**Manuales de estrategias, herramientas SIEM y herramientas SOAR**

Anteriormente, usted aprendió que los Equipos de Seguridad se encuentran con amenazas, Riesgos, vulnerabilidades e Incidentes de forma regular y que siguen libros de jugadas para abordar los problemas relacionados con la Seguridad. En esta lectura, aprenderá más sobre los libros de jugadas, incluyendo cómo se utilizan en la administración de información y eventos de seguridad (SIEM) y en la Orquestación, automatización y respuesta de seguridad (SOAR).

**Manuales de estrategias y herramientas SIEM**

Los manuales de estrategias son utilizados por los equipos de ciberseguridad en caso de incidente. Los manuales de estrategias ayudan a los Equipos de Seguridad a responder a los Incidentes garantizando que se sigue una lista coherente de acciones de forma prescrita, independientemente de quién esté trabajando en el caso. Los manuales de estrategias pueden ser muy detallados y pueden incluir diagramas de flujo y tablas para aclarar qué acciones hay que tomar y en qué orden. Los manuales de estrategias también se utilizan para los Procedimientos de recuperación en caso de ataque de ransomware. Los distintos tipos de incidentes de Seguridad tienen sus propios Manuales de estrategias que detallan quién debe tomar qué medidas y cuándo.

Los manuales de estrategias suelen utilizarse junto con las herramientas SIEM. Si, por ejemplo, una herramienta SIEM señala un comportamiento inusual del usuario, un Manual de estrategias proporciona a los analistas instrucciones sobre cómo abordar el Problema.

**Manuales de estrategias y herramientas SOAR**

Los manuales de estrategias también se utilizan con las herramientas SOAR. Las herramientas SOAR son similares a las herramientas SIEM en el sentido de que se utilizan para la supervisión de amenazas. SOAR es una pieza de software utilizada para automatizar tareas repetitivas generadas por herramientas como un SIEM o una detección y respuesta gestionadas (MDR). Por ejemplo, si un usuario intenta iniciar sesión en su computadora demasiadas veces con una contraseña incorrecta, un SOAR bloquearía automáticamente su cuenta para detener una posible intrusión. A continuación, los analistas consultarían un Manual de estrategias para dar los pasos necesarios para resolver el Problema.

**Claves**

Lo más importante que hay que saber es que los libros de jugadas, también denominados a veces runbooks, proporcionan acciones detalladas para que los equipos de Seguridad las lleven a cabo en caso de Incidente. Saber exactamente quién tiene que hacer qué y cuándo puede ayudar a reducir el impacto de un Incidente y reducir el riesgo de daños a los recursos críticos de una organización.