SecDevOps y Administración de Redes para Cloud

Jesús F. Rodríguez-Aragón

Presentación de la asignatura

Profesor de la asignatura

https://www.linkedin.com/in/jraragon/

- Jesús F. Rodríguez-Aragón

Carrera profesional

Ingeniero en Informática y Doctor en Informática por la Universidad de Salamanca

Miembro del Comité de Dirección de MEGA.nz (Director de Producto)

Fundador y CEO de Techtrid Ingeniería

Fundador y CEO de Iberbox.com

Premio Mejor Ingeniero en Informática de Castilla y León 2018

Iberbox – Premio a Mejor Startup de Castilla y León 2022

Actualmente

Startup Advisor & Investor (2022)

Profesor UNIR – GII, GMC, GDDV, GCS, MUDevOps (2022)

Profesor Asociado USAL – GII, GMat (2013)

Prof. Externo UBU,ULE,UVA: Máster en Inteligencia de Negocio y Big Data en Entornos Seguros (2019)

Miembro Junta de Gobierno del CPIICyL (2019)

Índice de la asignatura

Trabajos y actividades a realizar

- Test Temas
- Actividad 1: Análisis de tráfico
- Actividad 2 grupal: Arquitectura de red
- Laboratorio: Seguridad en AWS

Sistema de evaluación

- Examen final: 60%

- Evaluación Continua: 40%

Actividad	Tipo	Puntuación máxima
Actividad 1	Individual	5,0
Laboratorio	Individual	5,0
Test (x9)	Individual	0,9 [0,1 x 9]
Actividad grupal	Grupal	4,1
	TOTAL	**15,0**

Solo suman actividades con calificación mayor o igual a 5 puntos dentro de plazo

Satura en 10 puntos

Objetivos

- Un único sistema que ofrecía servicios ha evolucionado a un Conjunto de equipos en red que ofrece servicios
- Comprender el concepto de red
- Seguridad y su aplicación en entornos DevOps

Concepto de red

“Computer Networks” de Tanenbaum:

“El modelo tradicional de un único ordenador para todas las necesidades de computación de una organización ha sido reemplazado por un modelo en el que un gran número de ordenadores independientes pero interconectados realizan el mismo trabajo. Estos sistemas se denominan redes de ordenadores”

Concepto de red :: Protocolos

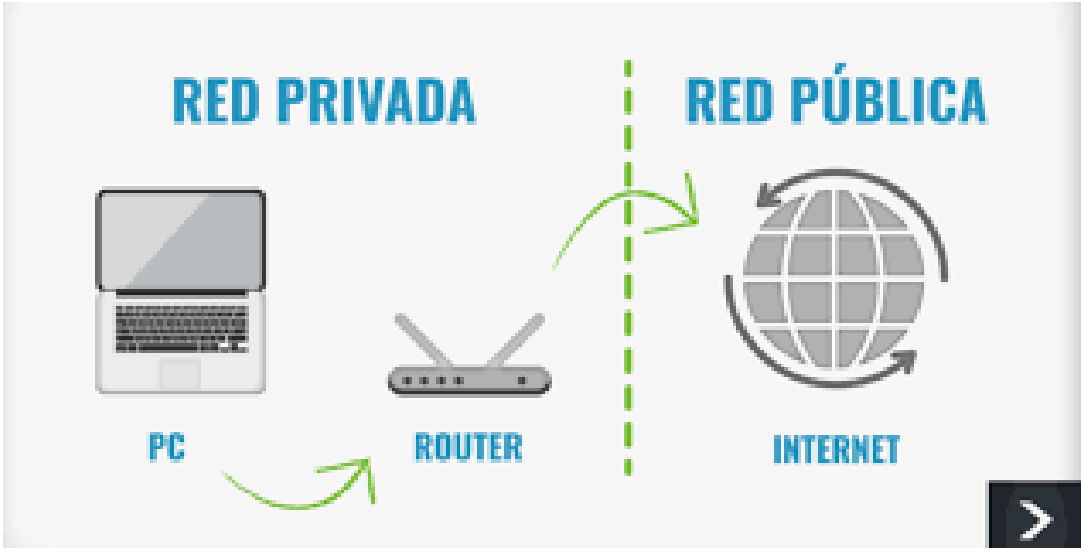
- Conjunto de reglas para comunicarse y transmitir información
- Diferentes Niveles → Patrón Arquitectónico Layers

	OSI	DARPA o TCP/IP	
Servicios de red para aplicaciones	Aplicación	Aplication	HTTP, SMTP, POP3…
Formato datos estándar	Presentación		
Información de sesión entre dos equipos	Sesión		
Transporte confiable	Transporte	Transport	TCP, UDP (con/sin conexión previa)
Direccionamiento lógico	Red	Internetwork	IP
Direccionamiento físico	Enlace	Medium Access	Network Access Layer (NAL)
Características eléctricas	Físico	Phisical	

From Wikimedia Commons

Clasificación de redes

- Desde el punto de vista de un Administrador



Topologías de red :: En base a la interconexión de elementos

- Representación de los elementos de una red y cómo están conectados

- Topología física
  - Disposición física real detallando todos los componentes: cableado, equipos finales, equipos de interconexión, etc

- Topología lógica
  - Representación conceptual donde lo principal es mostrar los equipos y el flujo de información

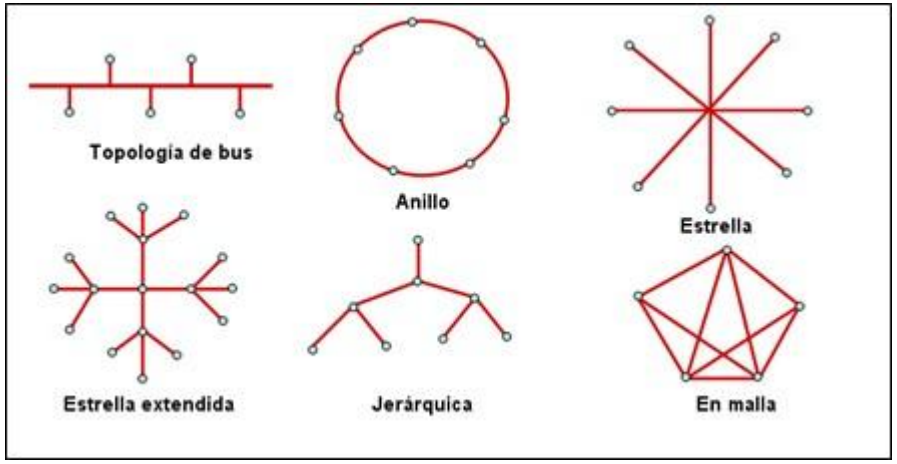
- Es más común utilizar la topología lógica (salvo que necesitemos especificar detalles físicos)

Topologías de red :: En base a la interconexión de elementos

- Bus: un único cable (compartido o varios enlaces punto a punto)

- Estrella: nodo central (concentrador/hub –envían a todos los nodos- o conmutador/switch –envían al nodo especificado-) con enlaces punto a punto a todos los dispositivos
  - Estrella extendida → Se conecta a otra estrella

- Anillo: Enlaces punto a punto interconectado
  - Doble anillo → Mayor tolerancia a fallos

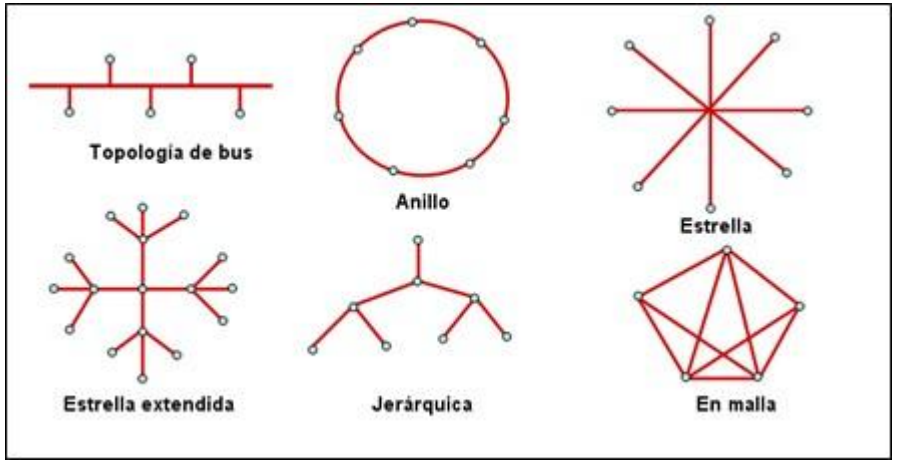


Topologías de red :: En base a la interconexión de elementos

- Árbol: estructura jerárquica con enlaces punto a punto entre nodos

- Malla: conexiones punto a punto entre algunos o todos los nodos de una red (malla completa)
  - Mayor tolerancia a fallos
  - Mayor complejidad

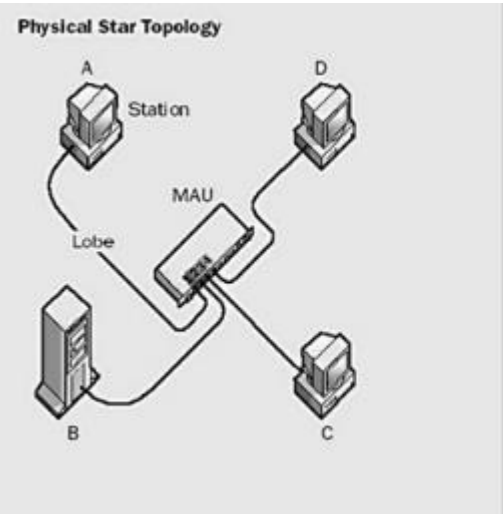
  - Malla completa de N elementos → N*(N-1)/2 enlaces punto a punto



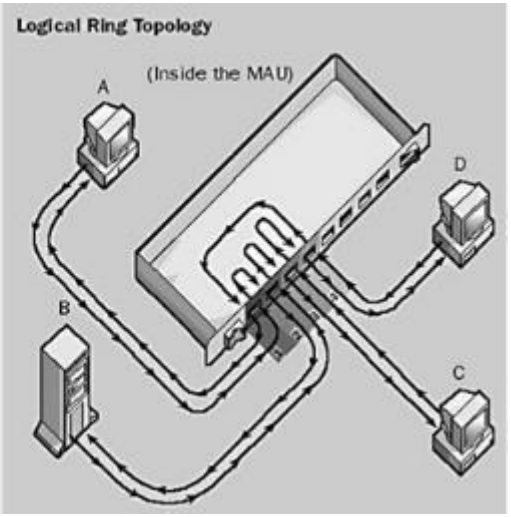
Topologías de red :: En base a la interconexión de elementos

- Mixta o irregular: mezcla de varias topologías
  - Internet es una red de este tipo
  - Suelen ser redes complejas, que han sufrido crecimiento y evolución

- La topología lógica puede ser diferente a la topología física



Estrella



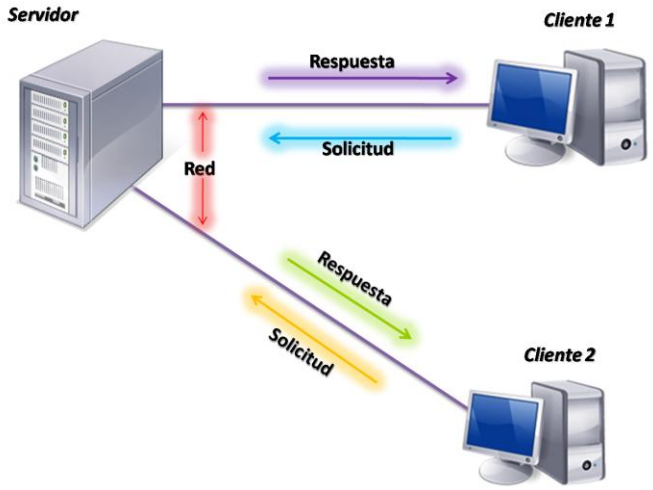
Anillo

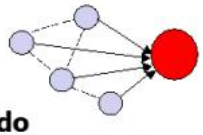
Clasificación de redes

- En base a su arquitectura

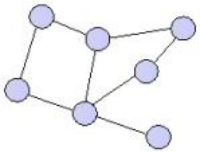
- Modelos:

Cliente-Servidor



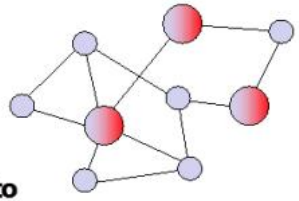


Híbrido
- Un coordinador central
- Napster



Puro
- Todos los pares contienen información de encaminamiento
- FreeNet, Gutella

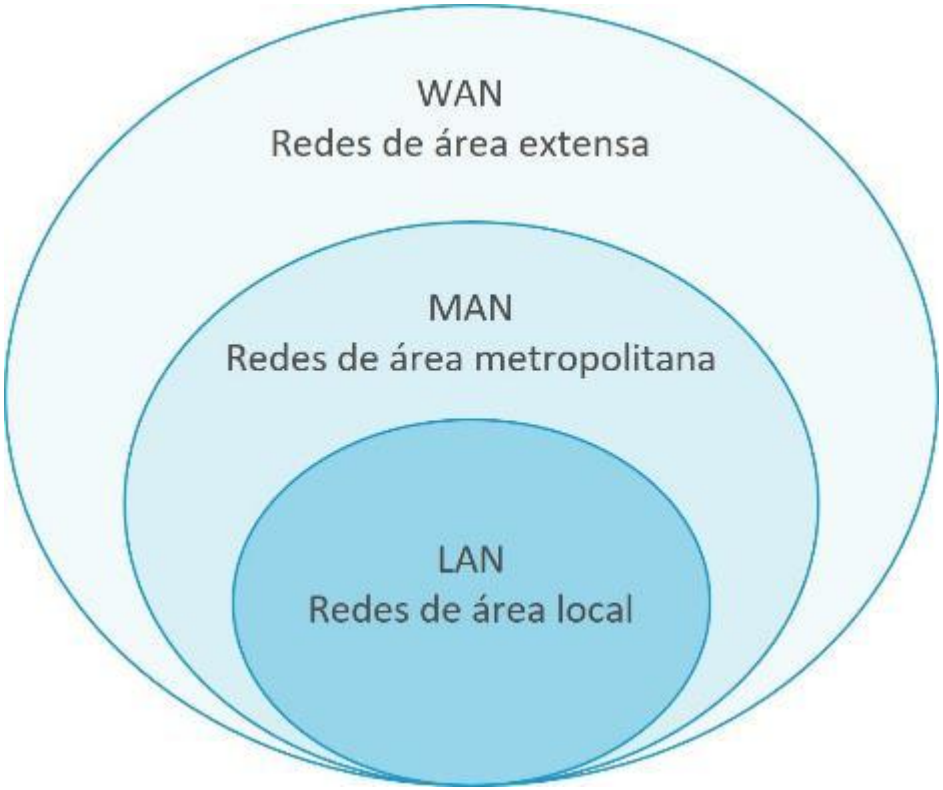
P2P (peer to peer)



Mixto
- Sólo los superpares contienen información de encaminamiento
- FastTrack, Gnutella2

Clasificación de redes

- En base a su extensión geográfica



Clasificación de redes cableadas, por su extensión

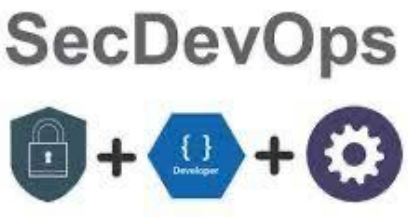
Clasificación de redes inalámbricas, por su extensión

Definición de SecDevOps

- Los gerentes de producto *(product managers)* miden las relaciones de compromiso y retención, los desarrolladores miden la ergonomía y la usabilidad, y los operadores miden el tiempo de actividad y los tiempos de respuesta.

- DevOps es un término usado para describir la mejor comunicación y colaboración entre profesionales de desarrollo de software y operaciones de infraestructura

Definición de SecDevOps



- SecDevOps es un paradigma en el que se integran los procesos de desarrollo de software y operaciones considerando requisitos de seguridad y conformidad

- DevOps, Manifiesto Ágil, etc → Se centran en un único objetivo: **Satisfacer al cliente**

Definición de SecDevOps

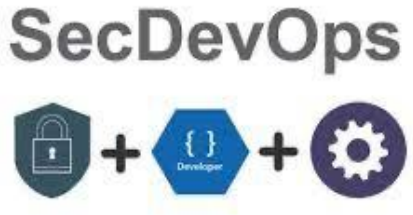
- Métricas de los equipos de seguridad
  - % de cumplimiento de un estándar de seguridad
  - Número de incidentes de seguridad
  - Tasa y velocidad de resolución
  - % equipos desactualizados
  - etc

- Métricas de los equipos de desarrollo
  - Metas e hitos temporales de finalización de desarrollo

- Tan negativo es centrarnos en unas como en otras (equipo de desarrollo haciendo caso omiso a las directivas de seguridad; equipo de seguridad proponiendo soluciones poco realistas sólo centradas en sus propios objetivos), perdiendo el foco de que lo fundamental es la **satisfacción del cliente**

- La satisfacción del cliente se mide en:
  - Cumplir con los requisitos de desarrollo, tiempos, etc.
  - También reducir el riesgo de seguridad de una aplicación

Definición de SecDevOps



El objetivo, al igual que en las metodologías ágiles, debe ser que el equipo pase de defender sus propias métricas a defender el resultado de toda la organización

- Integración entre
  - Desarrolladores
  - Operadores
  - Ingenieros de seguridad
- La seguridad es un servicio más de la cadena de requisitos del cliente
- Los ingenieros de seguridad añaden controles sobre el producto entregable

Seguridad en DevOps

- La seguridad en DevOps se organiza en tres áreas:

Seguridad basada en pruebas, o *test-driven security*	La fase más temprana consiste en implementar y probar controles de seguridad directamente en el pipeline DevOps. Por ejemplo, una prueba puede verificar que la configuración de un servidor cumple con los requisitos establecidos o que las aplicaciones incluyen las cabeceras de seguridad necesarias. El rendimiento de esta fase es muy alto, medido a partir de la mejora y el valor que aporta respecto a la dificultad de implementación de los controles. Las pruebas de seguridad deben manejarse de la misma manera que todas las pruebas de aplicaciones en los pipelines de CI y CD: automática y continuamente.
Monitorizar y responder a los ataques	Cualquier servicio en línea acabará siendo atacado. En este caso, el equipo de seguridad debe reaccionar a tiempo. Esta fase consiste en preparar a la organización para actuar en estas situaciones, monitorizando continuamente y respondiendo a las amenazas. En esta fase se consideran la detección de fraudes e intrusos, el análisis forense digital y la respuesta a incidentes.
Evaluar riesgos y madurar la seguridad	Una estrategia de seguridad exitosa no puede tener éxito cuando solo se enfoca en cuestiones técnicas. La tercera fase de la seguridad continua se centra en la operativa de alto nivel, en la que la tecnología no es el aspecto más importante. Entran en juego la gestión de riesgos y las pruebas de seguridad, tanto internas como externas, para ayudar a las organizaciones a reenfocar sus esfuerzos de seguridad e invertir sus recursos de manera más eficiente.

- El feedback del cliente es clave

Seguridad en DevOps

- Seguridad basada en pruebas
- Seguridad a nivel de aplicación
- Seguridad a nivel de infraestructura
- Seguridad del pipeline
- Pruebas continuas
- Monitorización y respuesta a ataques
- Evaluación de riesgos y maduración de la seguridad

Seguridad en DevOps :: Seguridad basada en pruebas

- Controles básicos que impidan vulnerabilidades “débiles / fáciles”

  - Inicio de sesión root deshabilitado

  - Sistemas actualizados a la última versión

  - HTTP → redirección a HTTPS

  - Credenciales no hardcodeados en código de la aplicación

  - Nivel de administración detrás de VPN

- Lista de controles consensuada entre equipo de seguridad, desarrollo y operaciones

Seguridad en DevOps :: Seguridad a nivel de aplicación

- Open Web Application Security Project: https://owasp.org/www-project-top-ten/

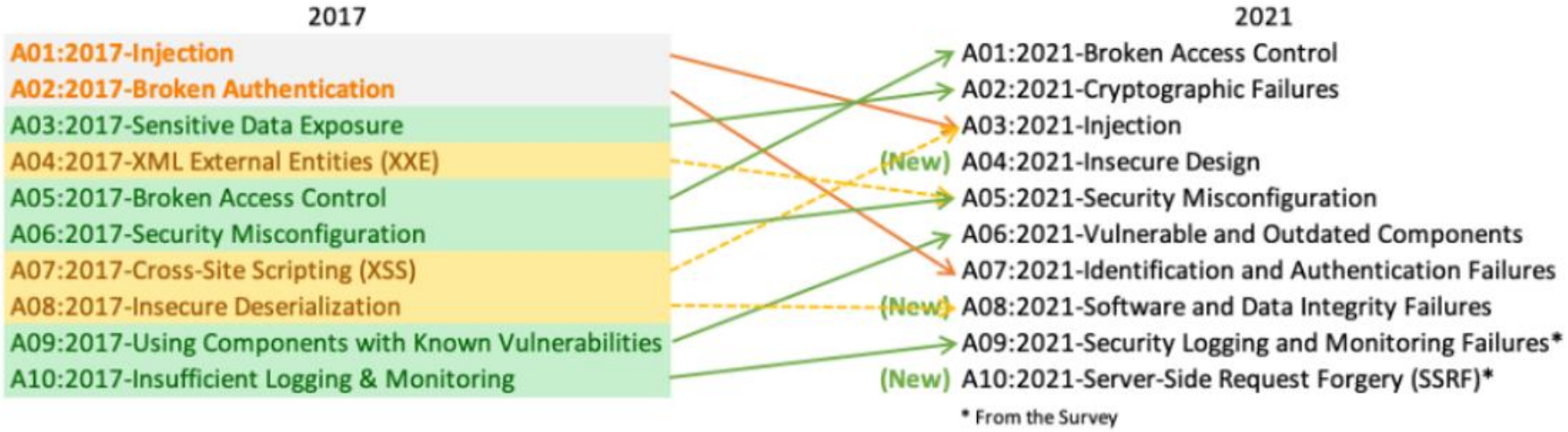
OWASP Top Ten 2025

Current project status as of September 2024:

- We are planning to announce the release of the **OWASP Top 10:2025** in the first half of 2025.
- **Data Collection (Now - December 2024)**: Please donate your application penetration testing statistics.

Stay Tuned!

- Diez ataques más comunes que deben ser vigilados a nivel de aplicación:



- Inyecciones (SQL, cross-site scripting, etc), fallos criptográficos, diseño no seguro del sistema, etc

Seguridad en DevOps :: Seguridad a nivel de infraestructura

- El hecho de utilizar una nube pública no exime de aplicar políticas de seguridad sobre la infraestructura
- Los proveedores de nube proporcionan herramientas y servicios que el cliente ha de mantener, configurar y adaptar a sus propias políticas de seguridad
- Por ejemplo, de nada sirve que el proveedor de nube nos proporcione un servicio de firewall si nosotros, como clientes, no configuramos dicho firewall de manera que cumpla nuestros requisitos de seguridad

Seguridad en DevOps :: Seguridad del pipeline

- Despliegue de productos basado en automatización → Proceso muy diferente al despliegue tradicional

- Pipelines CI/CD es un punto vital a proteger en un sistema, puesto que desde él podemos acceder al código de producción

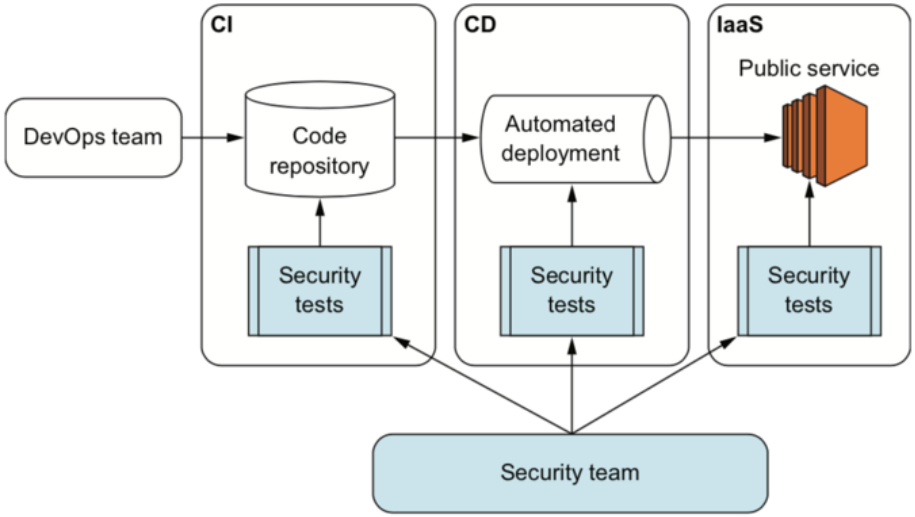
  - Controles de integridad de los commits
  - Acceso basado en roles en las herramientas de CI/CD

Seguridad en DevOps :: Pruebas continuas

- Pruebas de integración

- Test-driven Development
  - Las pruebas se implementan primero
  - Se desarrolla la solución
  - Se lanzan las pruebas

  - Si error → Se desarrolla la prueba y posteriormente la solución al error



Seguridad en DevOps :: Pruebas continuas

- Ventajas:

  - El diseño de las pruebas previo hace que el ingeniero de seguridad se involucre con el producto a priori (y no a posteriori tras su finalización para hacer meras comprobaciones)

  - Las pruebas son concretas y comprueban un comportamiento deseado completo. No son generalidades

  - Al igual que en el desarrollo, la reutilización es aplicable a las pruebas

- La experiencia es clave en el desarrollo de las pruebas, por lo que los ingenieros de seguridad podrán aportar su experiencia al resto del equipo DevOps

- La seguridad se debe incorporar como otra característica más del producto que ha de ser comprobada con las pruebas

Seguridad en DevOps :: Monitorización y respuesta a ataques

- Poseer un servicio público en Internet es asumir que ese servicio en algún momento **va a ser atacado**.

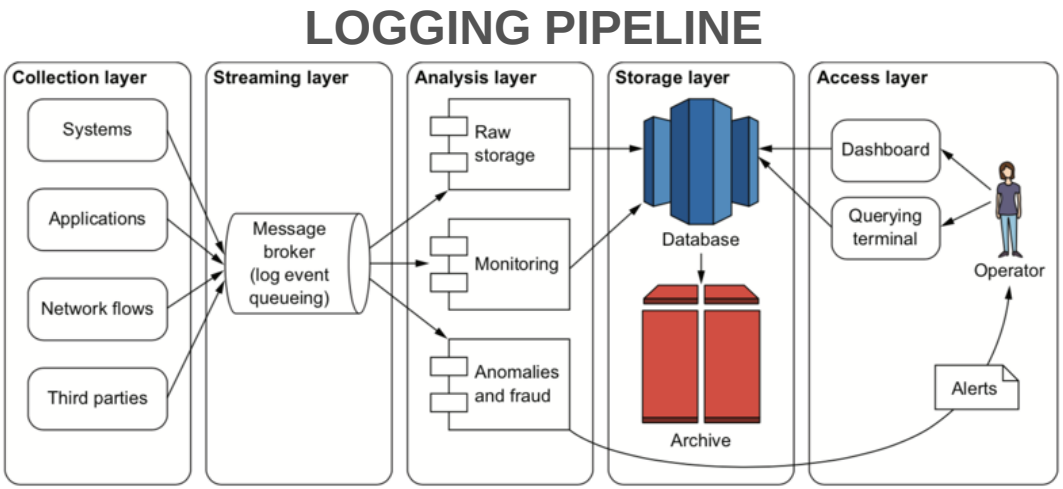
- Hay múltiples maneras:
  - Búsqueda de credenciales de usuario
  - Interrupción del servicio
  - Rescates por compromiso de datos o del propio negocio
  - Explotar vulnerabilidades en la infraestructura para acceder a los datos

- Los sistemas de monitorización y respuesta a ataques son vitales para prevenir y actuar rápidamente en caso de ataque

- Estos sistemas enfocan tres áreas:
  - Registro y detección de fraude
  - Detección de intrusiones
  - Respuesta a incidentes

Seguridad en DevOps :: Monitorización y respuesta a ataques :: Registro y detección de fraude

- Logging. El uso de logs es variado en función de los perfiles:
  - Desarrolladores y operadores → Resolver problemas
  - Product manager → estadísticas de uso, retención de usuarios, popularidad de funcionalidades, etc
  - Seguridad → detección de anomalías, análisis forense
- Varias fuentes → Cantidad ingente de datos → Centralizar en un solo túnel



Seguridad en DevOps :: Monitorización y respuesta a ataques :: Registro y detección de fraude

- Fases del Logging Pipeline

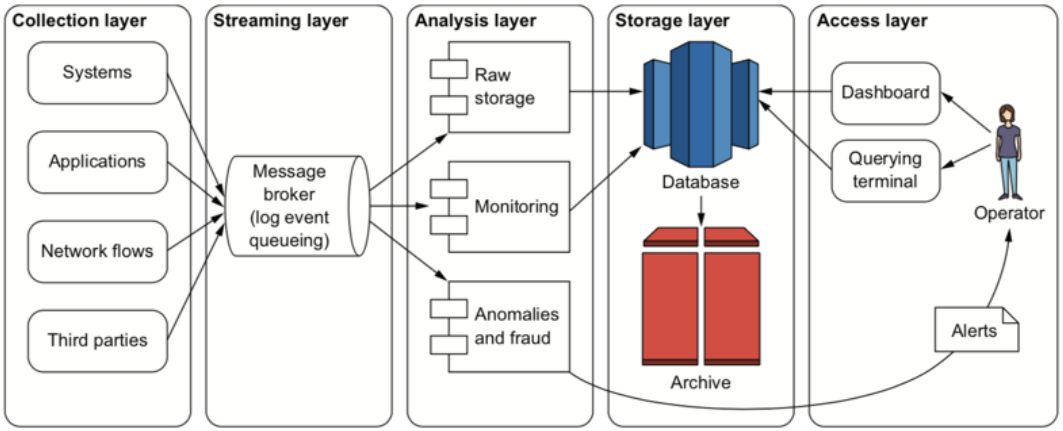
  - Capa de recopilación → Cada sistema recopila y envía a una cola central

  - Capa de transmisión → Enrutar registros a los consumidores

  - Capa de análisis → Inspeccionar, detectar fraudes y enviar alertas

  - Capa de almacenamiento → DB (acceso más inmediato) y Archivado

  - Capa de acceso → Permitir acceso a los operadores de modo interactivo



Seguridad en DevOps :: Monitorización y respuesta a ataques :: Detección de intrusiones

- ¿En qué consiste típicamente una intrusión? Cuando un atacante entra:

  - Deposita payload en servidor (que suele ser un script pequeño)

  - Lanza el script, que habilita puerta trasera para contactar con servidor remoto → Abre un canal de comando y control (C2)

  - Se ejecutan los comandos recibidos en la puerta trasera y se trata de replicar en otros equipos de la red

  - Si consigue encontrar datos valiosos, utilizará un segundo canal C2 para enviar los datos al atacante

- Nuestro objetivo será detectar estos pasos para detectar intrusos

- Existen herramientas que nos ayudan en esta tarea

Seguridad en DevOps :: Monitorización y respuesta a ataques :: Detección de intrusiones

- IDS: Intrusion Detection System
  - Buscan patrones y comportamientos sospechosos que identifiquen canales C2

  - Un firewall bloquea tráfico en base a unas normas (es meramente defensivo). Un IDS infiere comportamientos y detecta intrusiones (es proactivo)

- Auditoría de conexiones:
  - Es necesario mantener un control y registros sobre las conexiones de nuestros sistemas de manera periódica → Esto facilitará futuras inspecciones forenses tras ataques

- Auditoría del sistema:
  - Mantener un control también de los accesos al sistema (no sólo a la red)

- Este tipo de auditorías y registros puede generar sobrecargas (tanto en la infraestructura como en el personal)

Seguridad en DevOps :: Monitorización y respuesta a ataques :: Respuesta a incidentes

- Una violación de seguridad es una **situación caótica → CAÓTICA**
  - Incertidumbre, miedo, estrés, etc

- El objetivo es recuperar la normalidad cuanto antes de una manera segura

- La reacción debería consistir en seis fases
  - **Preparación**: previo al ataque donde protocolarizamos la situación
  - **Identificación**: detección del incidente de manera rápida
  - **Contención**: impedir que la violación se extienda más
  - **Erradicación**: eliminar las amenazas de la organización
  - **Recuperación**: volver al estado natural del negocio
  - **Lecciones aprendidas**: analizar a posteriori el ataque y sacar conclusiones

Seguridad en DevOps :: Evaluación de riesgos y maduración de la seguridad :: Evaluación de riesgos

- La gestión y el estudio de los riesgos de una organización

- Identificar y priorizar problemas que pueden amenazar el negocio

- Objetivos de un buen enfoque de gestión de riesgos

  - **Analizar los riesgos a la misma velocidad que las actividades DevOps**: si el software cambia, el análisis de riesgos debe poder cambiar a la misma velocidad. Si no → cuello de botella → Seguridad se convertirá en problema

  - **Automatizar**: En un entorno DevOps las operaciones manuales no deberían ocurrir

  - **Involucrar a todos los equipos en el análisis**: el análisis de riesgos debe formar parte de la arquitectura de seguridad por parte de todos los equipos. No es sólo una tarea que se hace a posteriori.

Seguridad en DevOps :: Evaluación de riesgos y maduración de la seguridad :: Pruebas de seguridad

- Lo que no se puede medir no se puede comparar / comprobar

- Se deben incorporar pruebas de seguridad regulares y periódicas. Por ejemplo:

  - Evaluar la seguridad de aplicaciones e infraestructura con escaneos de vulnerabilidades

  - Usar consultoras externas para auditar: diferentes puntos de vista

  - Establecer un programa de recompensa de errores: aprovecharse de investigadores de seguridad independientes.

www.unir.net