Nuvem e Cibersegurança

FEBRABAN
/CYBER LAB

Laboratório de Segurança Cibernética - 16/07/2025

TLP:AMBER

Traffic Light Protocol (TLP) Amber: Divulgação limitada aos participantes da organização. Destinatários podem compartilhar essas informações apenas com membros da própria organização que necessitem saber o conteúdo para tomada de ações cabíveis

Magno Logan – Instrutor GoHacking

FEBRABAN / CYBER LAB

- Especialista em Segurança da Informação, atuando no Canadá, liderando o programa de Security Champions
- Background em desenvolvimento com +15 anos de XP com AppSec, DevSecOps, Containers e K8s
- Implantou diversas ferramentas de AppSec em pequenas e grandes empresas (SAST, DAST, SCA, Secret Scanning)
- Possui diversas certificações da SANS, CompTIA, EC-Council AWS, Microsoft e EXIN
- Palestrante em diversas conferências internacionais como DEFCON, OWASP AppSec, NorthSec, H2HC, KubeCon, etc.

Magno Logan – Instrutor GoHacking

Agenda

1. Principais conceitos sobre nuvem
2. Principais tecnologias e provedores de nuvem
3. Modelos de serviços em nuvem
4. Principais ameaças
5. Mecanismos básicos de proteção

Principais Conceitos sobre Nuvem

FEBRABAN
/CYBER LAB

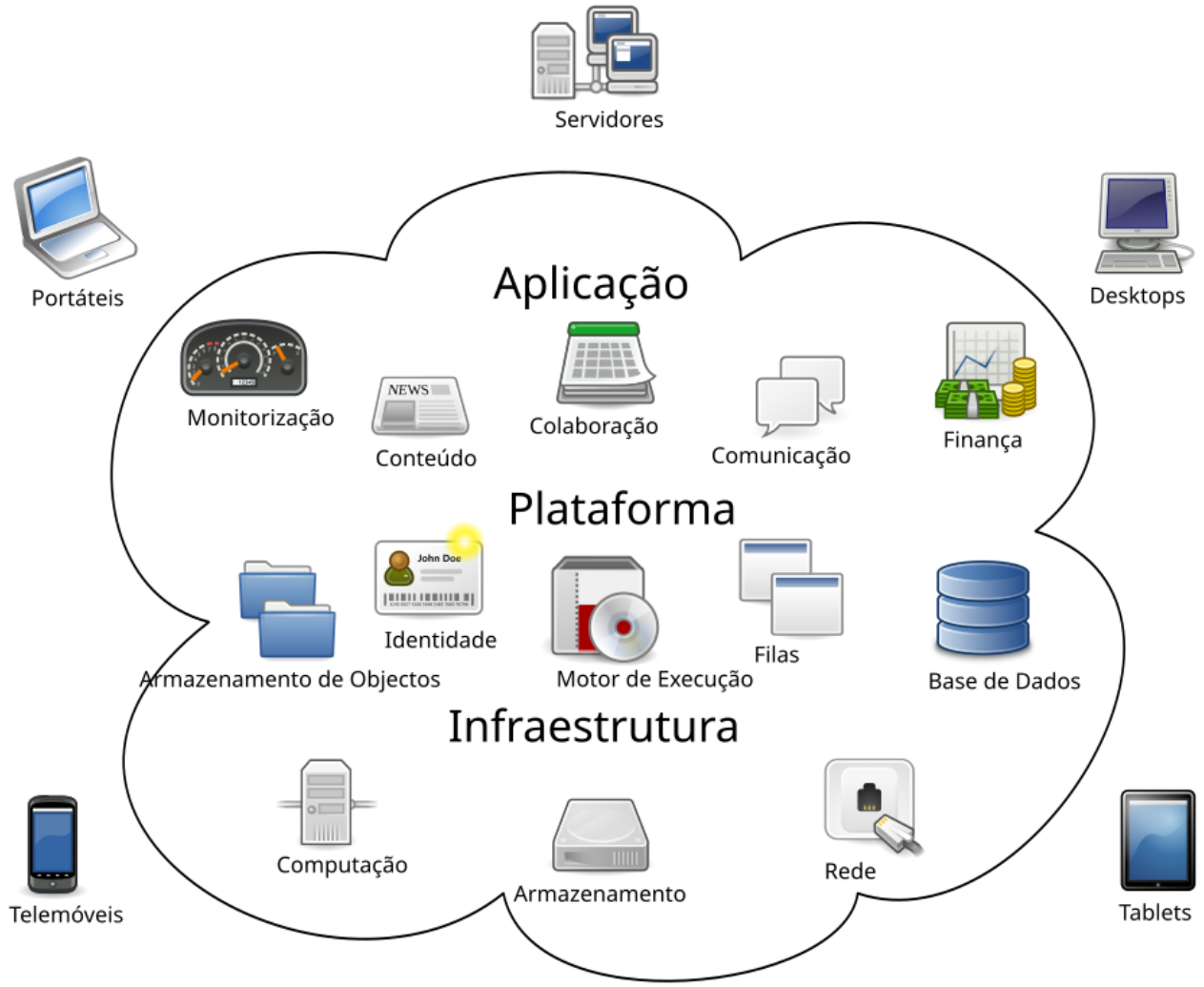
O que é Computação em Nuvem?

FEBRABAN
/CYBER LAB

Conceito Básico

- É o fornecimento de recursos de computação (como servidores, armazenamento, bancos de dados, redes, software) pela internet
- Ao invés de armazenar dados e rodar aplicativos no seu computador pessoal, você usa servidores remotos acessíveis via internet

O que é Computação em Nuvem?



https://pt.wikipedia.org/wiki/Computa%C3%A7%C3%A3o_em_nuvem

O que é Computação em Nuvem?

FEBRABAN
/CYBER LAB

Vantagens Básicas

- Acessibilidade: acesse de qualquer lugar
- Escalabilidade: cresça ou reduza conforme a necessidade
- Economia: pague apenas pelo que usar

O que é Computação em Nuvem?

FEBRABAN
/CYBER LAB

Mais Vantagens

- Custos operacionais mais baixos
- Aumento de recursos de TI
- Acesso rápido e conveniente à tecnologia
- Maior escala e automação
- Maior conformidade

O que é Computação em Nuvem?

FEBRABAN
/CYBER LAB

Desvantagens

- Dependência de fornecedor
- Estruturas de preços complexas
- Custos de transferência de dados de saída
- Um modelo de segurança compartilhada complexo
- Menos flexibilidade do que ambientes locais

Principais tecnologias e provedores

FEBRABAN
/CYBER LAB

Principais Tecnologias

FEBRABAN
/CYBER LAB

Tecnologias Envolvidas

- Virtualização
- Containers (como Docker)
- Redes definidas por software
- Armazenamento distribuído

Provedores de Nuvem

Provedores Mais Conhecidos

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- Outros: IBM Cloud, Oracle Cloud,

Modelos de serviços em nuvem

FEBRABAN
/CYBER LAB

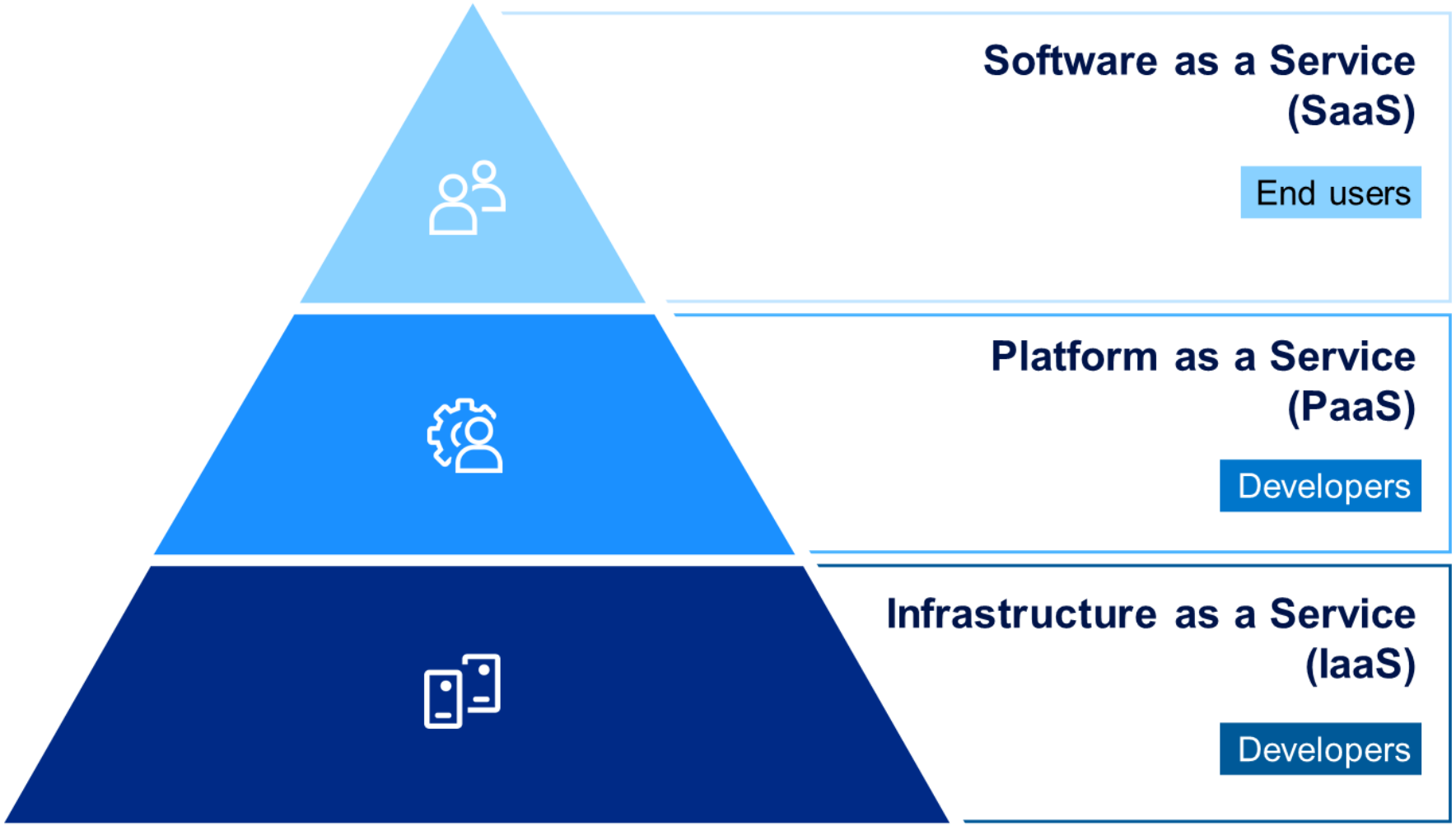
Modelos de Serviço em Nuvem

FEBRABAN
CYBER LAB

- **Tipos de Serviço**

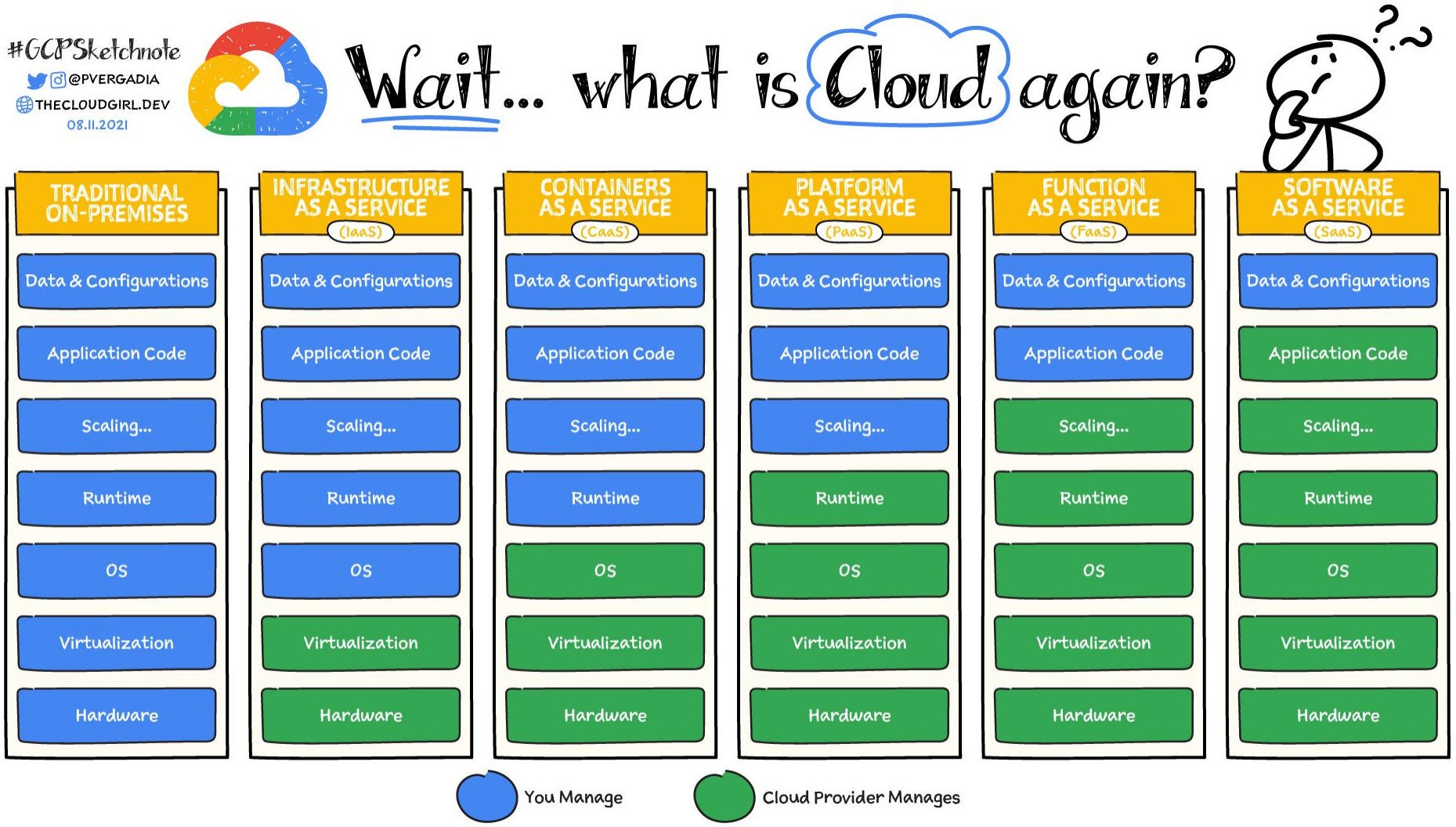
Modelo	O que é fornecido?	Exemplo
IaaS (Infraestrutura como Serviço)	Servidores, redes, armazenamento	AWS EC2
PaaS (Plataforma como Serviço)	Ambiente para desenvolvimento de apps	Google App Engine
SaaS (Software como Serviço)	Aplicativos prontos para uso	Gmail, Netflix, Office 365

Modelos de Serviço em Nuvem



https://learning.sap.com/learning-journeys/explore-sap-cloud-erp/differentiating-cloud-service-models

Modelos de Serviço em Nuvem



https://cloud.google.com/learn/paas-vs-iaas-vs-saas

Principais Ameaças

FEBRABAN
/CYBER LAB

Ameaças Gerais na Nuvem

FEBRABAN
CYBER LAB

Riscos Comuns

- **Vazamento de dados**: dados sensíveis expostos por falhas ou ataques
- **Ataques de ransomware**: sequestro de arquivos com pedido de resgate
- **Configurações incorretas**: deixar a “porta aberta” sem querer
- **Acesso não autorizado**: credenciais fracas ou vazadas
- **Ataques internos**: funcionários mal-intencionados ou descuidados

As Top 11 Ameaças da Nuvem - CSA

FEBRABAN
CYBER LAB

Principais Ameaças Abordadas:

- Configuração incorreta e controle de alterações inadequado
- Gerenciamento de Identidade e Acesso (IAM)
- Interfaces e APIs inseguras
- Seleção/implementação inadequada da estratégia de segurança em nuvem
- Recursos de terceiros inseguros

https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024

As Top 11 Ameaças da Nuvem - CSA

- Desenvolvimento de software inseguro
- Divulgação acidental da nuvem
- Vulnerabilidades do sistema
- Visibilidade/observabilidade limitada da nuvem
- Compartilhamento de recursos não autenticado
- Ameaças Persistentes Avançadas (APT)

https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024

MITRE ATT&CK Framework

FEBRABAN
CYBER LAB

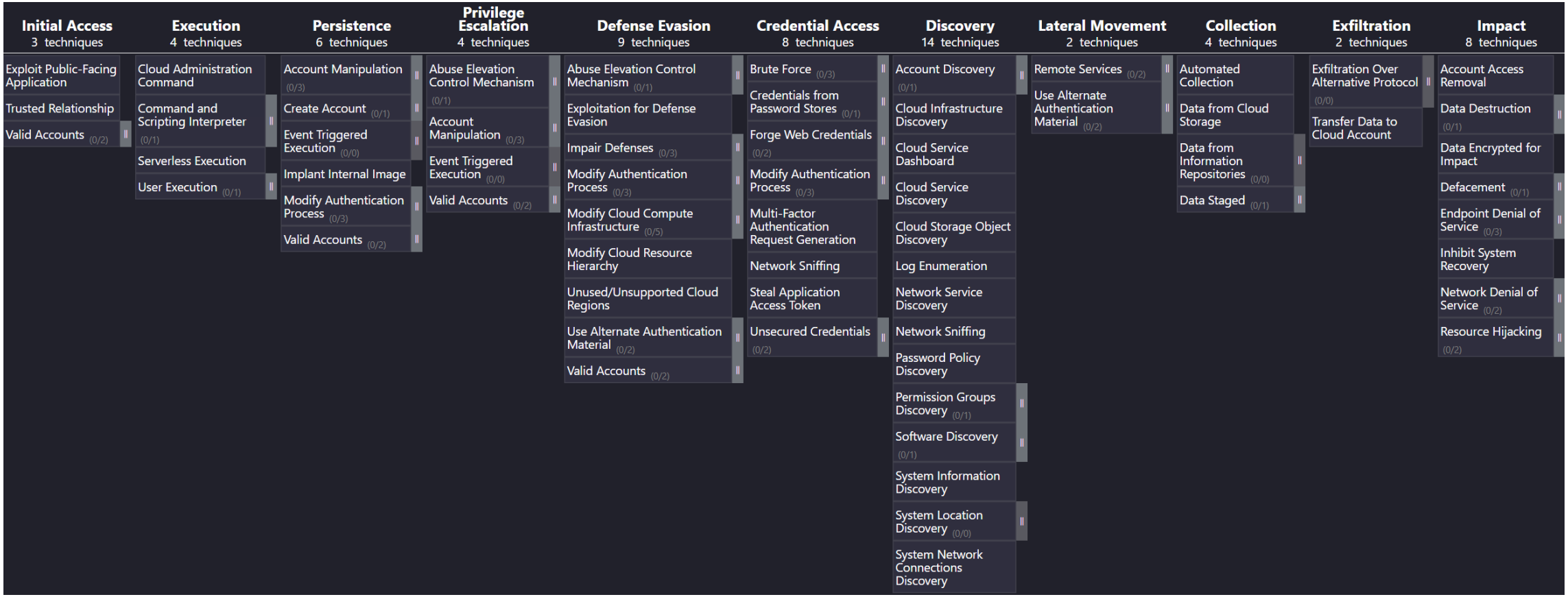
Táticas, Técnicas e Conhecimento Comum Adversarial - ATT&CK

- Base de conhecimento globalmente acessível sobre táticas e técnicas opostas, com base em cenários do mundo real
- Usado como base para o desenvolvimento de modelos e metodologias de ameaças específicas em diversos setores

https://attack.mitre.org/

MITRE ATT&CK Framework para Nuvem (IaaS)

FEBRABAN / CYBER LAB



https://attack.mitre.org/matrices/enterprise/cloud/iaas/

Mecanismos de Proteção

FEBRABAN
/CYBER LAB

Mecanismos Básicos de Proteção

FEBRABAN
/CYBER LAB

Boas Práticas

- **Autenticação multifator (MFA)**: não confie só na senha
- **Criptografia**: proteger dados em trânsito e em repouso
- **Backups**: sempre tenha cópias de segurança
- **Controle de acesso**: só quem precisa deve ter acesso
- **Atualizações e patches**: mantenha tudo atualizado
- **Monitoramento contínuo**: detectar atividades suspeitas cedo

Roteiro de Maturidade de Segurança da AWS

FEBRABAN
/CYBER LAB

- **Estágio 1:** Inventário
- **Estágio 2:** Ter backups
- **Estágio 3:** Visibilidade e correção inicial
- **Estágio 4:** Detecção
- **Estágio 5:** Acesso seguro ao IAM

https://summitroute.com/downloads/aws_security_maturity_roadmap-Summit_Route.pdf

Roteiro de Maturidade de Segurança da AWS

FEBRABAN
/CYBER LAB

- **Estágio 6:** Reduzir a superfície de ataque e mitigar comprometimentos
- **Estágio 7:** Reprodutibilidade e propriedade
- **Estágio 8:** Aprimorar a detecção e o refinamento de privilégios mínimos
- **Estágio 9:** Comunicações de rede seguras
- **Estágio 10:** Preparação para incidentes

https://summitroute.com/downloads/aws_security_maturity_roadmap-Summit_Route.pdf

Modelo de Maturidade de Segurança da AWS v2

FEBRABAN / CYBER LAB

CAF Níveis →	Start		Advance	Excel
CAF Capacidades ↓	Fase 1: Quick Wins	Fase 2: Fundação	Fase 3: Eficiência	Fase 4: Otimização
Security governance	Adicionar contatos de segurança Selecionar a(s) regiões	Identificar requerimentos regulatórios Plano de treinamento sobre segurança na nuvem	Projete sua arquitetura segura Uso de infraestrutura como código Tagging strategy	Compartilhar o trabalho e responsabilidade de segurança
Security assurance	Automatizar o alinhamento com melhores práticas com o AWS Security Hub	Inventario e Monitoramento das configurações	Crie seus relatórios para conformidade (como PCI-DSS)	Automatize a coleta de evidências
Identity and access management	Autenticação Multi-Fator Proteção da conta Root Repositório central de usuários com Federação do Identidades Limpar acessos não intencionais	GuardRails: Políticas Organizacionais - SCPs Use credenciais temporárias Instance Metadata Service (IMDS) v2	Revisão de privilégio mínimo Customer IAM: segurança de seus clientes	Perímetro de dados Pipeline de geração de políticas de IAM Acesso Elevado Temporário
Threat detection	Detecção de ameaças com o Amazon GuardDuty e revisão das descobertas Auditoria das chamadas de API com o AWS CloudTrail Alarmes de Billing	Detecção avançada de ameaças	detecção de ameaças personalizadas (SecLake / SIEM)	Inteligência de ameaças Análise de fluxos de rede (VPC Flow Logs)

https://maturitymodel.security.aws.dev/pt/model/

Modelo de Maturidade de Segurança da AWS v2

FEBRABAN / CYBER LAB

Vulnerability management		Gerenciar vulnerabilidades na sua infraestrutura e execução de pentesting Gerenciar as vulnerabilidades nas suas aplicações	Security Champions DevSecOps: segurança no pipeline	Equipe de gerenciamento de vulnerabilidades
Infrastructure protection	Cleanup risky open ports	limitar o acesso da rede Gestão segura de instâncias Segmentação de redes (VPCs) - Redes Públicas/Privadas Gestão multiconta	Pipeline de geração de imagens Anti-Malware / EDR / Runtime Protection Controle de tráfego de saída	Acceso Zero Trust Uso de serviços abstratos (Serverless)
Data protection	Block Public Access Analizar a postura de segurança de dados	Criptografia de Dados em repouso Backups Descoberta de dados sensíveis	Criptografia em trânsito	GenAI Data protection
Application security	WAF com regras gerenciadas	Envolver os times de segurança no desenvolvimento Sem segredos no Código	Criar uma modelagem de ameaças WAF com regras customizadas Mitigação avançada de DDoS (L7)	Formar um Red Team (Ponto de vista do atacante)
Incident response	Act on Critical Security Findings	Definir playbooks de respostas frente aos incidentes	Exercícios TableTop - Simulações Automatizar Playbooks críticos Investigações de Segurança - Análise de causa raiz	Formar um Blue Team (Resposta a incidentes) de segurança avançadas Orquestração de segurança & tickets Automatizar configuraÇões com correção de desvios
Resiliency	Avalie a resiliência	Redundância em múltiplas zonas de disponibilidade	Plan de Disaster Recovery	Automação do Disaster Recovery multi-região Formar uma time de Engenharia do Caos

https://maturitymodel.security.aws.dev/pt/model/

Conclusão

FEBRABAN
CYBER LAB

- A computação em nuvem transforma a forma como usamos tecnologia, mas também traz novas responsabilidades.
- Entender os conceitos básicos e adotar medidas simples de segurança pode fazer toda a diferença para proteger seus dados e sua privacidade
- "Na nuvem, conveniência e segurança devem caminhar juntas. A melhor defesa é o conhecimento."