fidélitas
Virtual

Computación Forense

Ataques Informáticos

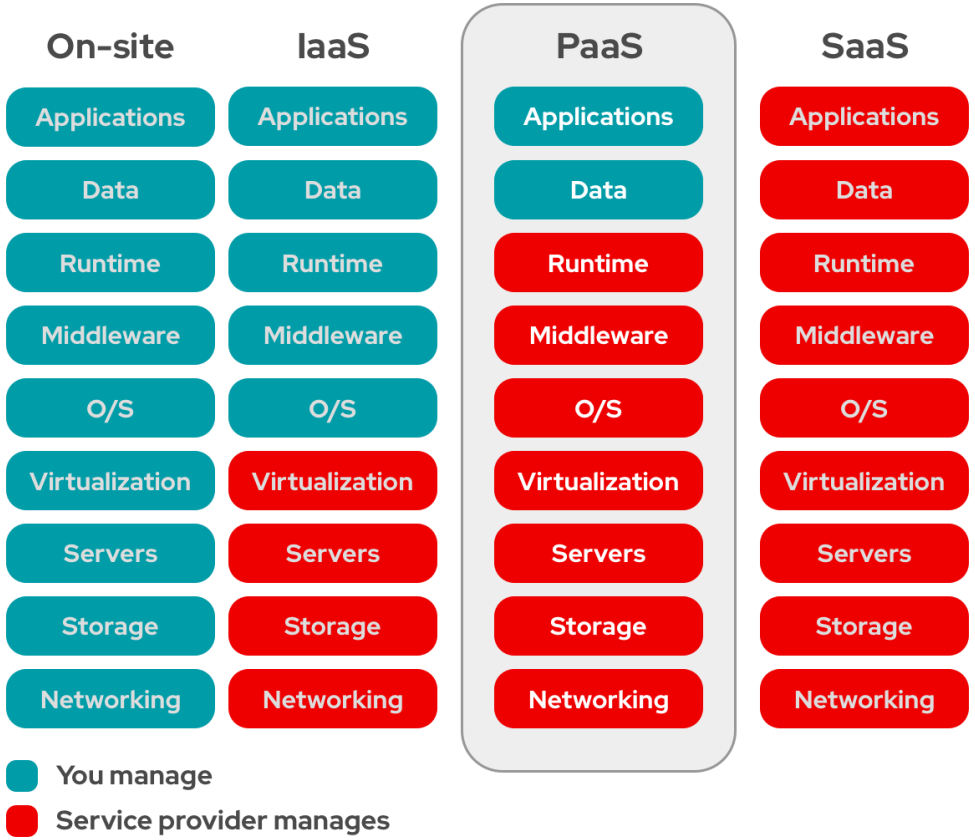
Clase 4b

Profesor: Ing. Alex Araya Rojas, MT

CISSP, CISM

Ataques Informáticos

- **Ataques en Ambientes de Nube**
  - Recordemos los siguientes términos:
    - Infraestructura como Servicio
    - Plataforma como Servicio
    - Software como Servicio



Ataques Informáticos

- **Ataques en Ambientes de Nube**

Secuestro de Servicio utilizando Ingeniería Social o ataques XSS

Ataques DNS

SQL Injection

Ataques de Denegación de Servicios (DoS y DDoS)

Enmascarado (Wrapping)

Ataques Informáticos

- **Ataques en Ambientes de Nube**
  - Las técnicas de investigación dependen del servicio y el modelo de despliegue.
  - Aplica como un subconjunto de investigación de ataques de redes de datos.
  - Los ataques pueden tener a la nube presente como sujeto, como objeto o como herramienta.
  - Los retos más importantes para los investigadores son la recolección de evidencias, latencia, temas legales y procesos de análisis complejos o remotos.

Ataques Informáticos

- **Ataques de Email**

  - El email es un método de comunicación ampliamente utilizado en las organizaciones y un vector de ataque muy bueno, ya que un atacante puede obtener mucho con un mínimo esfuerzo.

  - SPAM, Phishing, Inundación de Correos son manifestaciones de crímenes cometidos con el envío de emails.

  - Fraudes de identidad, ciber acoso, pornografía infantil entre otros, son ejemplo de crímenes que se respaldan en correos electrónicos en la mayoría de ocasiones.

Ataques Informáticos

- **Ataques de Email**
  - Un Email se compone de 3 partes: Encabezado, Cuerpo y Firma.
  - Pasos para investigar un crimen o violaciones de email:
    - Obtener orden judicial
    - Examinar correos
    - Analizar encabezados y realizar procesos de rastreo de ser posible
    - Adquirir archivos adjuntos del correo y analizarlos
    - Examinar los logs del correo electrónico

Ataques Informáticos

- **Ataques Web**
    - Dentro de los ataques que comúnmente se presentan en esta categoría están:
        - Clientes sin acceso a los servicios
        - Actividades sospechosas en las cuentas de usuario
        - Fuga de información
        - Redireccionamiento a sitios fraudulentos
        - Defacement de sitios web
        - Mal rendimiento
        - Errores 500 en los sitios web y problemas para procesar solicitudes

Ataques Informáticos

- **Ataques Web**
  - Una fuente valiosa para investigar este tipo de ataques son las bitácoras de los servidores de correo.
  - Una recomendación es siempre validar la hora del servidor contra la hora actual, ya que muchas veces vienen en horario UTC y nos pueden confundir.
  - Realice un manejo adecuado de los logs, cuide la sobreescritura.

Ataques Informáticos

- **Ataques Web**
    - Realice los ejercicios de laboratorio que le permitirán adquirir aún mayor experiencia sobre el tema.

Gracias

fidélitas Virtual