@ASLAN: Ingredientes para una óptima Estrategia de Seguridad en Cloud

ANADAT TECHNOLOGY

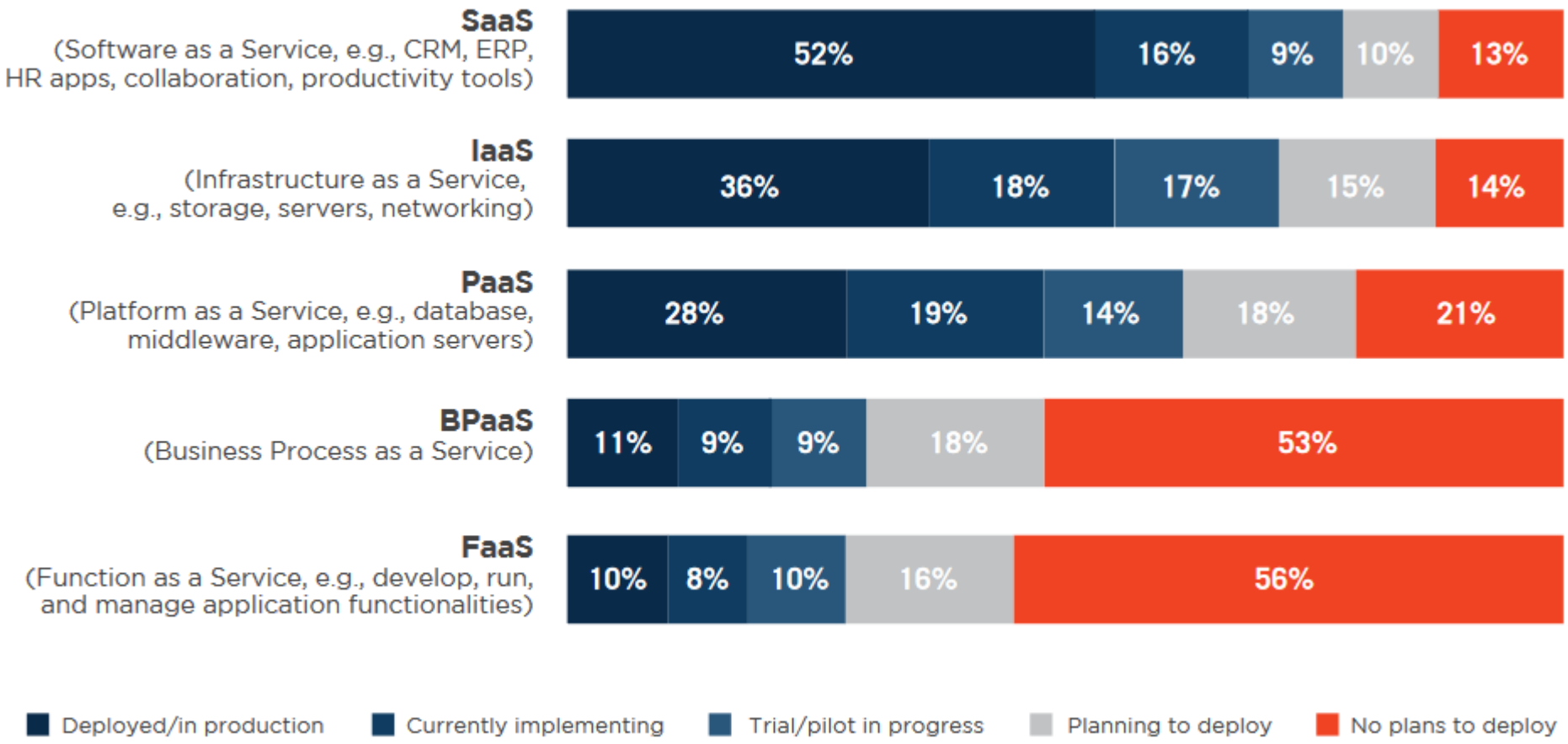
anadat technology Simplifying IT

Christiam José Carrillo Parada

christiam_carrillo@anadat.es

Ingeniero Técnico en Telecomunicaciones ULPGC
Postgrado en Ciberseguridad UC3M
Responsable Área Preventa en Ciberseguridad ANADAT TECHNOLOGY
+11 años de experiencia Arquitecto Seguridad de la Información

Consumo actual de Cloud Pública

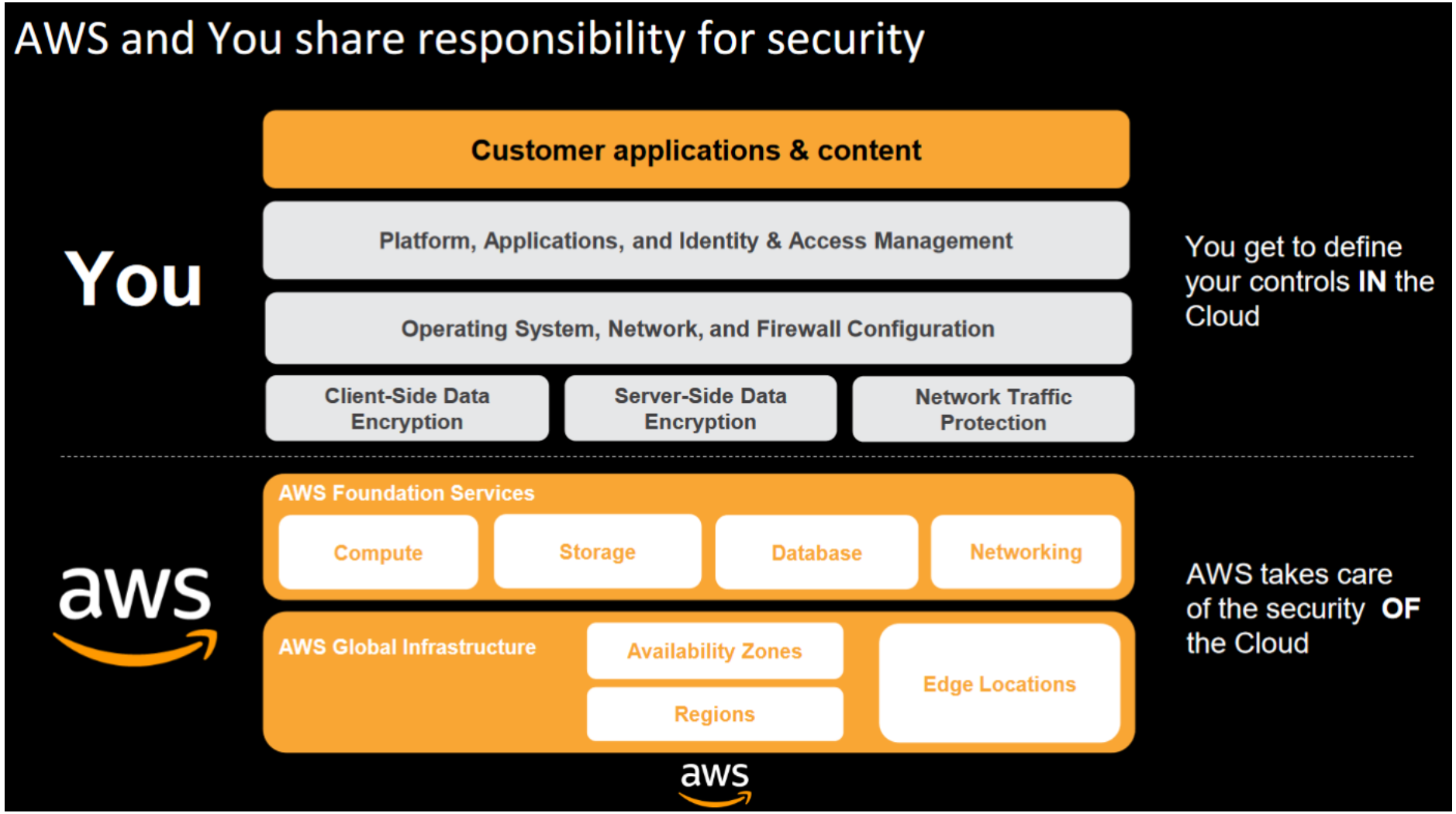


Fuente: Cloud Security Report 2018 Cybersecurity Insiders

Modelo de Seguridad Compartida

- ¿Qué hace el proveedor?
- ¿Qué necesita hacer el consumidor?
- ¿El proveedor de servicios en la nube permite al consumidor hacer lo que necesita?
- ¿Qué está garantizado en los contratos y en el acuerdo de nivel de servicio, y qué implica la documentación y los detalles de la tecnología?

Modelo de Seguridad Compartida (Ejemplo: AWS)



Modelo de Seguridad Compartida

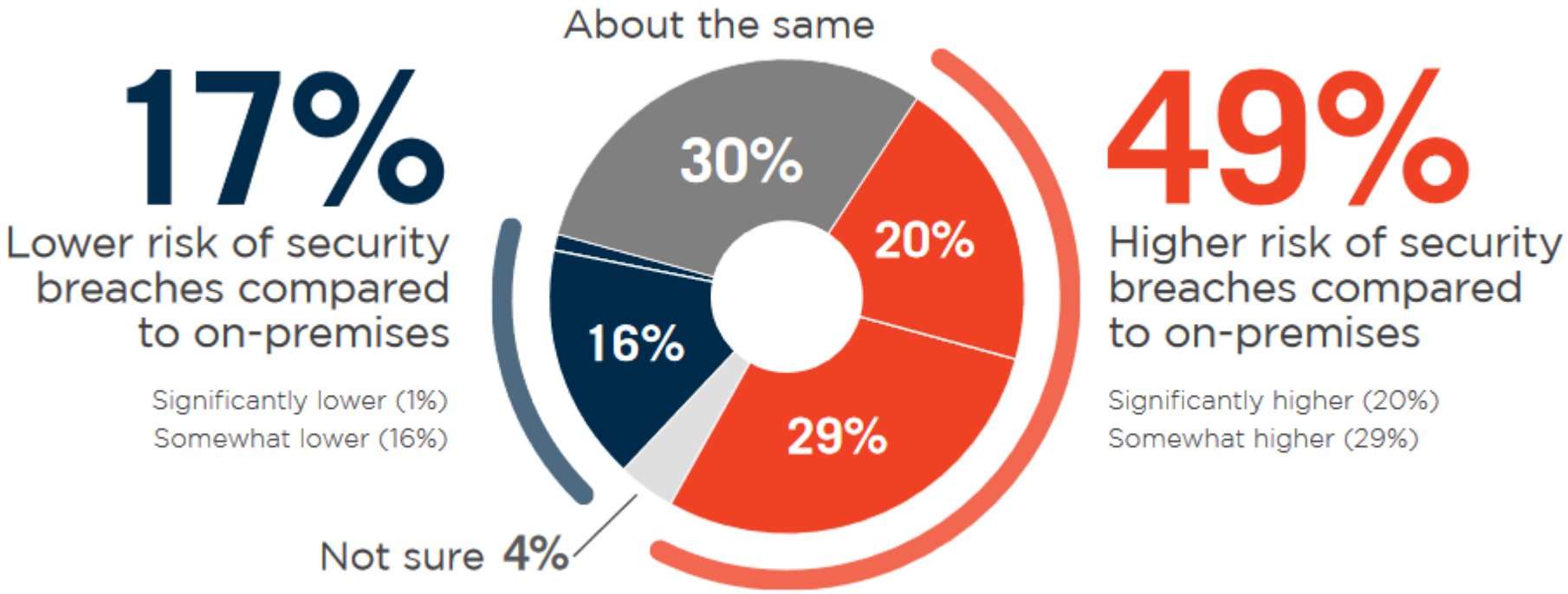
APPLICATION SECURITY

Fresh Spectre Vulnerabilities May Force Cloud Providers to Disable Intel Hyper-Threading

15 May 2019 2:53pm, by Joab Jackson

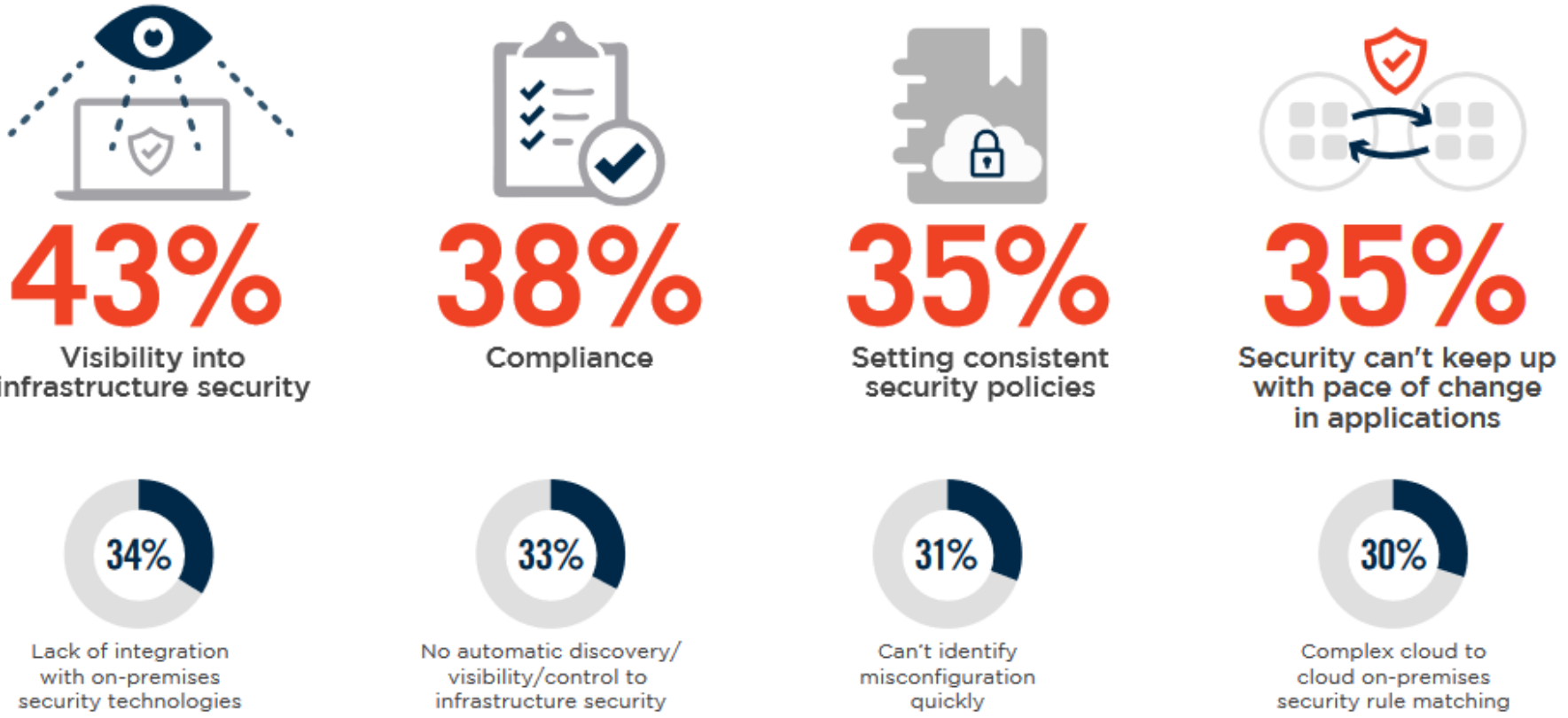
ZOMBIELOAD

Comparativa nivel de riesgo Cloud Pública vs OP



Fuente: Cloud Security Report 2018 Cybersecurity Insiders

Top Principales Desafíos en Ciberdefensa de Cloud Pública



Fuente: Cloud Security Report 2018 Cybersecurity Insiders

Top Amenazas Principales Cloud Pública

#1

Misconfiguration of the cloud platform/wrong set-up

62%

#2

Unauthorized access

55%

#3

Insecure interfaces /APIs

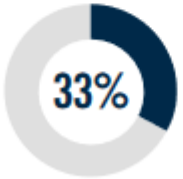
50%

#4

Hijacking of accounts, services or traffic

47%

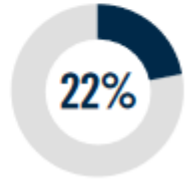
External sharing of data



Foreign state sponsored cyberattacks

Malicious insiders

Malware/ ransomware



Denial of service attacks

Fuente: Cloud Security Report 2018 Cybersecurity Insiders

Sistemas, Herramientas y Controles de Seguridad nativos Cloud

On-Premise	AWS	Azure	Google
Firewall &ACL	Security Groups	Network Security Groups	Cloud Armor VPC FW
IPS/IDS	3rd party only	3rd party only	3rd party only
WAF	AWS WAF	Application Gateway	Cloud Armor
SIEM	Security Hub Guard Duty	Advanced Log Analytics	Sta…
Antimalware	3rd party only	Microsoft Anti…	
PAM	3rd party only		…rty only
DLP	Amazon Made		Cloud DLP API
Vulnerability Assesment	Amazon Inspector. Trusted Advisor	Azure Security Center	Cloud Security Scanner
E-mail Protection	3rd party only	Office ATP	Embedded G-Suite
SSL Decryption	ELB	Application Gateway	HTTPS Load Balancing

PAY AS YOU GO!

On-Premise	AWS	Azure	Google
IAM	IAM	Azure AD	Cloud IAM
MFA	AWS MFA	Azure AD	Security Key enforcement
	…party only	Microsoft Defender	3rd party only
	AWS Certificate Manager	3rd party only	3rd party only
…ontainer Security	EC2 Container Service	Azure Container Service	Kubernetes Engine
VPN	VPC Customer Gateway	Virtual Network SSTP	Google VPN
Key Mgmt	KMS	Key Vault	Cloud Key Mgmt Service
DDoS	AWS Shield	Built-in DDoS Defense	Cloud Armor

Puntos clave Estrategia Seguridad Cloud

Seguir un modelo de arquitectura de referencia de seguridad en Cloud

Dotación de capacidad humana especializada en la materia

Evaluar el cumplimiento normativo y de buenas prácticas en seguridad de los CI de los servicios a consumir (p.e.: APIs, gestión de claves, etc.)

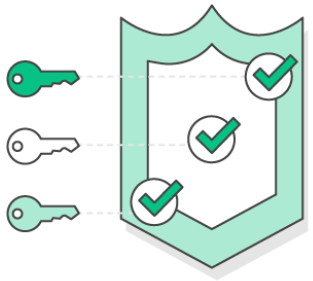
Formar y entrenar al equipo actual

Alianza con MSSP

Puntos clave Estrategia Seguridad Cloud

ML

Sistema maduro de gestión de accesos e identidades y gestión de privilegios incluyendo Múltiple Factor de Autenticación



Sistema de prevención de fuga de información con mecanismos de UEBA

Herramientas nativas Cloud

3rd Party vendors

Cifrado datos en reposo y en tránsito bien mediante herramientas nativas del Cloud o bien 3rd Party

GDPR

Ley de Secretos Empresariales

Puntos clave Estrategia Seguridad Cloud

ML

ML para Protección de las Comunicaciones

REGRESIÓN: predecir trafico anómalo en la red

CLASIFICACIÓN: identificar diferentes clases de ataques en red como spoofing, MITM, etc.

CLUSTERING: ayuda en análisis forense

ML

ML para Protección del Endpoint

REGRESIÓN: predecir siguiente llamada al sistema de un proceso y compararlo con el que realmente se esta ejecutando

CLASIFICACIÓN: clasificación de malware

CLUSTERING: protección malware en e-mail security gateways separando adjuntos legítimos del resto

Herramientas nativas Cloud

3rd Party vendors

servicios de seguridad del proveedor. P.e.: AWS CloudTrail, VPC Flow Logs. CloudWatch Logs, GuardDuty

¡Muchas Gracias por su atención!

anadat technology Simplifying IT