PAM Significa “Pluggable Authentication Module” (módulo de autenticación enchufable).

Se utiliza para gestionar la autenticación de usuarios en sistemas Linux.

Los diferentes métodos de autenticación se implementan modularmente, lo que facilita combinar varios métodos.

Se gestiona en un único archivo de configuración, /etc/pam.d/.

Registra los eventos de autenticación lo que nos puede ayudar a identificar actividades sospechosas en nuestro sistema.

PAM es muy útil, ya que nos proporciona una mayor seguridad y flexibilidad al permitir la configuración personalizada de las políticas, la adaptación de los métodos y la gestión centralizada.

ZTNA Significa “Zero Trust Network Access” (Acceso a la red de confianza cero).

Se basa en el principio de que no se debe confiar en ninguna entidad hasta que se haya identificado y autenticado de manera correcta.

Se desconfía de todas las conexiones de red por defecto. Cada entidad que intenta acceder tiene que identificarse previamente, generalmente mediante métodos como la autenticación multifactor (MFA)

Proporciona una mayor seguridad y control sobre la red.

SOAR Significa “Security Orchestration, Automation and Response” (Orquestacion, automatizacion y respuesta de seguridad)

Se utiliza para gestionar de manera mas eficiente las amenazas e incidentes de seguridad.

* Orquestacion: coordina las acciones de seguridad, garantizando que se sigan de manera adecuada cuando ocurre un incidente.
* Automatizacion: automatiza las tareas de seguridad.
* Respuesta: toma decisiones en función de las reglas predefinidas.

SOAR ayuda a reducir la carga de trabajo manual, permite respuestas mas rápidas, reduce el riesgo de errores humanos, facilita la gestión completa ante incidentes y la generación de informes.

TTP Significa “Tactics, Techniques and Procedures” (tacticas, tecnicas y procedimientos)

Son las distintas maneras en las que los hackers o ciberdelincuentes llevan a acabo sus ataques.

* Tácticas: son las estrategias para lograr sus objetivos.
* Técnicas: métodos específicos para llevar a cabo un ataque.
* Procedimientos: son los pasos detallados para implementar una técnica.

Tiene varias aplicaciones:

* Detección y prevención: identificar patrones y señales que indican un posible ataque.
* Análisis de amenazas: permite profundizar en los ataques.