A Migração do Datacenter de um Banco para a Nuvem na Perspectiva do CSO

ESTUDO DE CASO

Ferramentas Open Source para Ajudar

- Feitas pela AWS
  - Trusted Advisor

  - http://github.com/awslabs
    - 344 repositórios

  - http://github.com/awslabs/aws-security-automation
    - Coleção de scripts e recursos para DevSecOps, Automação da Segurança e Resposta a incidentes automatizada

  - https://github.com/awslabs/aws-security-benchmark
    - Testar uma conta AWS contra CIS Amazon Web Services Foundations Benchmark

TLP:WHITE

Ferramentas Open Source para Ajudar

- De outras fontes
  - ThreatResponse.cloud
    - https://threatresponse.cloud
    - Toolkit Open Source para Resposta a Incidentes
  - StreamAlert
    - https://github.com/airbnb/streamalert
    - Framework para análise de dados (tipo um SIEM serverless)
  - Security Monkey
    - https://github.com/Netflix/security_monkey
    - Monitoramento de AWS/GCP para mudanças de política e alerta sobre configurações inseguras

TLP:WHITE

Ferramentas Open Source para Ajudar

- De outras fontes
  - CloudSploit
    - https://github.com/cloudsploit
    - Scan de riscos de segurança na AWS
  - Prowler
    - https://github.com/Alfresco/prowler
    - Ferramenta CLI para *assessment* de melhores práticas de segurança na AWS, auditoria, *hardening* e análise forense.
  - Cloud Custodian
    - http://cloudcustodian.io
    - Mecanismo de regras *multicloud* para gerenciamento de contas e recursos

TLP:WHITE

Fontes de Estudo

- **Página dos whitepapers AWS**

- Well Architected Framework – Pilar Segurança

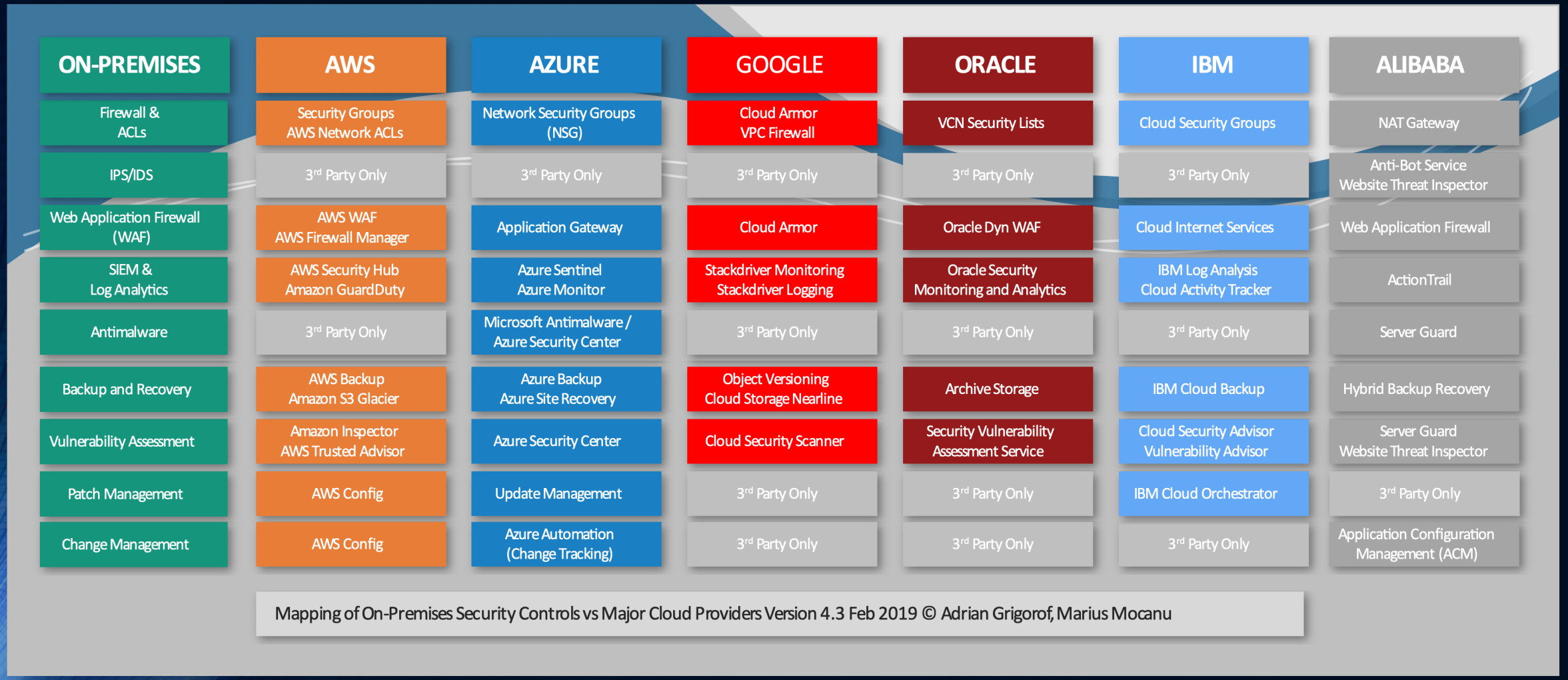
- CIS Amazon Web Services Foundations Benchmark
  - CloudFormation
  - Github AWS Labs – AWS Security Benchmark

- CIS Amazon Web Services Three-tier Web

- Google!

TLP:WHITE

Fontes de Estudo



ON-PREMISES	AWS	AZURE	GOOGLE	ORACLE	IBM	ALIBABA
Firewall & ACLs	Security Groups AWS Network ACLs	Network Security Groups (NSG)	Cloud Armor VPC Firewall	VCN Security Lists	Cloud Security Groups	NAT Gateway
IPS/IDS	3rd Party Only	3rd Party Only	3rd Party Only	3rd Party Only	3rd Party Only	Anti-Bot Service Website Threat Inspector
Web Application Firewall (WAF)	AWS WAF AWS Firewall Manager	Application Gateway	Cloud Armor	Oracle Dyn WAF	Cloud Internet Services	Web Application Firewall
SIEM & Log Analytics	AWS Security Hub Amazon GuardDuty	Azure Sentinel Azure Monitor	Stackdriver Monitoring Stackdriver Logging	Oracle Security Monitoring and Analytics	IBM Log Analysis Cloud Activity Tracker	ActionTrail
Antimalware	3rd Party Only	Microsoft Antimalware / Azure Security Center	3rd Party Only	3rd Party Only	3rd Party Only	Server Guard
Backup and Recovery	AWS Backup Amazon S3 Glacier	Azure Backup Azure Site Recovery	Object Versioning Cloud Storage Nearline	Archive Storage	IBM Cloud Backup	Hybrid Backup Recovery
Vulnerability Assessment	Amazon Inspector AWS Trusted Advisor	Azure Security Center	Cloud Security Scanner	Security Vulnerability Assessment Service	Cloud Security Advisor Vulnerability Advisor	Server Guard Website Threat Inspector
Patch Management	AWS Config	Update Management	3rd Party Only	3rd Party Only	IBM Cloud Orchestrator	3rd Party Only
Change Management	AWS Config	Azure Automation (Change Tracking)	3rd Party Only	3rd Party Only	3rd Party Only	Application Configuration Management (ACM)

Mapping of On-Premises Security Controls vs Major Cloud Providers Version 4.3 Feb 2019 © Adrian Grigorof, Marius Mocanu

http://www.eventid.net/docs/onprem_to_cloud.asp

TLP:WHITE