Purple Team = Red+Blue stop fighting

By **Antonio Juanilla**(Specter)

$Whoami

Antonio Juanilla

1. Autodidacta.
2. DevSecOps.
3. Co-Organizador de HackMadrid%27
4. Miembro del equipo de FlagHunters
5. Amante de la tecnología.
6. Defensor de la democratización de la tecnología para la mejora de la sociedad.

Redes

Twitter: **@spectertj**

Linkendin: https://www.linkedin.com/in/spectertj

Github: **spectertj**


Sólo el conocimiento nos hace libres
HACKMADRID
%27

https://hackmadrid.org

https://twitter.com/hackmadrid

Telegram: t.me/hackmadrid

https://meetup.com/HackMadrid-27

https://linkedin.com/company/hackmadrid

Hablaremos de:

Red Team
Seguridad Ofensiva

Hablaremos de:

Blue Team
Seguridad Defensiva

Hablaremos de:

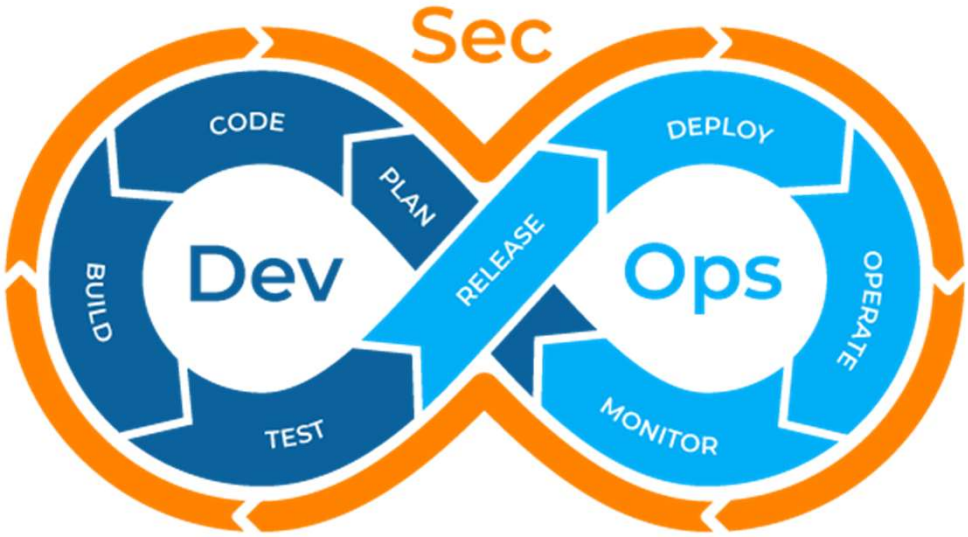
Purple Team
Seguridad Colaborativa

¿Que seria App Sec?

Cualquier actividad que se dedique a asegurar que el software es seguro.

¿Que es DevSecOps?

Se podría decir que es AppSec en los entornos DevOps



¿Que es Red Team?

Atacantes/Ofensiva

Encargados de encontrar riesgos y problemas reales, usualmente en sistemas en producción.

A través de:

- Penetration Testing
- Ethical Hacking
- Exploits

¿Que es Blue Team?

Defensores / Protectores.

Aseguran que las defensas son efectivas, también usando herramientas para bastionar los sistemas.

A través de:

Monitoreo

Logs

Parcheo de aplicaciones

¿Que es Purple Team?

Algunos dicen que es Red Team + Blue Team.

Colaboradores, cooperadores y comunicadores.

Enseñando , proveyendo de herramientas, habilitando y ayudando.

También conocido como el puente entre la seguridad y el desarrollo de software.

¿Que es Purple Team?

Es el AppSec como un todo.

Los Red y Blue ambos se solapan con AppSec.

Es el equipo que trabajo junto con los desarrolladores.

El equipo que guía, asiste, da disponibilidad, que entrega herramientas.

Que se busca con AppSec?

Zero trust

1. En las aplicaciones.
2. Entre las aplicaciones.
3. En las configuraciones.
4. En la red.

Brechas asumibles

1. En cada aspecto IT se puede asumir que una brecha existe.
2. No mas “solo proteger el perimetro”.

Recomendaciones de seguridad

1. Trabajar con entornos securizados.
2. Monitorización y funciones de logs.
3. Uso de estándares y convención segura para el código de la aplicacion.
4. Uso de certificados **SSL/TLS**.
5. Securizar y verificar el transito de los datos.
6. Uso de application gateway.
7. Uso de WAF (**Web Applications Firewall**).
8. Manejo de secretos.
9. Desplegar funciones en una granulidad mínima(microservicios).
10. Verificar el uso de imágenes **Docker** publicas.

Gestion de componentes y librerias de terceros

1. Sea Open source o no, cada componente nuevo que metes es un riesgo que aceptas.
2. Usar múltiples herramientas para verificar componentes que no se conoce que sean inseguros para asi recopilar información de diferentes lugares.
3. Escaneo del repositorio regularmente para notificar cuando hay que actualizar un componente y también para notificar cuando se puede convertir en vulnerable.
4. Escanear en los pipelines para asegurarte que no estas entregando un código vulnerable nuevo.

Almacenamiento Online

1. Usar un estándar o un formato para almacenar.
2. Clasificar los datos para asegurar un uso apropiado de los mismos y conocer su valor.
3. Monitorizar accesos, integridad, etc. A los datos, con alertas y respuestas automatizadas.
4. Accesos por solo por service account, directamente desde una aplicación, nunca debe haber contacto humano.

Contenedores y orquestación

Seguir las mejores practicas para Cloud Security y para redes.

Hay que recordad que pueden ser nuevas configuraciones, nuevas reglas y nuevas herramientas pero se siguen manteniendo los mismos principios de Zero Trust.

¿Cloud Security?

Spoiler Alert!!!!

Si quieren lo hablamos en el Hack&Beers de mas tarde xD

APIs y microservicios

Seguir las misma mejores practicas para AppSec

Herramientas

1. IAST Interactive Application Security Testing
2. RASP Real-Time Application Security Protection
3. Controles Cloud Native
4. Herramientas de seguridad dentro de los pipeline DevOps
5. Herramientas para el inventariado de aplicaciones.

Nunca olvidar el DevSecOps xD

Eventos HackMadrid%27

Eventos de FEBRERO

27/02 - 20:00 horas - HackMeetingOnline
<Una aproximación a la seguridad de Kubernetes>
Presenta: Rod Soto

Eventos de MARZO

03/03 - 18:30 horas - Mercado de la Guindalera
<Jakeando Kañas> Evento social

05/03 - 19:00 horas - Agora de Liferay
<Los Trucos del Bugbounty>
Presenta: Jaime Andrés Restrepo

28/03 -10:00 horas - La Nave de Madrid
<Jornadas de Ingeniería Social>
Presentan: Kneda, Gema y Miguel Angel Liébanas

Eventos de ABRIL

07/04 - 18:30 horas - Mercado de la Guindalera
<Jakeando Kañas> Evento social

16/04 - 19:00 horas - Oficina de MNEMO
<Introducción a la Ingeniería Social>
Presenta: Kneda

18/04 -10:00 horas - La Nave de Madrid
<HackLAB: LoRaWan - Guifinet>
Presentan: David Marugan - ttnMAD - HackMadrid

World.Party->2020

Octubre 30/31 del 2020
Lugar: La Nave de Madrid

Una fiesta para compartir el conocimiento y el hacking inteligente

Hacking in the free world

hackmadrid.org/flaghunters.html | Telegram: flagHunters | Telegram: t.me/hackmadrid

Gracias.....