Tipos de dashboards recomendados

1. Threat Intelligence
2. Security Suite
3. Network
4. Alert
5. Application Server
6. System Events
7. Guest Access
8. Database Control
9. Identity Management
10. File Access Control

1. Threat Intelligence
Esta categoría debe de tener dos pantallas. Proporcioná información sobre la clasificación de los mensajes de amenazas, las direcciones IP externas de origen y destino maliciosos, la gravedad de la inteligencia sospechosa, las fuentes / destinos de amenazas más activos, el análisis de tiempo y los recuentos de actividades maliciosas.

2. Security Suite
Esta categoría tiene seis paneles: análisis de ataques, análisis de endpoints, descripción general de seguridad, IDS, análisis de filtrado de contenido y Trend Micro.

Widgets de información
Análisis de ataque
Ataque la actividad mediante direcciones IP de origen internas / externas, puertos de destino, interfaz de origen, países de origen y cronograma
Análisis de punto final
Fuentes infectadas, detalles de amenazas, virus detectados y eventos de seguridad de endpoints
Resumen de seguridad
Actividades de seguridad, riesgo por fuentes de eventos, resumen de riesgos por gravedad, resumen de riesgos por país de origen / destino, junto con actividades detectadas para ataques, malware, virus y spam
IDS
Histograma de ataque, ataque por direcciones IP de origen / destino, mapa de ataque de destino / origen y gravedad del ataque IP externo / interno
Análisis de filtrado de contenido
Acceso al dominio permitido / bloqueado, categorías permitidas / bloqueadas, fuentes de URL permitidas / bloqueadas y categorías de URL
ESET

Productos ESET o la consola, información de mapas de eventos, tipos de eventos, actividades de eventos, subtipos de eventos, entre otra información relacionada con eventos (la consola genera estos eventos actualmente)

3. Network
En esta categoría se podrían mostrar algunos modulos de la red a nivel general.
Widgets de información
Análisis FTP
Análisis de tiempo de FTP y principales fuentes / destinos
Análisis UDP
Análisis de tiempo UDP, principales fuentes / destinos, principales países de origen / destino y puertos de destino
Centro de Protocolo
Uso por línea de tiempo del protocolo, principales fuentes de conexión, uso de puertos y conexiones salientes / entrantes por puertos de destino
Conciencia del tráfico
Análisis de tiempo de anomalías de tráfico, fuentes de anomalías de tráfico y país de origen / destino crítico
Resumen de tráfico
Análisis de tráfico, país de origen / destino, país de origen / destino principal y análisis de tráfico desde la IP de origen hasta las IP de destino únicas
Análisis HTTP / S
Solicitudes HTTP / S bloqueadas / permitidas, principales fuentes / destinos y análisis de tiempo
Análisis de DNS
Análisis de tiempo de DNS y principales fuentes / destinos
Análisis de ancho de banda
Uso de ancho de banda (descarga / carga), uso de MB de descarga / carga y uso de descarga para TCP y UDP

4. Alert
Paneles de control preconfigurados sobre alertas y objetos de acciones.
Widgets de información
Alertas de nivel de advertencia
Detalles de alerta, recuentos únicos por objeto de acción, recuento total y alertas de nivel de información
Alertas de nivel crítico / de emergencia
Detalles de alerta, recuentos únicos por objeto de acción y recuento total
Alertas de cumplimiento y casos de uso
Objetos de acción y descripción general de alertas
Recuento de alertas de nivel de información / advertencia / crítico / emergencia, usuarios sospechosos, hosts internos / externos sospechosos, objetos sospechosos y alertas
Descripción general de las reglas de alerta

5. Application Server (byad-cenapp1)
Este estará centrado en el servidor de aplicaciones y otros de alto impacto como servidores web, FTP, correo, DHCP y DNS.
Widgets de información
Servidor web
Cronograma de eventos, direcciones IP externas, códigos de resultado, país de origen, rutas de URL, fuentes de datos y mensajes
Servidor FTP
Cronología de uso, direcciones IP de origen superior, mensajes del servidor, usuarios de origen y acciones de eventos
Servidor de correo
Cronología de eventos, principales destinatarios / remitentes de correo, eventos de correo, mensajes de servidor, asuntos de correo y phishing (ideal)
servidor DHCP
Línea de tiempo, mensajes del servidor, direcciones IP de origen principal, direcciones MAC principales y fuentes de datos
Servidor DNS
Análisis de tiempo, mensajes del servidor, direcciones IP de origen principal, acciones del servidor y fuentes de solicitud de DNS

6. System Events
Esta categoría se centra en los eventos del sistema dentro de la infraestructura en general.

Widgets de información
Eventos del sistema de capa de red
Actividad y sus detalles, mensajes de eventos y eventos con gravedad
Resumen del sistema
Categorías del sistema, mensajes de información, actividad del sistema por fuentes de eventos y mensajes de error del sistema
Eventos del sistema de capa de aplicación
Actividades, mensajes, errores del sistema y detalles de los mensajes
Eventos críticos del sistema
Análisis de tiempo, eventos críticos, recuento de eventos críticos y dispositivos críticos
Eventos del sistema SIEM
Utilización de CPU, utilización de disco, estadísticas de EPS y estado crítico / último de verificación de estado
Eventos del sistema de capa de seguridad
Actividades, mensajes, errores del sistema y detalles de los mensajes

7. Guest Access
Esta categoría de paneles proporciona información sobre los usuarios invitados que se conectaron a la red inalámbrica GUEST – RED INVITADOS.

Widgets de información
Análisis de recuento de usuarios de hotspot
Recuento de usuarios de inicio / cierre de sesión, recuento de usuarios en línea / registrados, recuento de usuarios fallidos en el inicio de sesión, análisis basado en la ubicación para inicio de sesión, inicio de sesión fallido, usuarios registrados y cierre de sesión
Análisis de uso de datos de usuario de hotspot
Los usuarios cargan / descargan el uso de MB y el uso de datos basados en la ubicación
Análisis de la actividad del usuario del hotspot
Actividad del usuario de inicio / cierre de sesión, usuarios fallidos en el inicio de sesión, actividad y motivos del usuario fallido en el inicio de sesión, cancelación de la cuenta y todos los mensajes de usuario

8. Database Control
Esta categoría brinda información valiosa sobre las bases de datos del grupo en general. Tiene tres paneles: uno ofrece una descripción general, mientras que uno está dedicado para SQL SERVER y Oracle.
Widgets de información
Descripción general de la base de datos
Cronograma de uso, fuentes de datos y acciones
SQL
Línea de tiempo de uso, nombre del objeto y nombre de la base de datos, eventos generales, tipo y acciones, y detalles de la actividad
Oracle
Línea de tiempo de uso, nombre de objeto, mensajes, comandos SQL,

9. Identity Management
Esta categoría de paneles ilustra información sobre la administración de cuentas de usuario, administración de identidad de usuario y actividades de usuario basadas en VPN.
Widgets de información
Descripción general del usuario de VPN
Recuentos de actividad de inicio de sesión, recuentos de fallos de inicio de sesión, usuarios principales para intentos / fallos de inicio de sesión, detalles de actividad, análisis de tiempo e inicio de sesión / fallo por países
Administración de cuentas
Recuento de actividades, 10 actividades principales, usuarios creados / eliminados, habilitar / deshabilitar usuarios, bloquear / desbloquear usuarios, mensajes, actividades de cambio de contraseña y contraseña caducada por cuenta
Descripción general de la identidad

Recuento de actividad de inicio de sesión, recuento de fallos de inicio de sesión, usuarios principales por intentos / fallos de inicio de sesión, fallos de inicio de sesión y de inicio de sesión por dirección IP de origen y actividad de cierre de sesión por parte de los usuarios

10. File Access Control
Esta categoría de paneles presenta información visualizada sobre el sistema de archivos del grupo en general. Cubre las actividades de los usuarios, los eventos de uso compartido de archivos y la información detallada sobre los eventos de cambio.
Widgets de información
Archivo compartido
Análisis de tiempo, carpetas compartidas, eventos de archivos compartidos y detalles de eventos
Sistema de archivos
Análisis de tiempo, acciones, actividad de archivos de usuario y nombres de objetos
Descripción general del archivo
Cronología del servidor de archivos, carpetas compartidas, recuento de eventos de archivos modificados, eventos modificados por usuarios y detalles de eventos de cambio de archivos compartidos