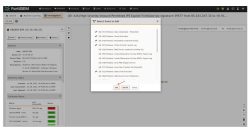
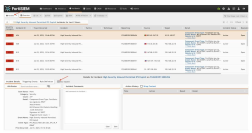
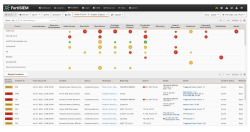
Guia Preventa - Product Tour (SOC)

Storytelling SOC (5 minutos)

⏱️ ***Duración estimada: cada bloque toma entre 35 y 45 segundos, sumando en total unos 5 minutos con ritmo fluido.***

Pantalla	Speech (para presentar)	Tarjetas (mini-storytelling autónomo)
1 – Dashboard General: Risk Score y Timeline 	"En nuestro SOC comenzamos con una visión global. El tablero muestra la evolución del riesgo en burbujas: cuanto más grande y roja, mayor el impacto. También monitoreamos accesos exitosos y fallidos, y detectamos usuarios con intentos sospechosos. Esto nos da un panorama completo: del riesgo global, hasta el ataque puntual y el comportamiento de los usuarios. En el Incident Timeline vemos incidentes en tiempo real, como un ataque al ERP.	🔮 El tablero muestra la evolución del riesgo en tiempo real: cada burbuja refleja un incidente y su severidad. Así priorizamos lo más crítico de un vistazo. 👤 Tambien Vigilamos logins exitosos y fallidos para identificar cuentas comprometidas y accesos sospechosos antes de que se conviertan en una brecha. 🚨 En el timeline detectamos intentos de explotación de alta severidad sobre sistemas clave como el ERP, con todo su contexto para iniciar la investigación.
2 – Incident Risk View 	"Al hacer clic en el ataque al ERP, entramos en el detalle del incidente. Vemos su ID, el número de veces que ocurrió, el origen, el destino y la descripción técnica. Pasamos de un dato general a un diagnóstico puntual y accionable."	🔎 Al abrir el incidente, vemos su ID, origen, destino y cuántas veces se disparó. Esto convierte una alerta general en un diagnóstico preciso y accionable.
3 – Triggering Events 	"Aquí analizamos los eventos que originaron la alerta. FortiSIEM muestra el log original y los datos normalizados, lo que nos permite confirmar la actividad maliciosa y reducir falsos positivos."	📜 Analizamos los eventos que dispararon la alerta: tanto el log original como los datos normalizados. Así validamos el ataque y reducimos falsos positivos.

4 – Investigate (Mapa de relaciones) 	“Con un clic entramos en la investigación visual. El mapa conecta el incidente con direcciones IP externas y sistemas internos, ayudándonos a entender de dónde viene el ataque y qué activos están comprometidos.”	🕵️ El grafo conecta sistemas internos con direcciones externas, mostrando de dónde viene el ataque y qué activos podrían estar comprometidos.
5 – Related Incident  s	“Los ataques rara vez son eventos aislados. Sumamos incidentes relacionados para entender si forman parte de una campaña más amplia. Esto nos permite anticipar movimientos del atacante y descubrir patrones.”	🔗 Los ataques rara vez son aislados: vinculamos incidentes relacionados para detectar campañas más amplias y anticipar movimientos laterales.
6 – Context 	“Aquí vinculamos la información del incidente con el inventario de activos (CMDB). Así sabemos si el ataque afecta sistemas críticos como un ERP o servidores financieros, y priorizamos la respuesta según el impacto en el negocio.”	🏢 Integramos la CMDB del cliente para saber si el ataque afecta activos críticos como ERP o servidores financieros, priorizando según impacto real en el negocio.
7 – Incident  Overview	“En esta vista obtenemos una radiografía completa: incidentes agrupados por severidad, tipo, frecuencia y hosts más impactados. Es un panel pensado también para clientes, porque entrega información clara y ejecutiva.”	📊 Nuestro equipo tiene una visión panorámica de incidentes por severidad, frecuencia y hosts impactados. Una radiografía clara para informar a nuestros clientes
8 – Incident List View 	“Esta es la vista operativa del SOC. Aquí nuestros analistas gestionan todo el ciclo de vida del incidente: correlacionan eventos, ejecutan playbooks, documentan hallazgos y coordinan la remediación. Es el corazón de nuestra operación diaria.”	⚙️Aquí los analistas actúan: analizan eventos correlacionados, documentan hallazgos e informan incidentes en tiempo real para tomar acciones de contención.
9 – Explorer, UEB  A y MITRE ATT&CK	“Finalmente, usamos vistas avanzadas como MITRE ATT&CK para mapear tácticas y técnicas utilizadas por el atacante y mostrar cómo fueron bloqueadas. Incluso en entornos industriales (OT/ICS), ofrecemos la misma cobertura y visibilidad.”	🛡️ Mapeamos cada ataque contra MITRE ATT&CK para mostrar qué tácticas se usaron y cómo fueron contenidas, incluso en entornos industriales (OT/ICS).