiento anómalo**
- Permite **respuesta ante incidentes**
- Facilita el **soporte para casos forenses**
- Agiliza la **correlación de eventos**
- Ayuda con el **cumplimiento de normas** internacionales (ej. PCI, ISO 27000, HIPAA, GDPR)
- Permite la definición de **reglas de seguridad y del negocio**

Introducción

Es indispensable tener un SIEM?

La respuesta directa es **NO**, pero...

- Siempre depende de lo que necesitemos y busquemos.

La pregunta que debemos saber responder es:

- Cómo ayuda el SIEM a lograr los objetivos del negocio?

Introducción

Qué hay antes y después del SIEM?

19

- Orígenes/fuentes
- Datos
- Colectar
- Consolidar
- Agregar valor/información
- Correlacionar
- Interpretar/analizar
- Notificar
- Reporting
- Ejecución de acciones

• **SIEM**

- **SOC:** Security Operation Center
- **CSIRT:** Equipo de Respuesta ante Incidentes de Seguridad
- **War room:** equipo colegiado multidisciplinario donde se deciden las acciones cruciales

Introducción

Similitudes y diferencias básicas

20

- **Colector de log:** colecta, pero no lo gestiona ni analiza
- **Administrador de logs:** gestiona el almacenamiento y la depuración, no analiza ni correlaciona
- **Correlacionador:** consume del almacenamiento y las distintas fuentes para identificar información común, pero no analiza
- **SIEM:** es el conjunto de todas las herramientas anteriores, con capacidad de agregar inteligencia por medio de soluciones complementarias a fin de entregar información de valor

Introducción

Cuál es el fin de un SIEM?

Interpretar los datos de distintas fuentes y orígenes, para proveer información de valor que ayude a tomar decisiones y acciones tempestivas, para brindar soporte al negocio.

Funcionamiento

Funcionamiento

Contenido

Funcionamiento

1. Taxonomía de un SIEM (componentes)
2. Fases de implementación
3. Cuánto dura un proyecto maduro?

23

Funcionamiento

Taxonomía de un SIEM (componentes)



24



Funcionamiento

Fases de implementación

25

Step 1
Collect data from sources, finding all assets on your network.

Step 2
Aggregate and normalize collected data.

Step 3
Use analytics to examine data, looking for trends and suspicious behavior.

Step 4
Confirm security breaches enabling organizations to investigate and respond to threats.



Funcionamiento

Cuánto dura un proyecto maduro?

La respuesta directa es que **nunca** termina de madurar como tal, el SIEM más que una herramienta o solución, **es un proceso**. Los procesos **tienen vida propia y** por consiguiente **constantes cambios**.

26

La definición del **alcance es clave**, la **implementación por etapas** debe estar definida, pero puede sufrir cambios en virtud de la **necesidad del negocio**. Siempre hay nuevos orígenes, datos, necesidades; y como mínimo, un **constante tuning** de los colectores.

Principales características

Principales características

Contenido

Principales características

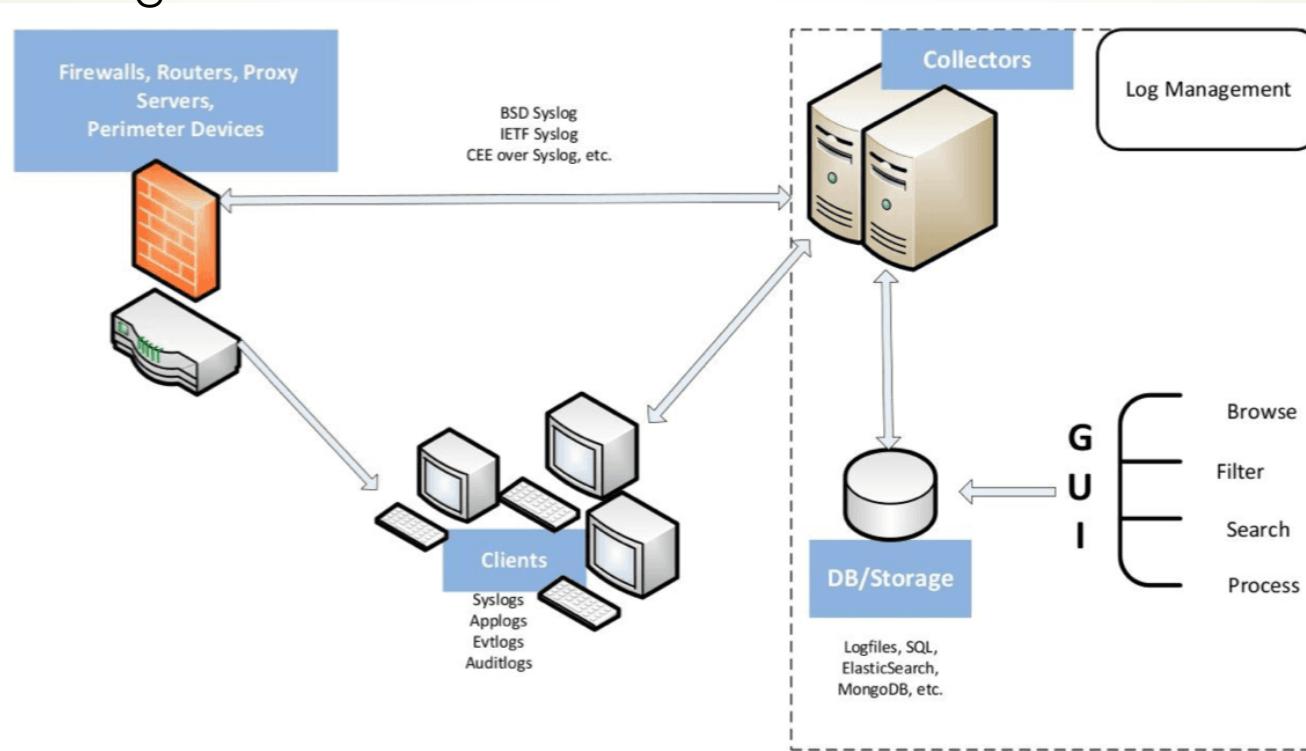
1. Gestión de logs
2. Importancia de la sincronización
3. Dashboards
4. Reportes
5. Informes
6. Notificaciones
7. Acciones
8. Correlación de criticidad
9. Análisis

Principales características

Gestión de logs

La **gestión centralizada de logs** es de suma importancia al momento de cruzar información, correlacionarla, realizar análisis forense online y offline, **identificar un rastro secuencial**, consolida eventos de **diversas fuentes y dispositivos**, agiliza el **análisis centralizado** sin recurrir a otros gestores de eventos, facilita la **resolución oportuna de incidentes** de seguridad.

29



Principales características

Importancia de la sincronización

La sincronización de los datos **es clave** al momento de correlacionarla, analizarla y generar información para la toma de decisiones, ya que **permite mantener la hora estandarizada entre distintos sistemas** que intervienen o son monitoreados por medio del SIEM.

30

Esto se logra por medio de un **servidor NTP** (Network Time Protocol), que a su vez puede estar sincronizado a un reloj atómico. Por lo tanto, ya no estarían afectados por ejemplo por las distintas zonas horarias.

Idealmente todos los servidores, appliance, bases de datos, dispositivos y sistemas deben estar configurados contra un NTP Server **desde su instalación**. Esto permitirá que la información que vaya al SIEM ya sea con una **marca de tiempo estandarizada**.



Principales características

Dashboards

Permite **visualizar de manera más directa** y ordenada los eventos importantes, a su vez la mayoría poseen la capacidad (previa configuración) de ir explotando los datos sobre los cuales queramos analizar en mayor profundidad, esta **granularidad permite detectar comportamientos anormales** de la red o **fallas en la colecta de información**.

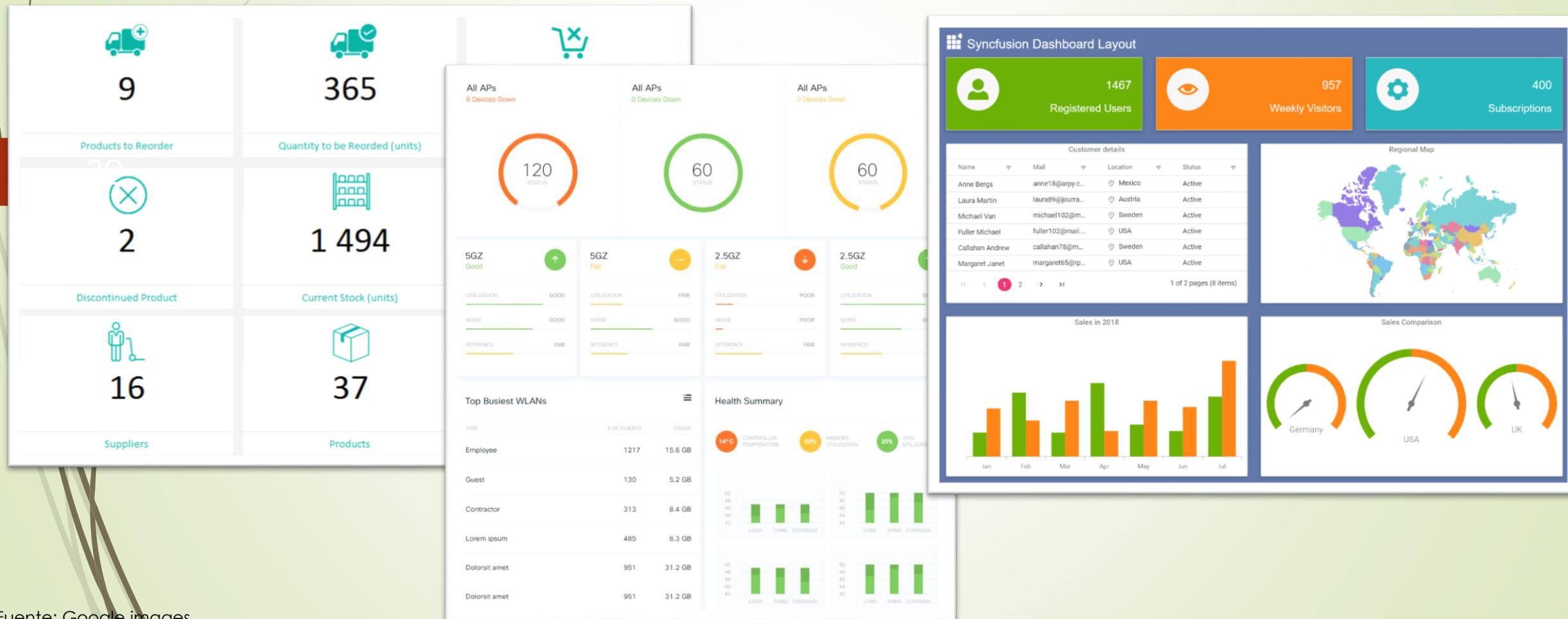
31

Cada solución cuenta con sus fortalezas, en general todas cuentan con facilidades en la utilización de **gráficos, números, porcentajes, indicadores, semáforos, mapas**, etc.

Principales características

Dashboards

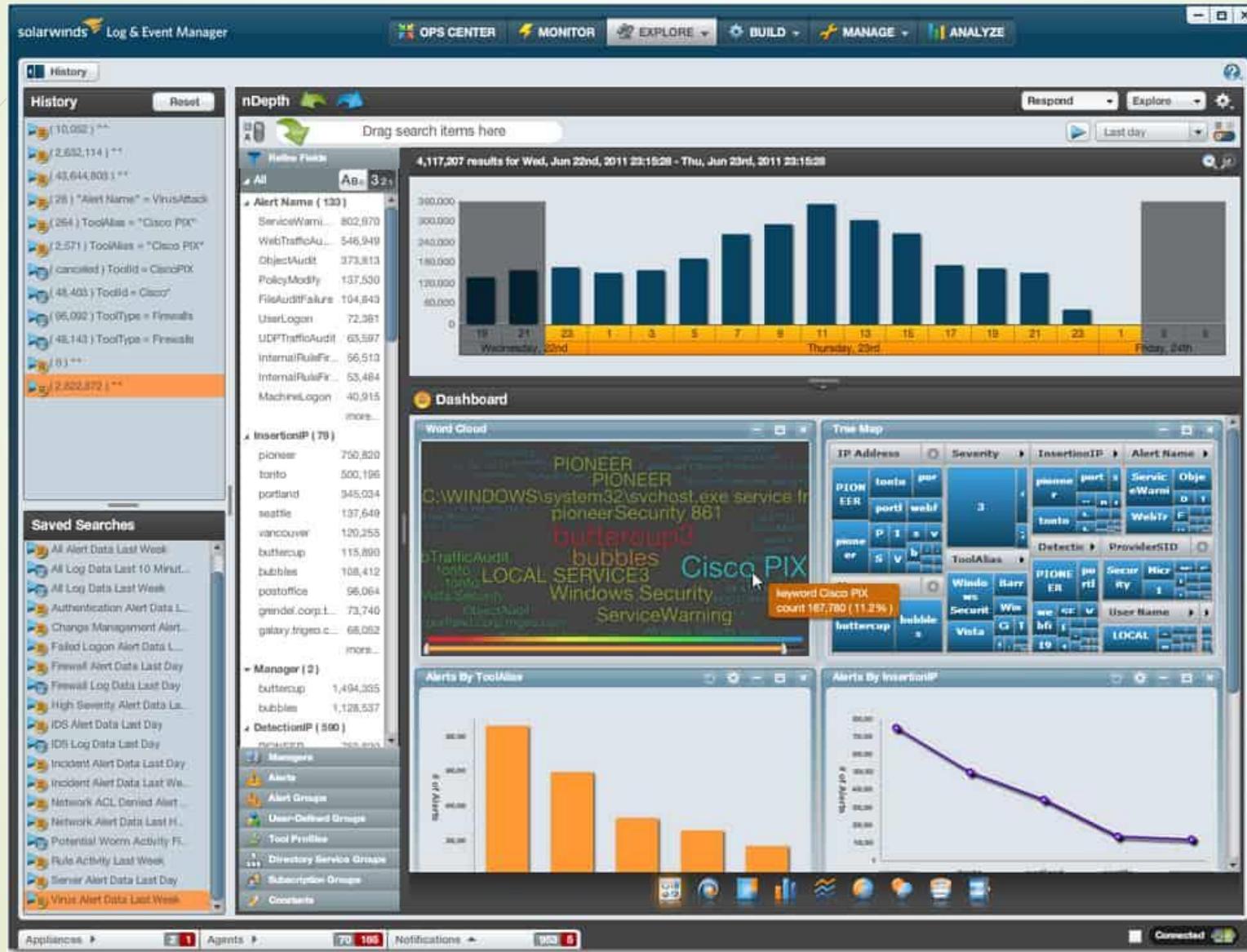
Sugerencia: debe ser **comprendible por cualquiera, mientras más simple, mejor.**



Principales características

Dashboards | SolarWinds Security Event Manager

33



Principales características

Dashboards | Micro Focus ArcSight Enterprise Security Manager (ESM)

The screenshot displays the ArcSight Console interface with the following components:

- Navigator:** Shows a tree view of resources and packages, with "Dashboards" selected. Under "Dashboards", there are categories like "admin's Dashboards", "Shared", "All Dashboards", "ArcSight Administration", "ArcSight Foundation", "ArcSight Solutions", "JumpStart", "LOGbinder", and "SP". Under "SP", "User Activity Event Graph" is highlighted.
- Viewer:** Contains three tabs: "Object Activity Summary", "Search Activity", "Security Changes", and "SharePoint Audit Snapshot". The "Object Activity Snapshot" tab is active, showing a table of audit flags by user. The "Audit Flag by User Snapshot" table shows the following data:

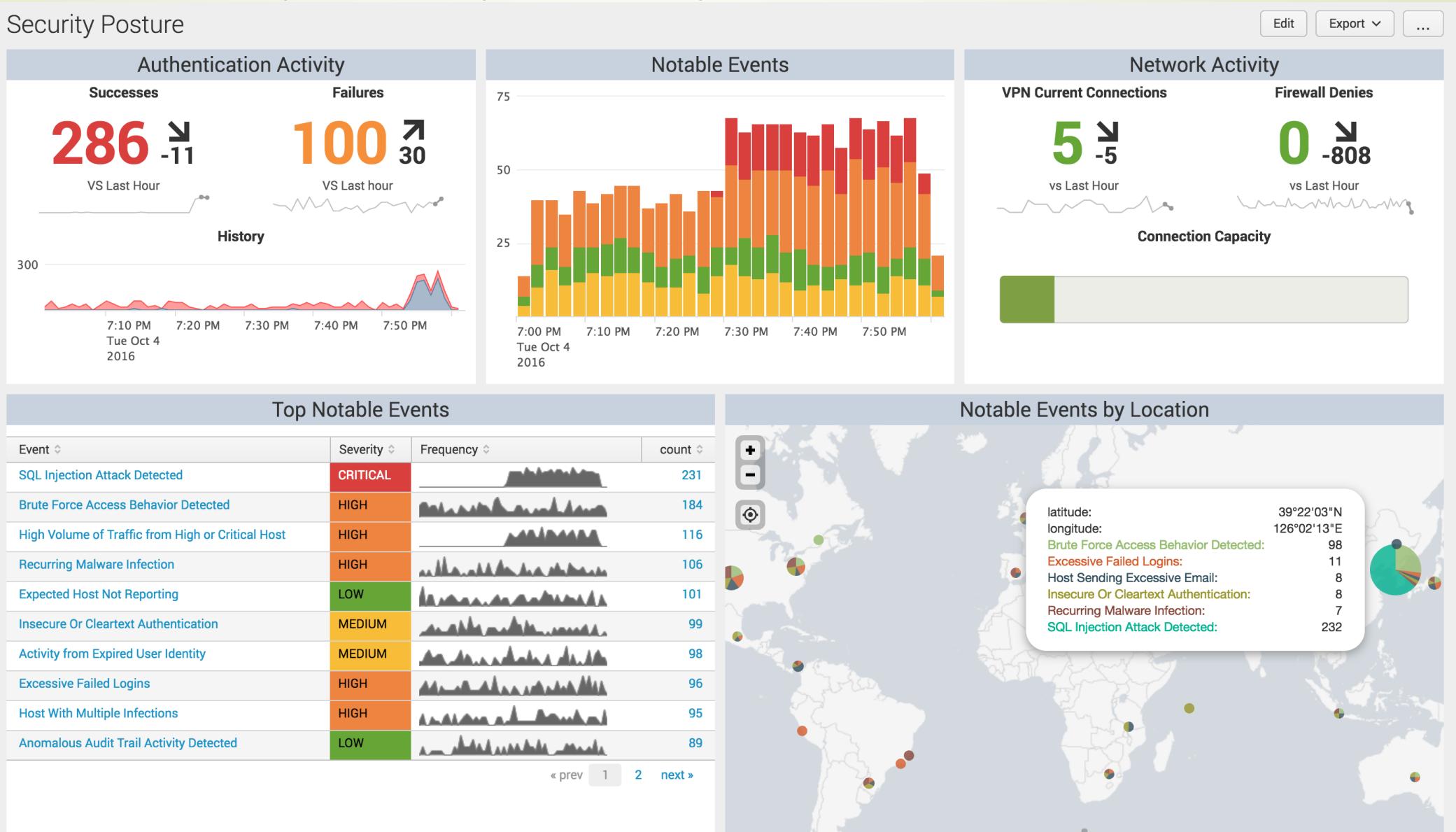
Target User Name Audit Flag	Total (Total Legends 21)
System Account SchemaChange	10901
System Account View	9174
System Account Update	1040
Richard Lowe View	309
John Lock View	307
Richard Lowe SecurityChange	241
System Account SecurityChange	241
John Lock SecurityChange	221
Richard Lowe Update	162
John Lock Update	161
Thomas Sydenham View	154

- Inspect/Edit:** Shows event details for a selected item: "List or Library Level Audit Policy Changed" with the annotation "Audit policy changed".

Principales características

Dashboards | Splunk Enterprise Security

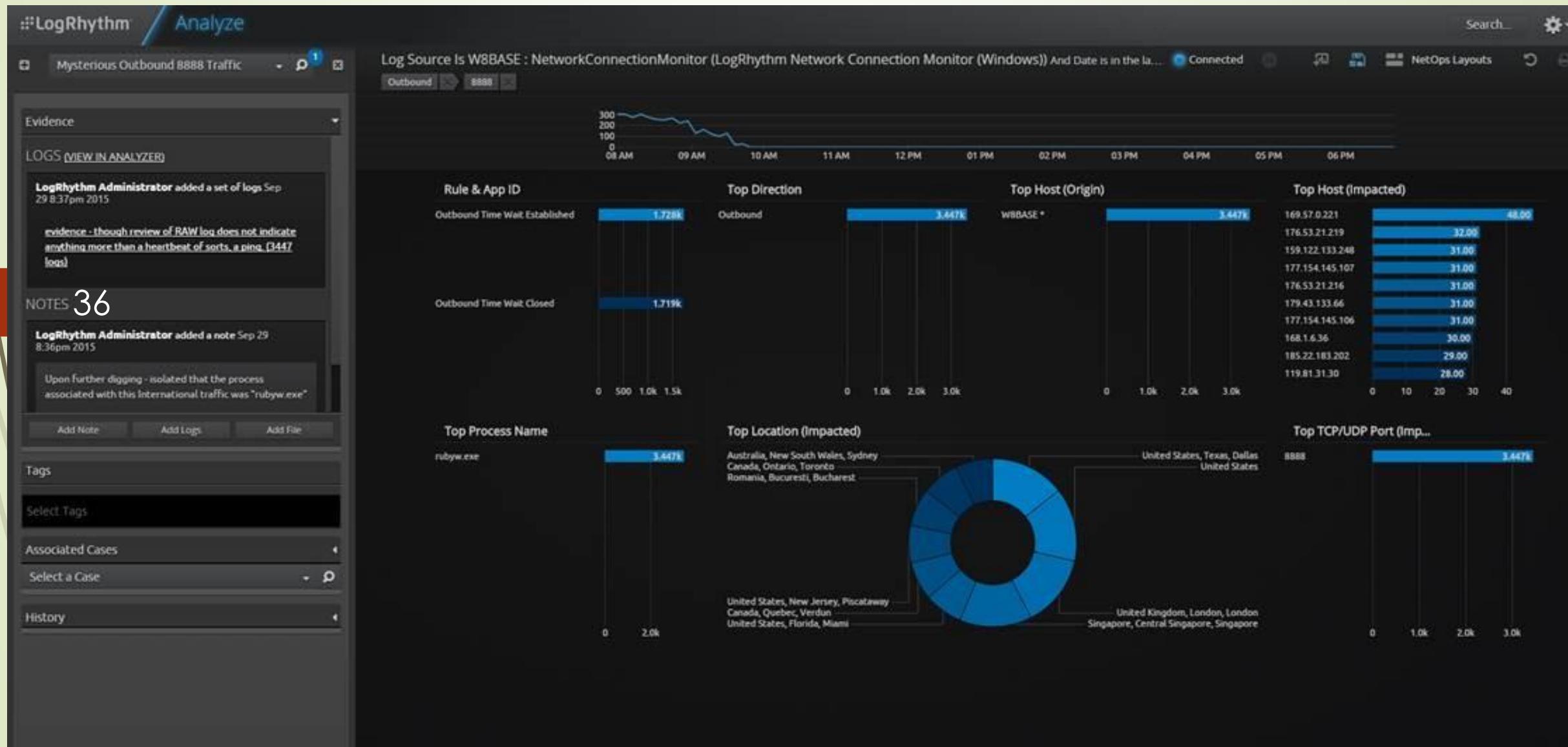
Security Posture



35

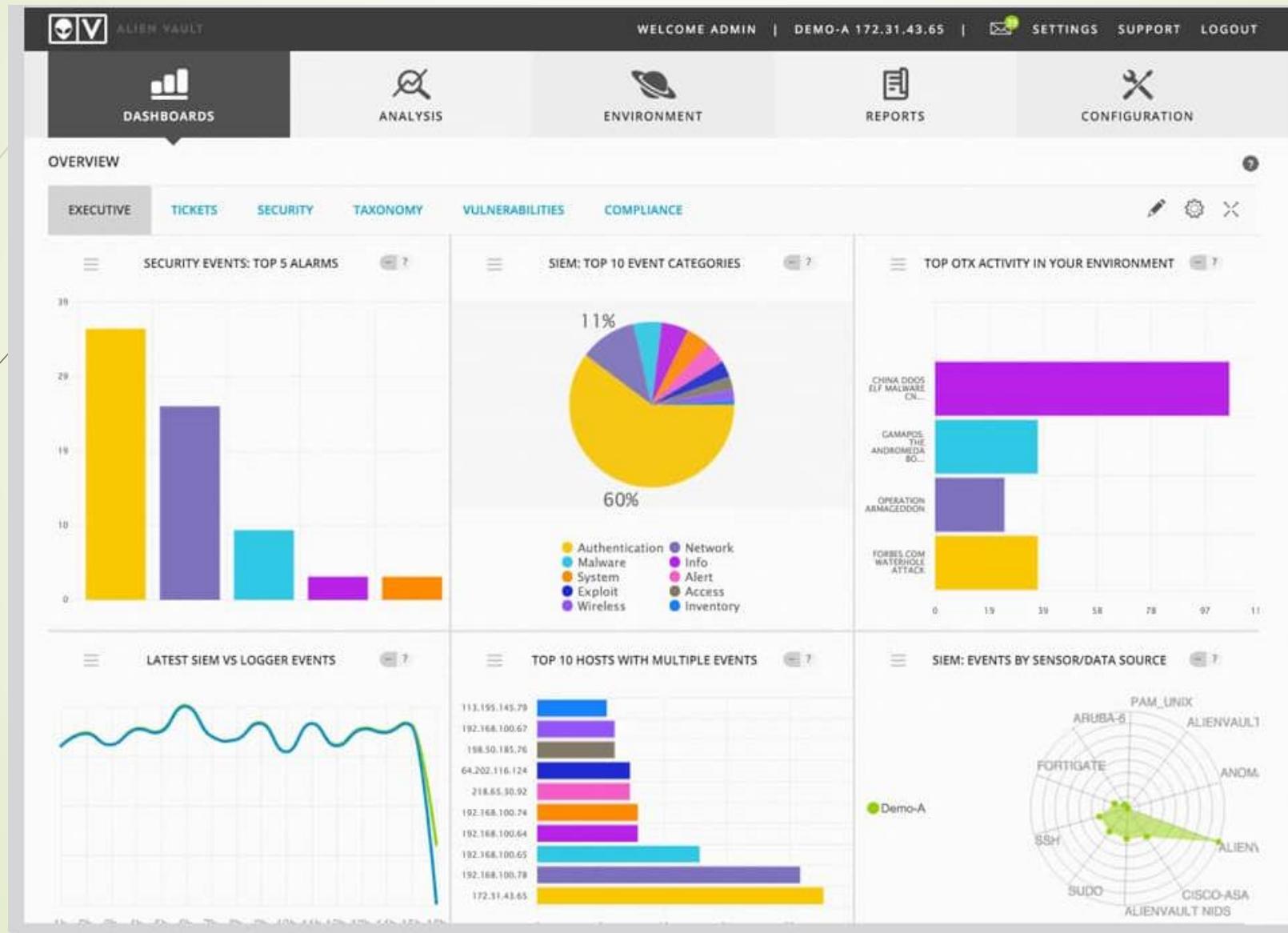
Principales características

Dashboards | LogRhythm Security Intelligence Platform



Principales características

Dashboards | AlienVault Unified Security Management



Principales características

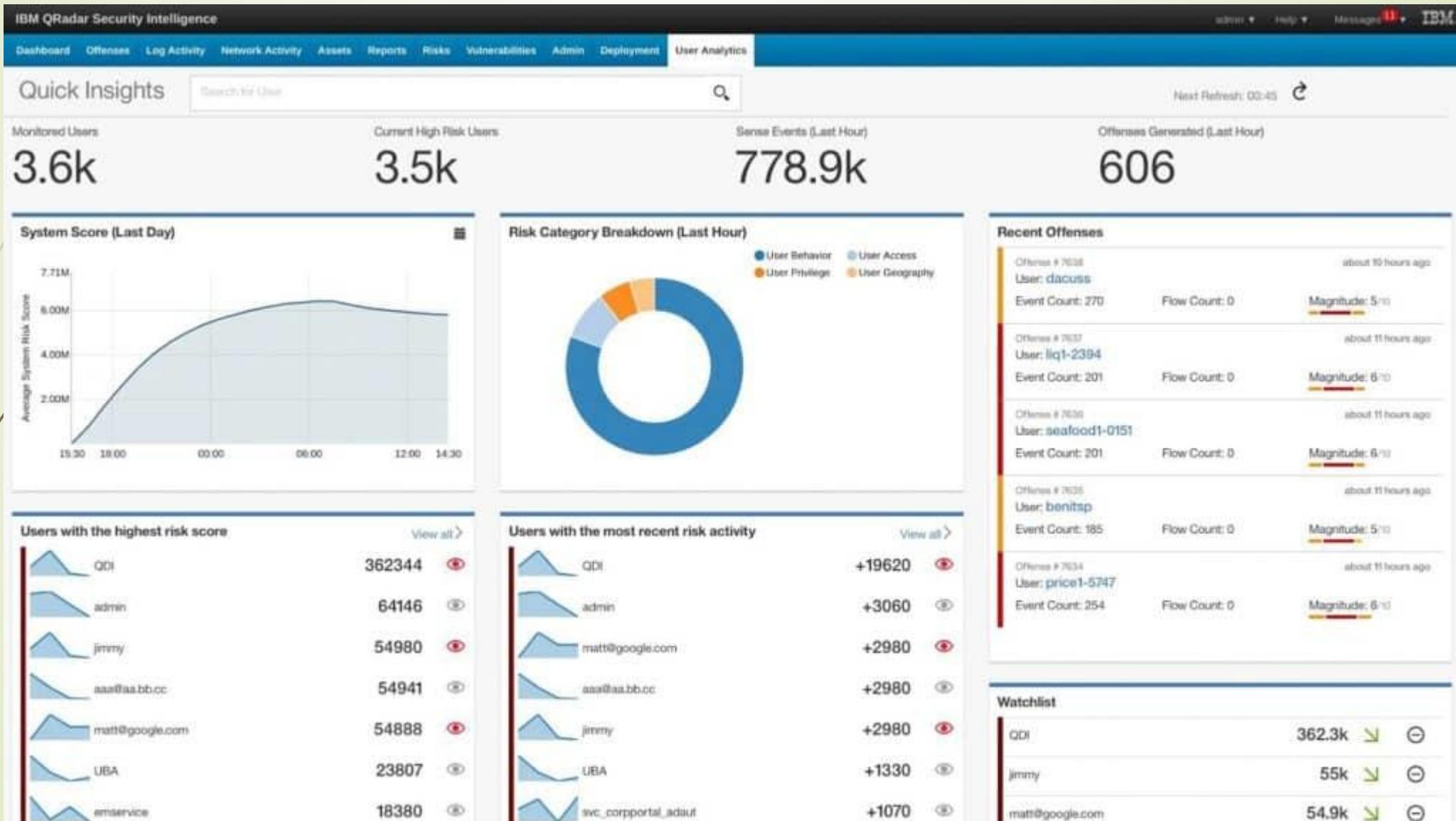
Dashboards | RSA NetWitness

38

The screenshot displays the RSA NetWitness Platform interface. At the top, there's a navigation bar with links for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below the navigation is a search bar showing results for "Broker" from "03/10/2017 19:41:00" to "03/10/2017 19:41:59". The main area is titled "All Events (1)" and shows a single network event from "03/10/2017 19:40:29" to "03/10/2017 19:40:29". The event type is "Network" and the source IP is "45.140.181.156". The event summary indicates it's a "New Service Broker" with a calculated packet size of 5410 bytes and a calculated payload size of 3579 bytes. The "Packet Analysis" tab is selected, showing detailed hex and ASCII representations of the captured traffic. To the right of the packet view is a sidebar with various service and action definitions, such as "ALIASIP", "EMAIL", "EMAIL.DEST", "EMAIL.SRC", "EMAIL.CONTENT", and "EMAIL.ACTIONS". The bottom of the interface shows pagination with "1 of 7 events" and "Selected 23 of 23 packets in current performance".

Principales características

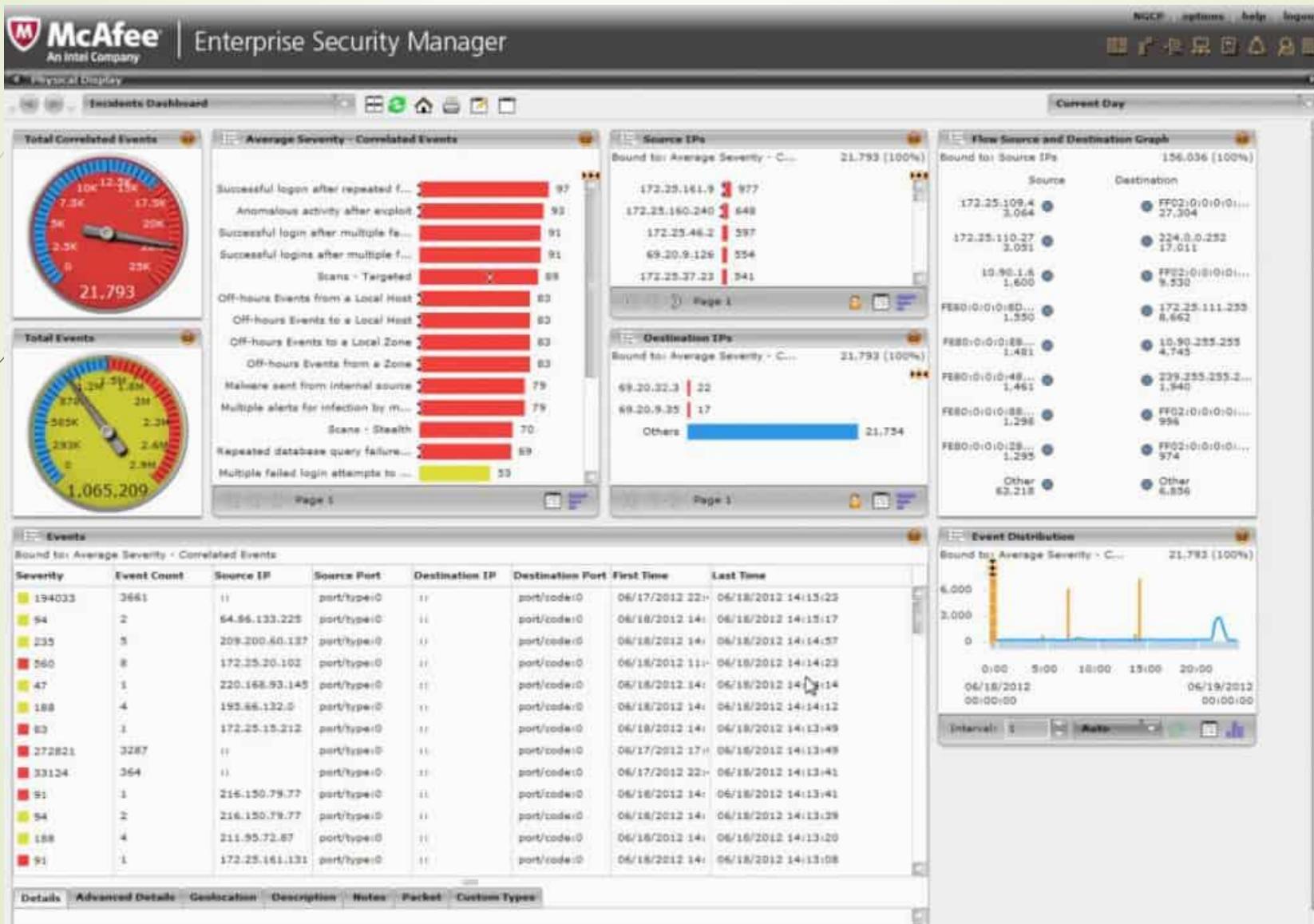
Dashboards | IBM QRadar



Principales características

Dashboards | McAfee Enterprise Security Manager

40

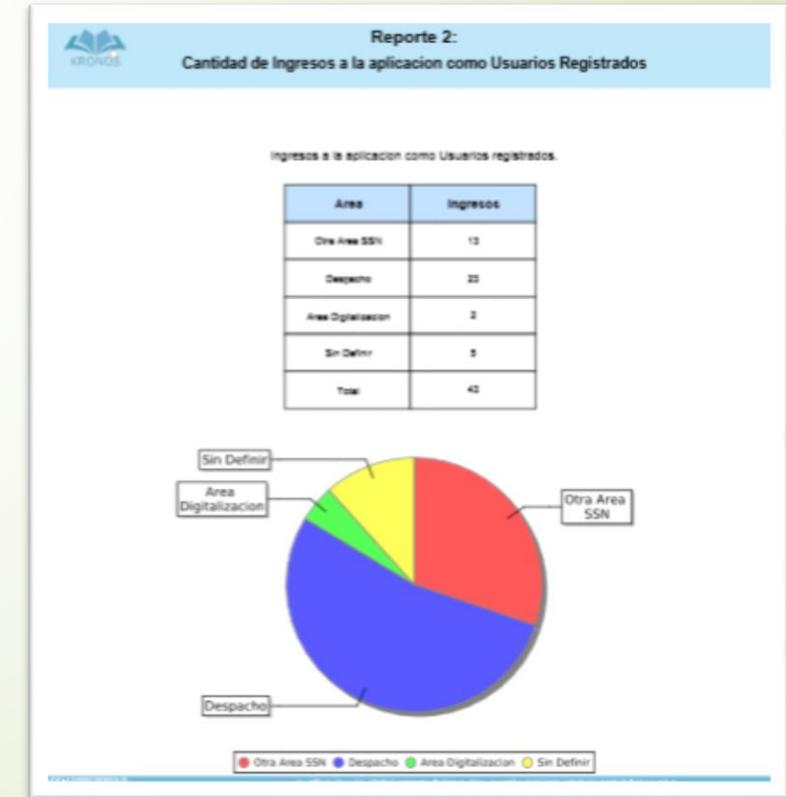
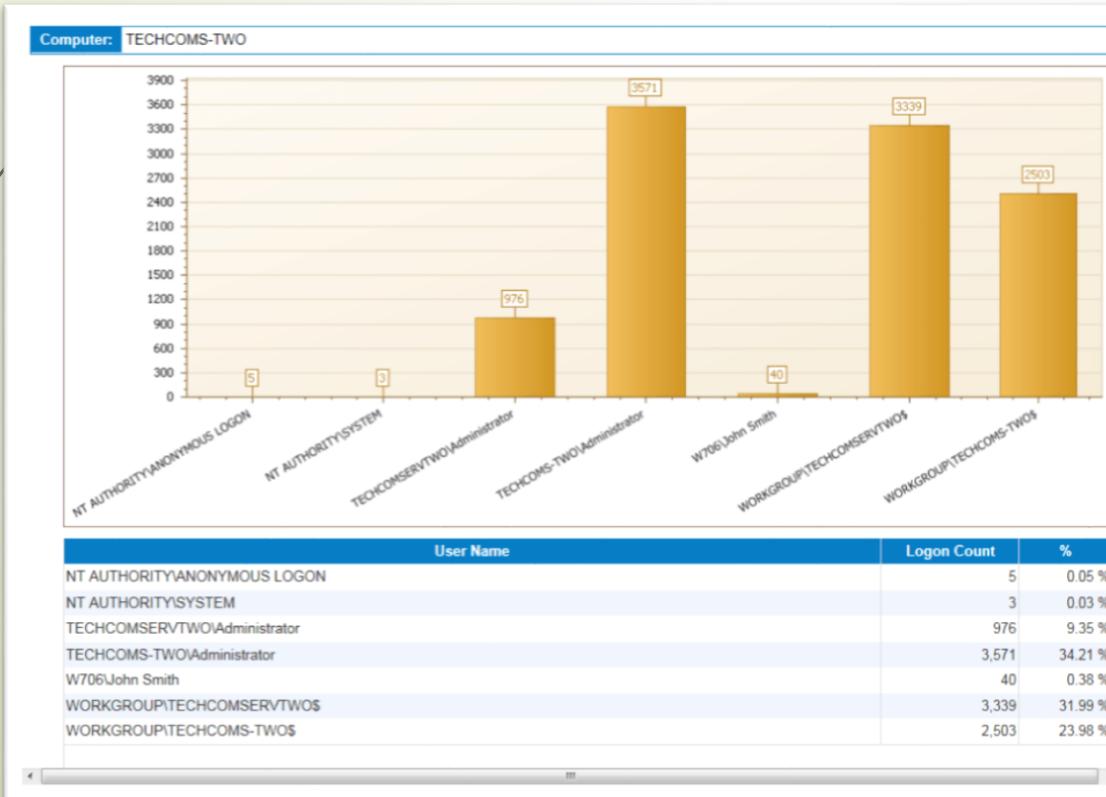


Principales características

Reportes

Los reportes deben ser **específicos, precisos, entendibles** y por sobre todo tener un **objetivo**. Características comunes: permiten **agendamientos o calendarizaciones**, aplicación de **filtros**, envío por **distintos medios y formatos**, etc.

41



Principales características

Informes

42

Ciertas soluciones permiten la emisión de **informes de cumplimiento** contra alguna **norma o estándar internacional**, ej. PCI, ISO 27000, HIPAA, GDPR , expresándolo en **% de adherencia** por dominio y pueden ser **calendarizadas**.

Esto ayuda principalmente al **respaldo y compliance** para la **norma específica**, así como nos ayuda a **identificar los puntos débiles** donde podemos realizar **ajustes o monitoreos más cercanos**.



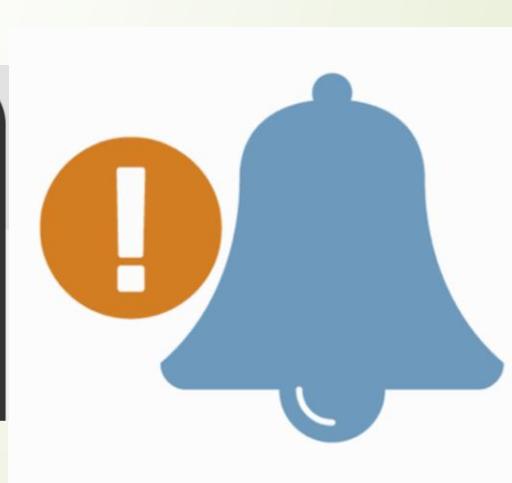
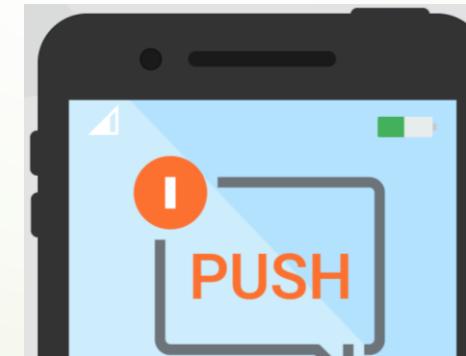
Principales características

Notificaciones

Una **funcionalidad esencial** de este tipo de solución, son las **notificaciones**. Las mismas tienen el objetivo de **alertar** sobre ciertas situaciones **definidas inicialmente**, lo que permite **accionar tempestivamente** ante algún incidente de seguridad.

Ej. e-mail, sms, push, llamadas, popup, sonidos, etc.

43



Principales características

Acciones

Entre las características más apreciadas y que **agregan valor** a las soluciones se encuentran las **acciones**, las mismas permiten realizar procesos de forma **reactiva inmediata** ante algún **evento específico**.

44

Ej.

- Ejecutar comandos
- Bajar servicios
- Bloquear tráfico
- Enviar notificaciones
- Iniciar workflow
- Etc.



Principales características

Correlación de criticidad

45

El objetivo de la **correlación por criticidad** es mantener una **independencia** y **guía** para **asignar una criticidad** a los eventos o conjunto de eventos. A su vez provee **nombres estandarizados** para vulnerabilidades y otras exposiciones de seguridad.



Principales características

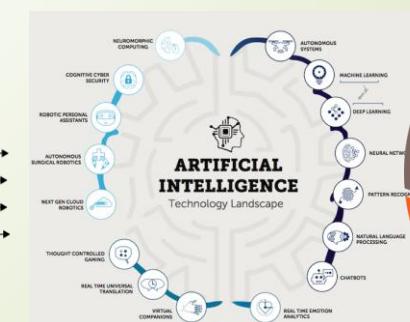
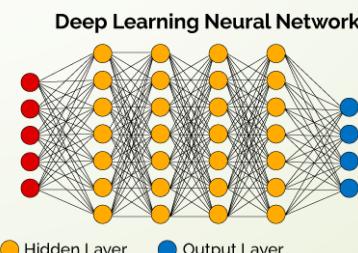
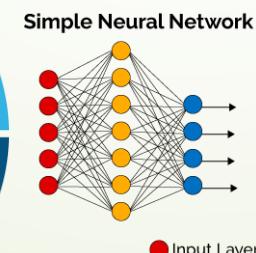
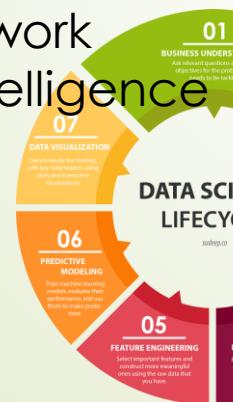
Análisis

46

Tal vez la funcionalidad más **destacable y deseada** sea la de **análisis**, donde **se aplica la inteligencia a los datos, obteniendo información**, pero que sea **de valor**, que **anticipe situaciones**, que **resuma eventos**, que **cuente la historia**, que **sugiera el mejor camino o acción a tomar..** podemos llamarlo como queramos, lo que necesitamos es **aplicar inteligencia a los datos.**

Ej.

- Data mining
- Deep learning
- Machine learning
- Data science
- Neural network
- Artificial Intelligence
- Big data



Qué monitorear?

Qué monitorear?

Contenido

Qué monitorear?

1. Criticidad
2. Apetito de riesgo y Tolerancia al riesgo
3. Conocer los objetivos estratégicos del negocio
4. Agregando valor
5. Definición de alcance
6. Activos críticos
7. Requerimientos

Qué monitorear?

Criticidad

Lo que es importante para mí, tal vez no es importante para el resto.

49



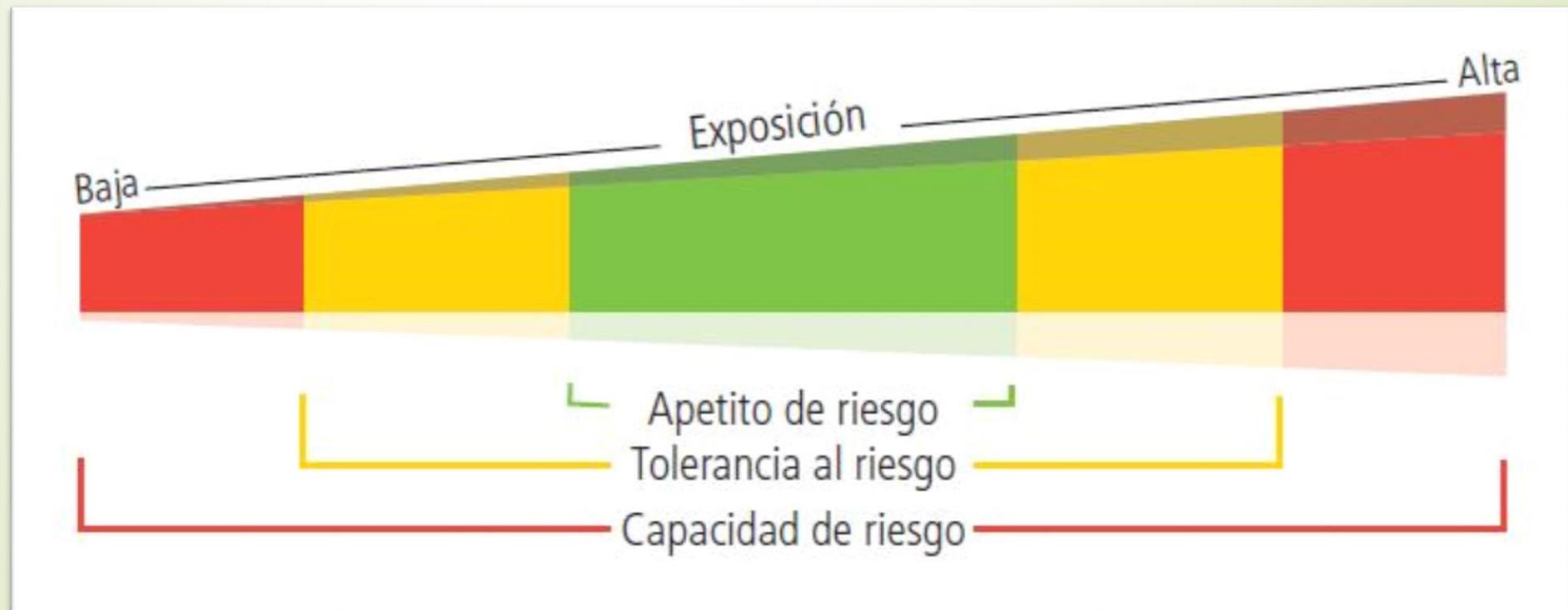
Qué monitorear?

Apetito de riesgo y Tolerancia al riesgo

Debo conocer:

- Cuáles son sus riesgos más relevantes?
- Cuáles son sus debilidades?
- Qué espera el negocio?
- Qué le interesa?

50



Qué monitorear?

Objetivos estratégicos del negocio

Siempre es **difícil explicar** la importancia de un SIEM para la **alta gerencia**, conocer los **objetivos del negocio** nos ayudará a poder **encarar el planteamiento** de forma que sea **interesante a los tomadores de decisión**, teniendo en cuenta que por lo general nosotros debemos **soportar las metas institucionales**.

51



Qué monitorear?

Agregando valor

Una de las maneras más comunes de **agregar valor** es la **formación de alianzas estratégicas**, con esto ganaremos la obtención de **apoyo de áreas internas**, por medio de lo que nosotros podemos hacer para ellos y que les **sume en la operativa**. Centrado siempre en **mostrar información importante para el negocio** (no para Seguridad).

52

No:

- Cantidad de virus detectados
- Cantidad de ataques recibidos
- Cantidad de nodos, sensores, dispositivos monitoreados

Ej.:

- Cómo le ayudo al negocio a ganar más?
- Cómo le ayudo a no perder dinero?
- Cómo ayudo a mejorar la disponibilidad?
- Cómo puedo sacar el jugo a la herramienta de análisis?



Qué monitorear?

Definición de alcance

No podemos hacer todo en un primer momento, los **recursos siempre son escasos**, debemos **priorizar**.

Ej. Segmento específico, servidores críticos, bases de datos más sensibles, infraestructura de borde, aplicaciones transaccionales, personas clave, etc.

53

Ley de Pareto



Qué monitorear?

Activos críticos

54

Para saber **qué monitorear primero**, debemos respondernos la siguiente pregunta: Qué es lo que me **entregaría más valor** o cuál es el **talón de Aquiles** de mi infraestructura **(negocio)**?

- Banco
- Manufactura/Industria
- E-commerce
- Procesadora
- Telco
- Farmacéutica
- Frigorífico
- Etc.



Qué monitorear?

Requerimientos

55

Determinar y prever lo que se necesita para la implementación de un SIEM es crucial para un **proyecto exitoso**.

Esquema

- On premise vs. Virtual vs. Cloud

S.O.

- Windows vs. Linux

Infraestructura

- Núcleos, RAM, Disco

Network

- Redes, puertos, sentidos

Tipo de origen

- Syslog, BD, txt, etc.

Dispositivos soportados

- Servidores, Bases de datos, Workstation, equipos de comunicación, etc.

Etc etc etc..

Orígenes de datos

Orígenes de datos

Contenido

Orígenes de datos

1. Infraestructura y aplicaciones
2. Fuente y formato
3. Depuración

Orígenes de datos

Infraestructura y aplicaciones

58

Infraestructura y aplicaciones

1. **Servidores / S.O.:** Windows, Linux, AIX
2. **Bases de datos:** Oracle, SQL Server, DB2, Postgres, MongoDB, MariaDB
3. **Equipos de seguridad:** Firewalls, IDS/IPS, WAF, AV, DLP, Anti-DDoS, Anti-Spam, Proxy, Honeypot, HIDS/HIPS, SIEM
4. **Red:** Routers, Switches, Access Point, Wirelesslan Controller
5. **Aplicaciones / Servicios:** Mail, Swift, DC, LDAP, VPN, File Server, FTP, AAA, Applications Server
6. **Workstation:** Windows, Linux, Mac
7. **Mobile:** Android, iOS, Windows phone
8. **Datos internos:** clientes, cuentas, productos, movimientos, inventario, etc.
9. **Etc, etc, etc..**

Orígenes de datos

Fuente y formato

Fuente y formato

1. Syslog
2. Bases de datos
3. Port mirroring
4. EventLogs
5. Agent / agentless
6. Plugins
7. WMI (Windows Management Instrumentation)
8. CMD
9. Xml
10. Snmp
11. Json
12. Scripts bash
13. Archivos planos (txt, csv, planillas)
14. Logs de sistemas operativos
- 15....

Orígenes de datos

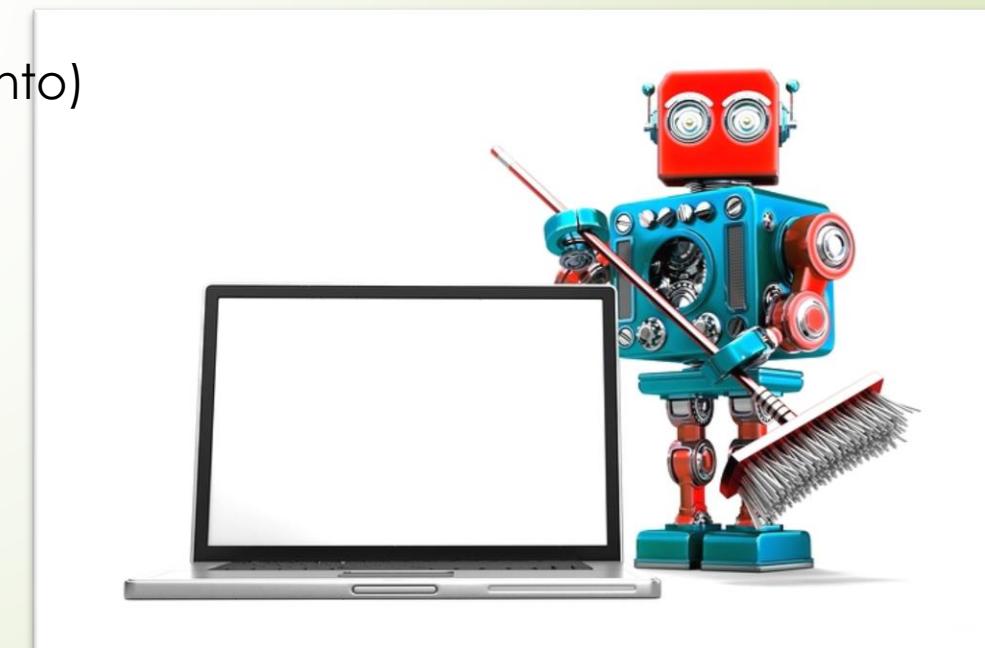
Depuración

El proceso de **depuración de logs** es tan importante como el mantenimiento al vehículo, cada cierto tiempo es necesario hacerlo para mantener su **funcionamiento en óptimas condiciones**, a fin de garantizar **espacio, velocidad y usabilidad**.

A depurar/limpiar:

60

1. Lo que no sirve (la basura)
2. Lo que no se va a usar (ej. imágenes)
3. Lo que no es importante (ej. el departamento)
4. Lo que ocupa espacio (ej. debug)
5. Lo muy antiguo (6 meses / 1 año)



Aseguramiento

Aseguramiento

Contenido

Aseguramiento

1. Accesos y perfiles
2. Auditoría
3. Replicación de eventos
4. Respaldos
5. Políticas de descarte
6. Política de depuración
7. Sincronización

Aseguramiento

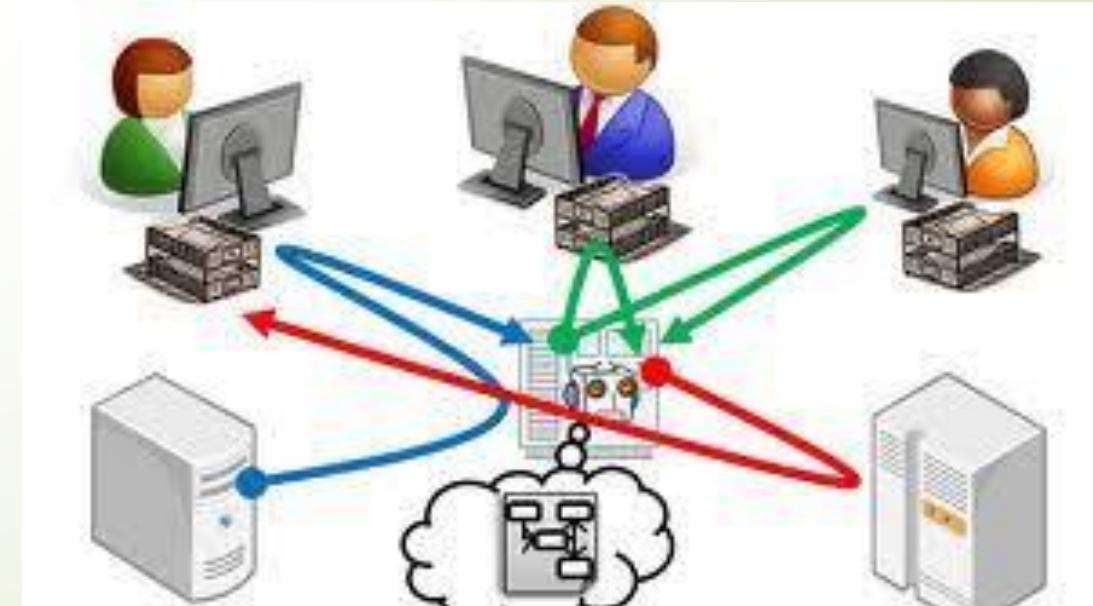
Accesos y perfiles

63

El **acceso al SIEM** debe estar **restringido** y **controlado**, siguiendo las directrices de:

- Red segmentada (ideal)
- Deber de saber
- Mínimo privilegio
- Perfilado
 - Sólo consulta/reportes
 - Monitores
 - Analistas
 - Administradores
 - ..

Obs: todos nominados, nada genérico



Aseguramiento

Auditoría

Uno de los aspectos más importantes desde el punto de vista del control, es que **todo debe ser auditabile**, para esto es importante garantizar que **toda la actividad sea registrada y respaldada**. En este sentido, los más elementales pueden ser:

1. Accesos
2. ABM de configuraciones
3. ABM de políticas

64



Aseguramiento

Replicación de eventos

Ante un **eventual ataque** durante el proceso de **borrado de huellas**, uno de los **objetivos primarios** son los **logs de los sistemas**, el **segundo objetivo** podría ser **el SIEM**, por lo tanto el SIEM también debe contar con una replicación de los eventos al igual que un servidor normal (ej. online, en cinta, locación distinta, etc.)

65



Aseguramiento

Respaldos

Las distintas herramientas que componen el SIEM **puede sufrir fallas**, para lo cual los respaldos también son importantes. Para ello (idealmente) se debe contar con **backups de configuraciones** y en lo posible también con **alta disponibilidad**.

66



Aseguramiento

Políticas de descarte

Las **políticas de descarte** básicamente hacen referencia a la **documentación de aquellos datos** que se van **a considerar en la ingesta y cuáles no se utilizarán**. Idealmente **los descartados** deben contar con una **justificación** para ello, es importante recordar que **todo el proceso debe ser auditabile**.

67

En términos amplios, puede considerarse al descarte como el proceso de separación de la paja del trigo. De aquellos **datos** que puedo **capturar**, realizo una **limpieza** y se **ingesta lo utilizable**.



Aseguramiento

Política de depuración

La **política de depuración** formaliza el proceso mediante el cual se analizarán los datos, revisando la necesidad puntual o experiencia, **eliminando aquello que no será de utilidad** con su debida **justificación** y **aprobación**, con qué **frecuencia** se realizará, si será **por demanda** o cuando se crea conveniente, **cuánto tiempo**atrás de dejará en el **acceso online** y el **offline**.

68



Aseguramiento

Sincronización

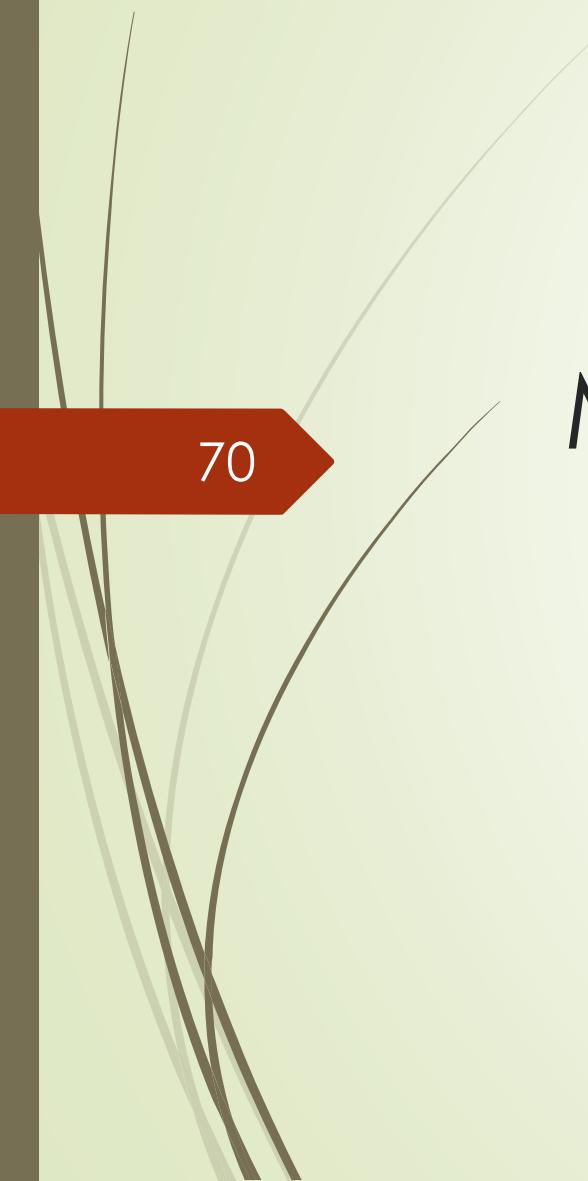
Como vimos anteriormente, la **sincronización de los eventos** ayuda a **correlacionar las acciones** capturadas, **permitiendo su análisis y tomar decisiones** en base a las mismas.

Desde el **punto de vista del control**, la sincronización **brinda trazabilidad** a los eventos registrados, logra una **mejor interpretación y coherencia con el contexto**.

69

Al igual que lo anterior, desde el **punto de vista legal y jurídico**, permite ser **respaldo forense** complementando las evidencias propias presentadas en un juicio.





70

Monitorear el SIEM

Monitorear el SIEM

Contenido

Monitorear el SIEM

1. Disponibilidad del SIEM
2. Performance
3. Revisión de accesos
4. Disponibilidad de orígenes
5. Ingestas
6. Tuning

Monitorear el SIEM

Disponibilidad del SIEM

Parece **básico** y por lo tanto **lo dejamos de lado**, pero es importante conocer si el SIEM está trabajando como debiera:

- Envía los **reportes programados**
- Realiza las **notificaciones**
- El servidor cuenta con los **parches actualizados**
- Presenta alguna **alerta**
- Etc.

72

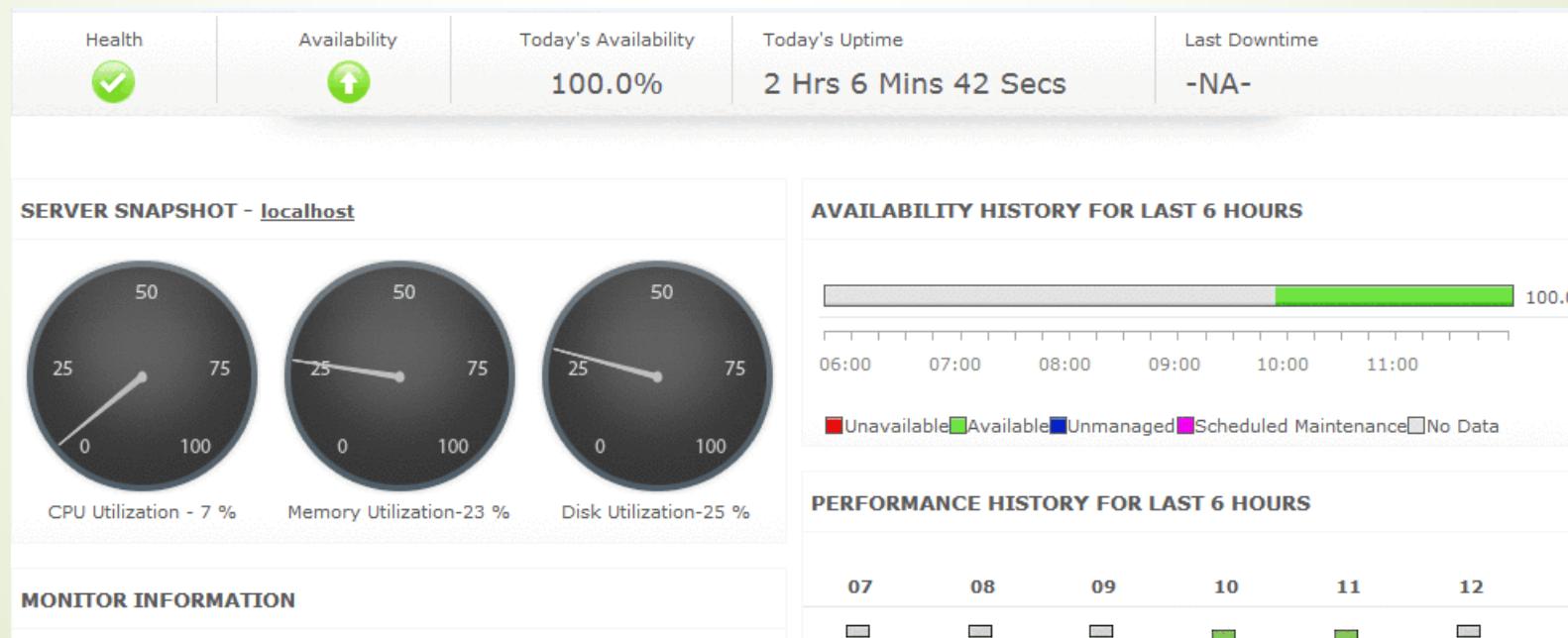


Monitorear el SIEM

Performance

El **desempeño de las herramientas** que componen el SIEM no deja de ser una información importante por mirar. El **consumo excesivo de recursos** o **elevado nivel de procesamiento**, podría indicar la **necesidad de revisión de los recursos** asignados al servidor, de un **tunning en las configuraciones**, **mejorar la ingesta** de logs o también un **ataque** en progreso.

73



Monitorear el SIEM

Revisión de accesos

Los accesos concedidos inicialmente **no son eternos** y pueden sufrir más cambios de los que uno quisiera. Para ello una **revisión y validación periódica** sería lo recomendable para garantizar que todos estén cumpliendo con la **debida necesidad de conocer y nivel de acceso**, también descubrir **si hubieron rotaciones**, si solicitaron el acceso pero **no lo utilizan**, si la dirección de **correo sigue siendo la misma**, etc.

74



Monitorear el SIEM

Disponibilidad de orígenes

75

Las cosas pasan, los servidores, BD's, dispositivos, etc. dejan de funcionar adecuadamente. Por ello, también es importante tener un **monitor hacia las fuentes de los logs**, para saber si:

- Están **activos**
- Si envían el **caudal** de datos **habitual**
- Si se **cambió de IP/Nombre**
- Si se encuentra en **mantenimiento**
- Si se **descartó**
- Etc.



Monitorear el SIEM

Ingestas

La salud del SIEM puede verse afectada por un **inadecuado dimensionamiento** de los **recursos**, así como factores externos como la **habilitación del debug** en algún **servidor o aplicación**, provocando un crecimiento excesivo de las ingestas.

En este escenario, **los logs** deberían **volver a la normalidad**, los **recursos deben ser adecuados**, o bien, **iniciar un proceso de depuración** de las mismas.

76



Monitorear el SIEM

Tunning

Todos los aspectos relacionados a la **alteración de la configuración** propia del funcionamiento del SIEM lo catalogamos como **tunning**.

Las configuraciones en general tampoco se mantienen así eternamente, se **van modificando de acuerdo a la necesidad**, del **negocio**, de **desempeño**, por **necesidades nuevas**, por se **eliminan ciertos reportes o destinatarios**, porque **surgen nuevos activos**, etc.

77



Comparativo de soluciones

Comparativo de soluciones

Contenido

Comparativo de soluciones

1. Por dónde empiezo?
2. Free o pagas?
3. Gartner

Comparativo de soluciones

Por dónde empiezo?

- Identificar la necesidad
- Identificar los activos relacionados
- Identificar factibilidades de obtención de logs
- Verificar requisitos de infraestructura
- ...

80

Comparativo de soluciones

Free o pagas?

81

SIEM VENDOR	THREATS BLOCKED	SOURCES INGESTED	Top SIEM Vendors			IMPLEMENTATION	MANAGEMENT	SUPPORT	SCALABILITY
			BEST	VERY GOOD	GOOD				
splunk > ES	••••	•••	•••	•••	•••	••	•••	••	•••
#LogRhythm™ ENTERPRISE	•••	••••	•••	••	••	•••	•••	•••	••
AV USM ALIEN VAULT	•••	•••	•••	••••	•••	•••	••	••	•••
MICROFOCUS ArcSight	••	•••	•••	••	••	•••	••••	••	•••
MICROFOCUS Sentinel	••	••	••	•••	•••	•••	•••	••	•••
McAfee® ESM	•••	•••	•••	•••	•••	••	••	•••	•••
Trustwave® SIEM	•••	•••	•••	•••	•••	••	•••	••	••••
IBM QRadar	•••	•••	••••	•••	•••	••	•••	•••	•••
RSA NetWitness	••	••	•••	••	••	••	••	•••	•••
solarwinds LEM	••	•••	••	••	••••	••	•••	••	••

SOURCE: eSecurityPlanet.com

Comparativo de soluciones

Free o pagas?

Esquema ELK

Elasticsearch: almacenamiento, búsqueda y análisis

Logstash: colector de eventos

Kibana: visualización

82



elastic



Comparativo de soluciones

Gartner

83





84

Resumen

Resumen

Contenido

Resumen

1. Necesito un SIEM?
2. Lo que importa (saber qué queremos buscar, encontrar, monitorear, reaccionar)
3. Identificar activos críticos
4. Cuál es mejor Vs. cuál me conviene?
5. Comprensible: mientras más simple, mejor
6. Por default todo debe tener logs (activados)

Bibliografía

Bibliografía

Contenido

- https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_informaci%C3%B3n_y_eventos_de_seguridad
- <https://www.comparitech.com/net-admin/siem-tools/>
- <https://phoenixnap.com/blog/siem-security-information-event-management-tools>
- <https://www.esecurityplanet.com/products/top-siem-products.html>
- Google images
- Diseño e Implementación de una solución de gestión centralizada de logs de aplicaciones, sistemas y dispositivos basada en Logstash que permita la creación de cuadros de mando para explorar, analizar y monitorear eventos de seguridad (Byron Alfonso Carrión Ramírez)
- Implementación de un gestor de seguridad de la información y gestión de eventos (SIEM) (Juan David Pedroza Arango)

Trabajo práctico

Trabajo práctico

Generalidades

89

Generalidades

1. **Ejercicio grupal:** 4 personas c/u
2. **Objetivo:** definir la estrategia de implementación de un SIEM de acuerdo al rubro asignado y escenario establecido
3. **Enfoque:** concreto, al punto, sin vueltas y coherente
4. **Extensión:** máximo 5 páginas/slides
5. **Formato:** docx, xlsx, pptx, pdf
6. **Nota:** 100% de la puntuación asignada (a definir)
7. **Entrega:** hasta el sábado 20/07 23:59 hs.
8. **email:** lucaslagrave@gmail.com

Trabajo práctico

Rubros

Rubros:

1. Banco
2. Manufactura/Industria
3. E-commerce
4. Procesadora
5. Telco
6. Farmacéutica
7. Frigorífico
8. Hospital
9. FFMM
10. Justicia/Fiscalía
11. Comisión de Valores
12. Aduana
13. Energía
14. Institución gubernamental

90

Trabajo práctico

Desarrollo

91

Grupo

- **Nro. de grupo:**
- **Integrantes:**
- **Rubro:**

Escenario (30%)

- **Contexto:** cómo se llama la empresa y a qué se dedica (3 líneas, breve)
- **Objetivos del negocio:** cuáles son? (mínimo 3)
- **Servicios externos:** posee servicios publicados externamente? No / Sí (cuáles?)
- **Servicios críticos:** cuáles son los servicios críticos de la misma? (mínimo 4)
- **Información crítica:** cuáles son las informaciones más sensibles que posee o gestiona?
- **Nivel de exposición al riesgo:** regulatorio, financiero/liquidez, reputacional, operativo, mercado, crediticio, etc.

Trabajo práctico

Desarrollo

92

Definir alcance (50%)

- **Activos críticos:** identificar cuáles son
- **Colecta:** qué tipo de información colectar
- **Objetivo:** qué queremos buscar, encontrar, monitorear o reaccionar?
- **Indicadores:** cuáles son las mediciones clave que nos interesan (mínimo 10)
- **Visualización:** por qué medios se tendrá acceso a los indicadores y con qué frecuencia (dashboards, reportes, informes, notificaciones)
- **Valor agregado:** cómo el SIEM agregará valor a otras áreas del negocio? (mínimo 2 ejemplos)
- **Política de depuración:** definir tiempo online / offline y frecuencia de revisión de logs e ingestas

Requerimientos (20%)

- **Infraestructura:** definir infraestructura necesaria (redes, servidores, bases de datos, monitoreo, etc.)

SIEM (Security Information & Event Management)

GRACIAS!!

93

Ing. **Lucas Lagrave**

MBA, CISA, CISM, CAMS, OpRM

lucas.lagrave@itau.com.py

Banco Itaú Paraguay SA

lucaslagrave 

lucaslagrave@gmail.com 