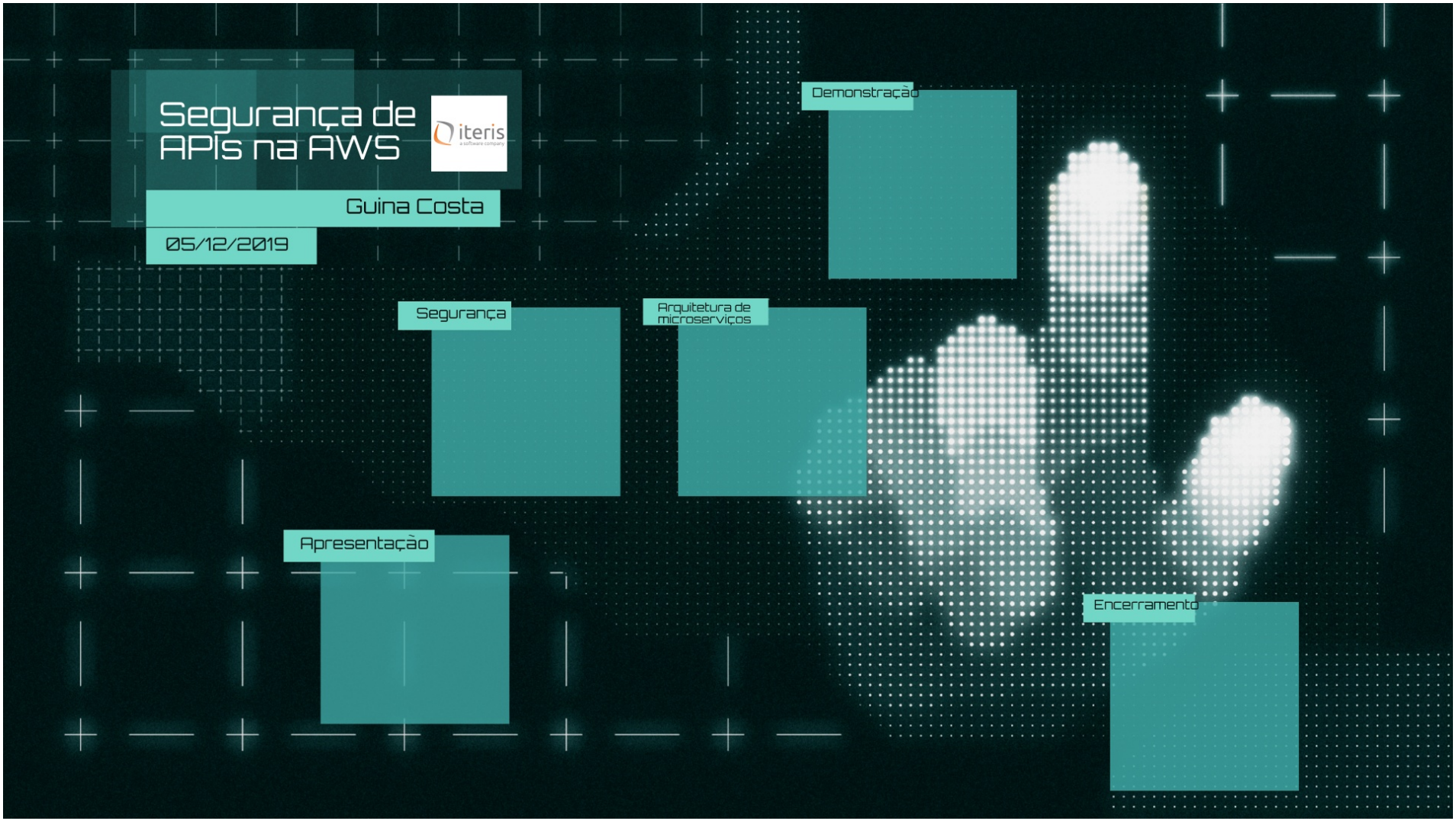

Segurança de APIs na AWS
iteris
a software company
Guina Costa
05/12/2019
Demonstração
Segurança
Arquitetura de microserviços
Apresentação
Encerramento

Agnaldo

Agnaldo Costa

Guina

Educação

Experiência

Guina

O Guina não tinha dó
Se reagir, bum, vira pó

Educação

Etec
Prof. Horácio Augusto da Silveira
São Paulo

Técnico em Informática (2009)

Tecnólogo em Análise de Sistemas (2014)

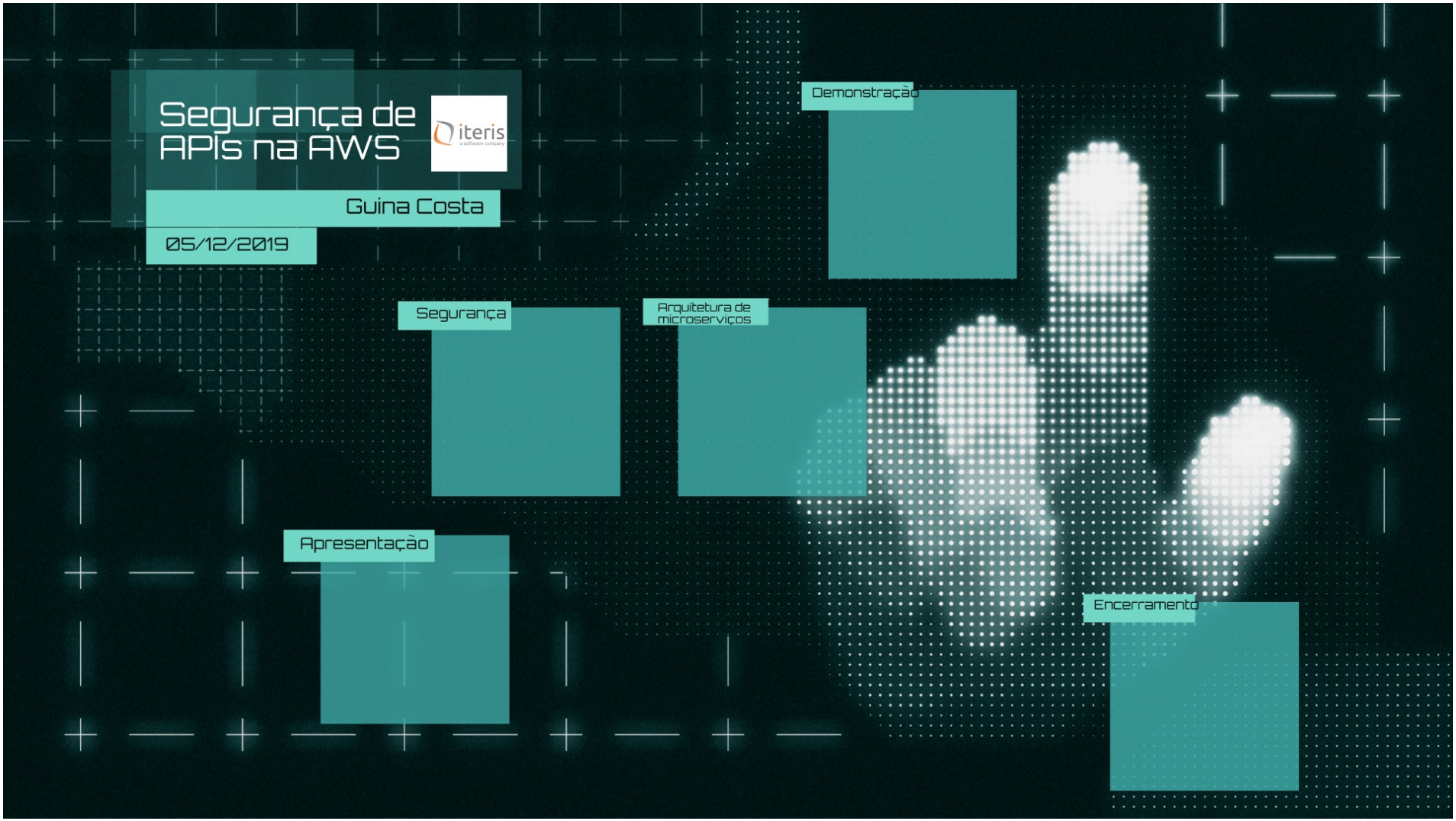
Fatec
São Paulo

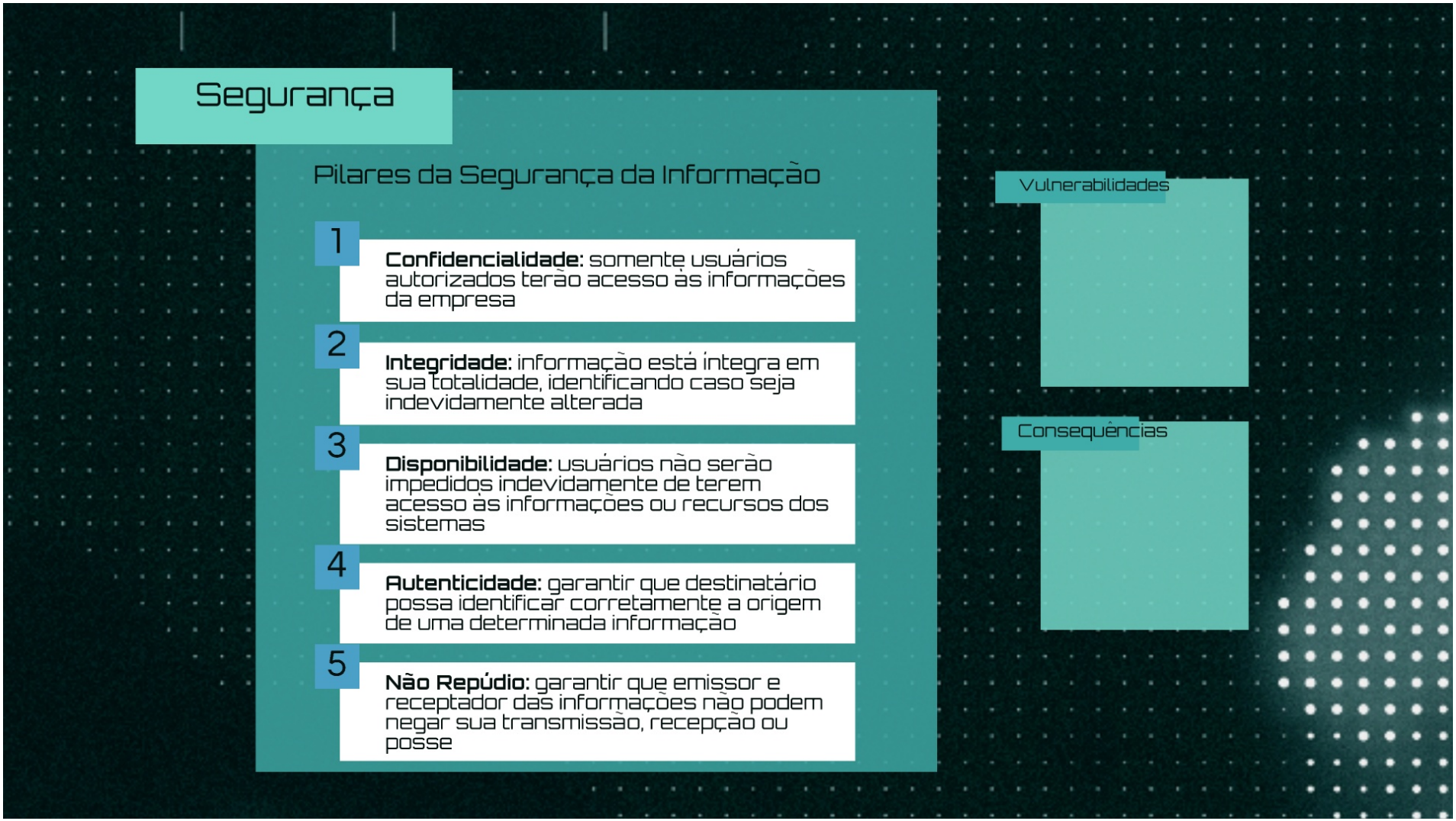
FIAP

Especialização em Engenharia de Software (2019)

Experiência

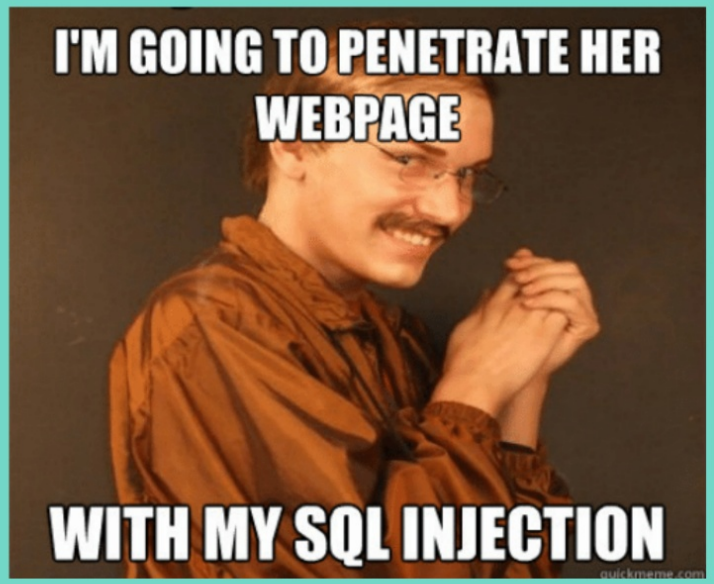
Trabalho com desenvolvimento desde 2010


Segurança de APIs na AWS
iteris
Guina Costa
05/12/2019
Demonstração
Segurança
Arquitetura de microserviços
Apresentação
Encerramento


Segurança
Pilares da Segurança da Informação
1
Confidencialidade: somente usuários autorizados terão acesso às informações da empresa
2
Integridade: informação está íntegra em sua totalidade, identificando caso seja indevidamente alterada
3
Disponibilidade: usuários não serão impedidos indevidamente de terem acesso às informações ou recursos dos sistemas
4
Autenticidade: garantir que destinatário possa identificar corretamente a origem de uma determinada informação
5
Não Repúdio: garantir que emissor e receptador das informações não podem negar sua transmissão, recepção ou posse
Vulnerabilidades
Consequências

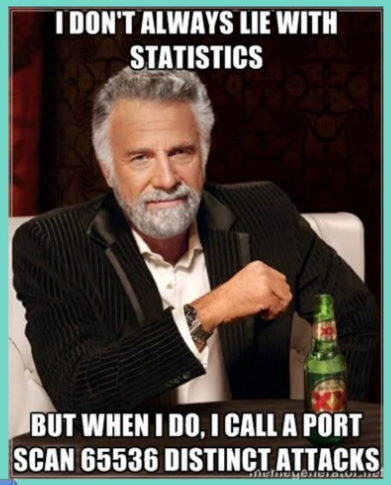

Vulnerabilidades
Meio pelo qual uma ameaça pode ocorrer, fatores que podem resultar em risco para um sistema ou organização
ataque comum 1
ataque comum 4
ataque comum 2
ataque comum 3

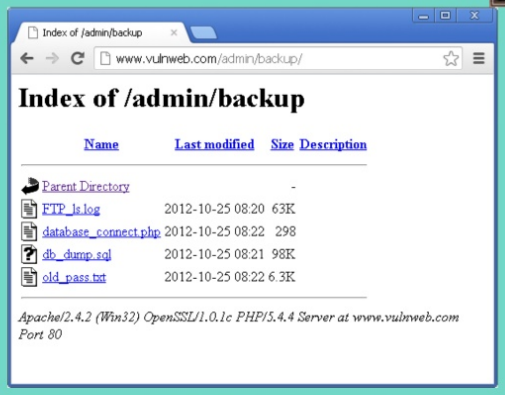
SQL Injection



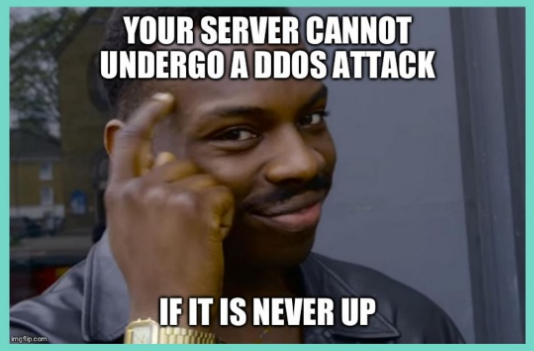
XSS (Cross-Site Scripting)

Scan e testes exploratórios



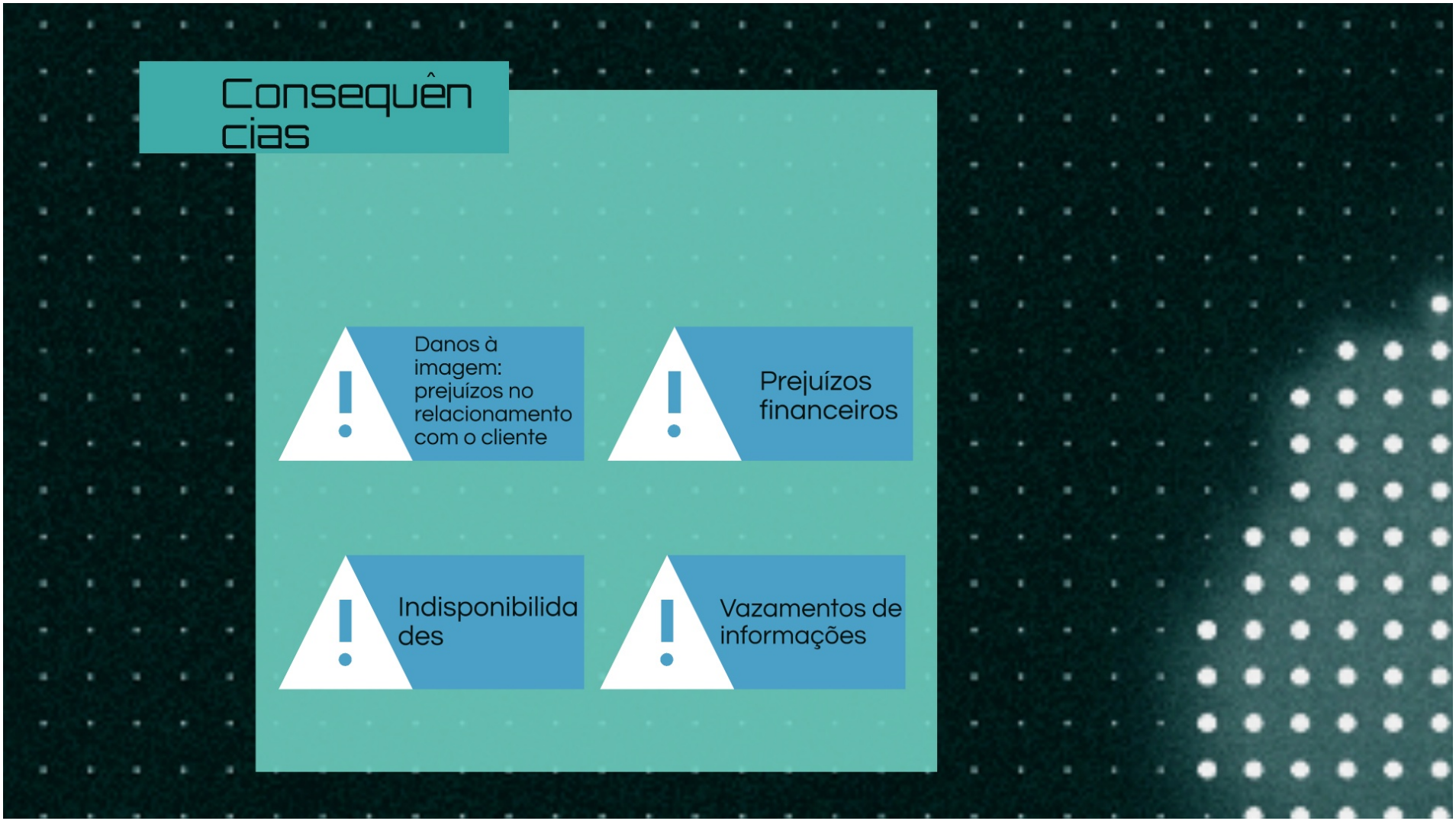


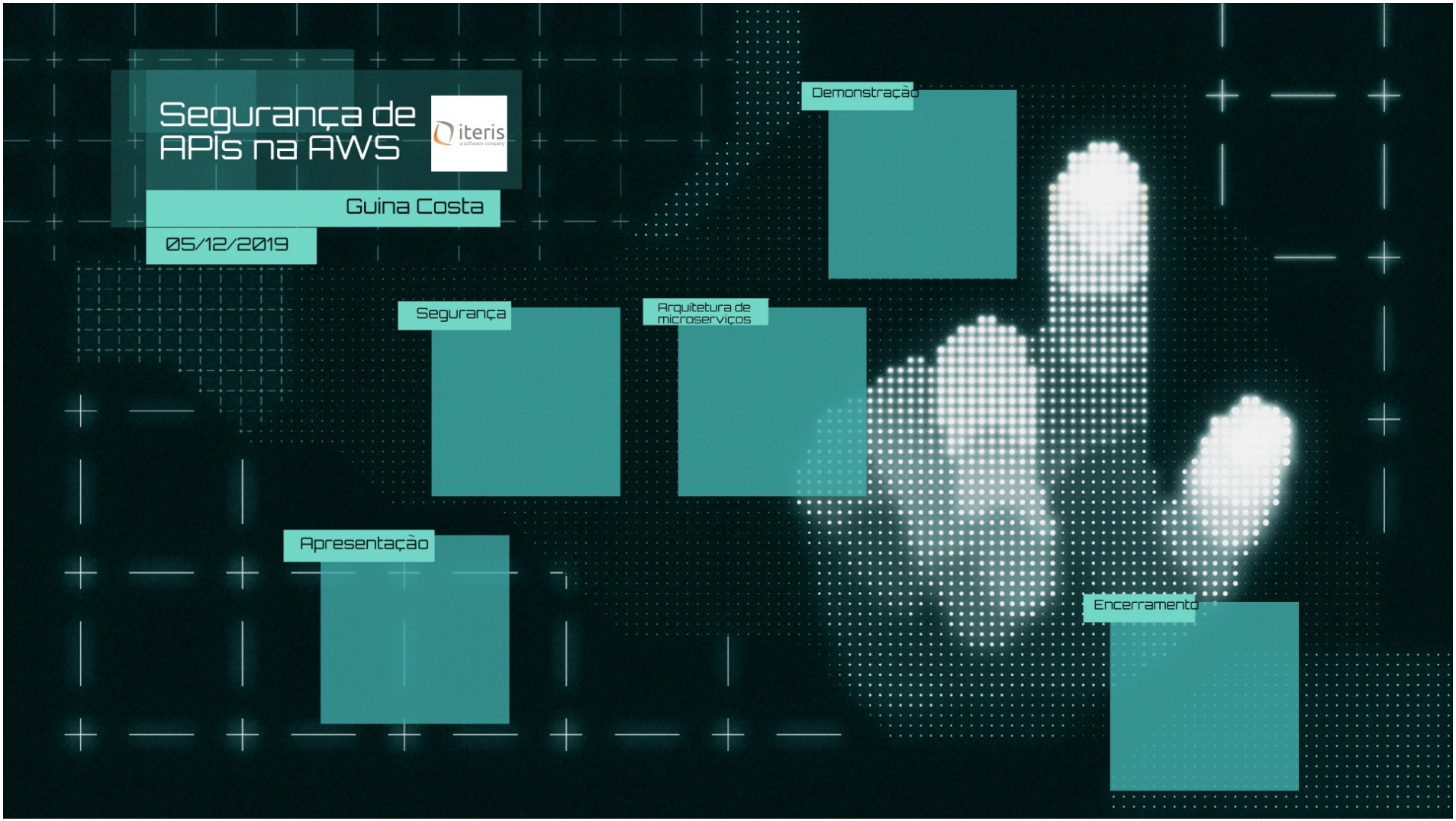
DDoS/DoS


YOUR SERVER CANNOT
UNDERGO A DDOS ATTACK
IF IT IS NEVER UP


SON GOKU
9:11
إنها مخيفة جداً !


YouTube
SON GOKU最強
9:11
إنها مخيفةٌ جداً !

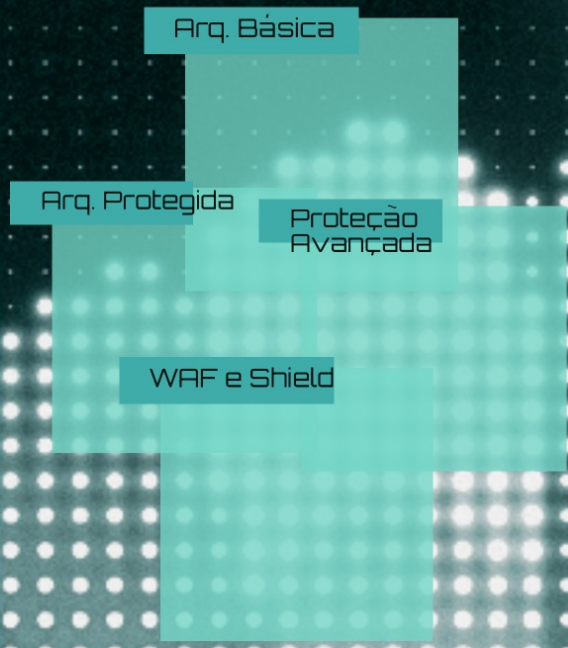

Consequências
Danos à imagem: prejuízos no relacionamento com o cliente
Prejuízos financeiros
Indisponibilidades
Vazamentos de informações


Segurança de APIs na AWS
iteris
a software company
Guina Costa
05/12/2019
Demonstração
Segurança
Arquitetura de microserviços
Apresentação
Encerramento

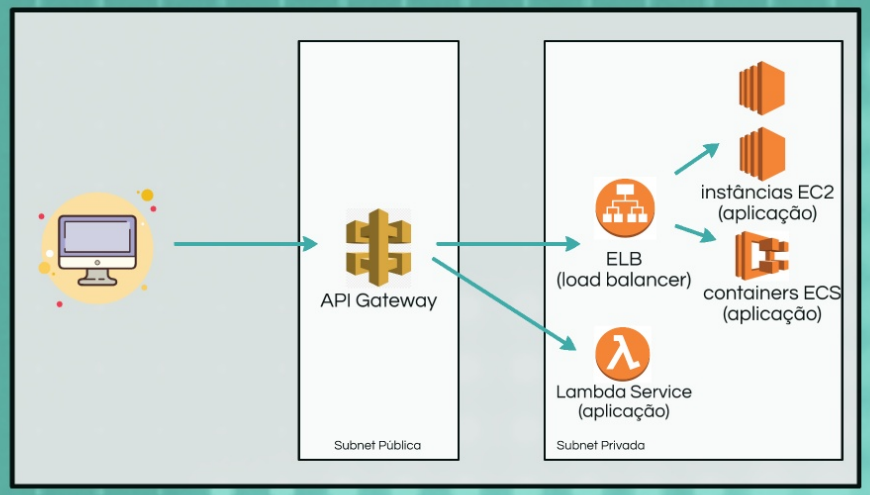
Arquiteturas

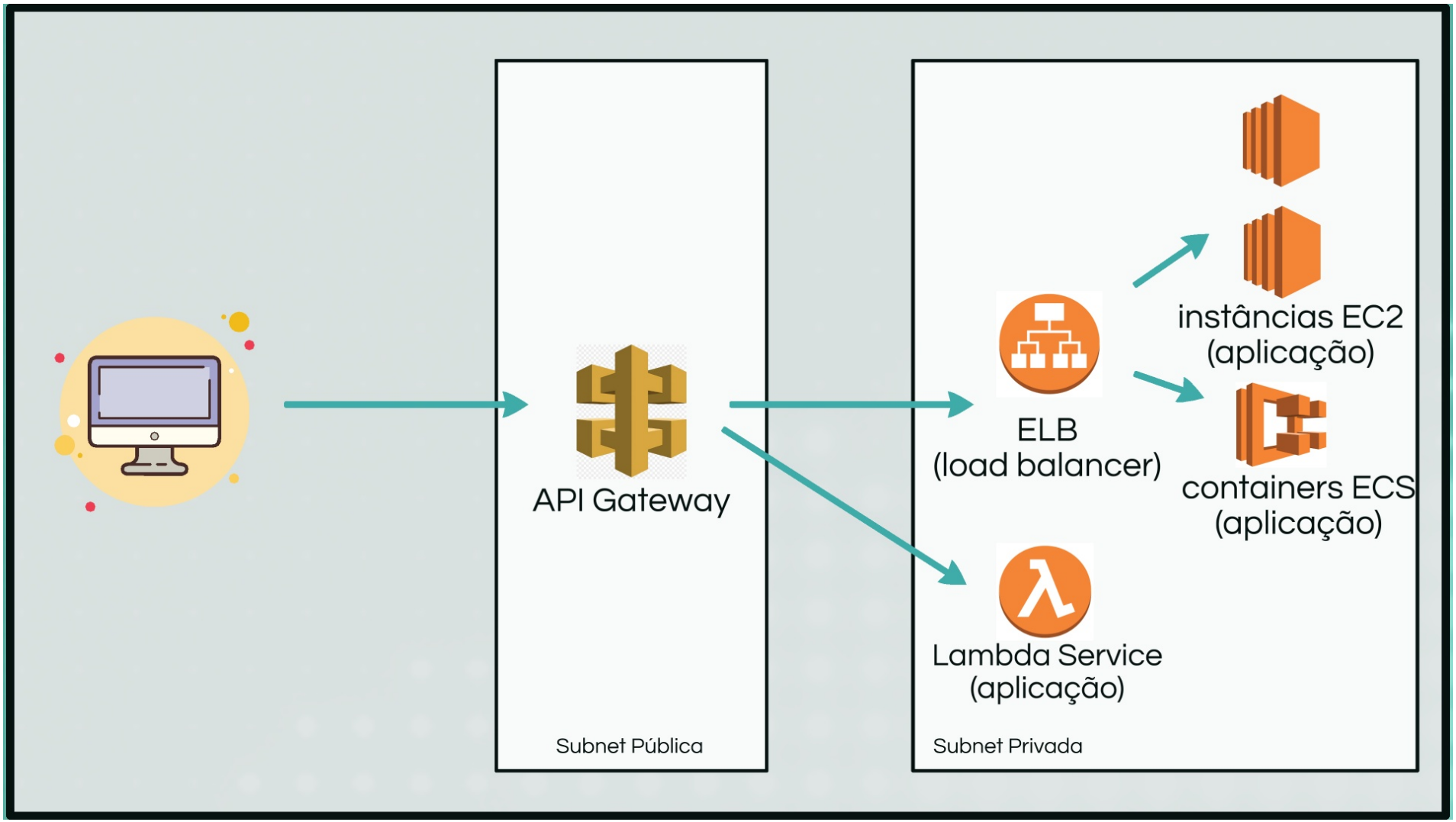
Arquiteturas baseadas em serviços da AWS

- Arquiteturas básicas de aplicação
- Arquitetura com aceleração e proteção básica de aplicação
- Arquitetura de proteção avançada



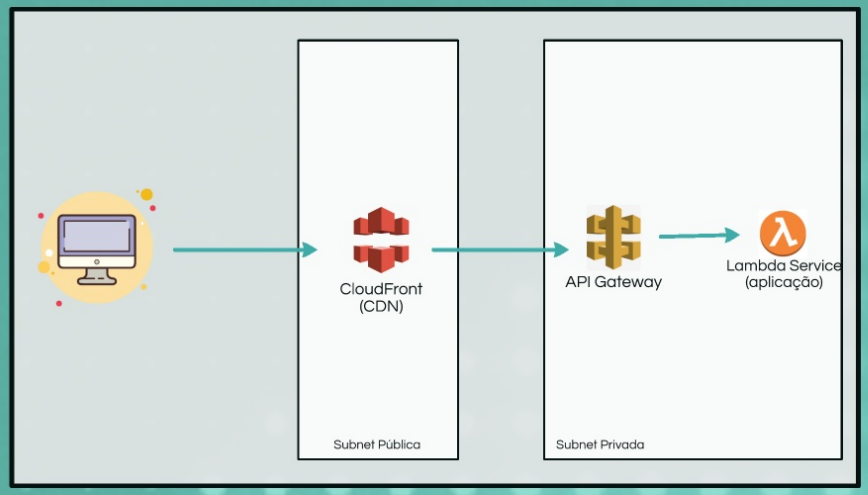
Arquitetura básica

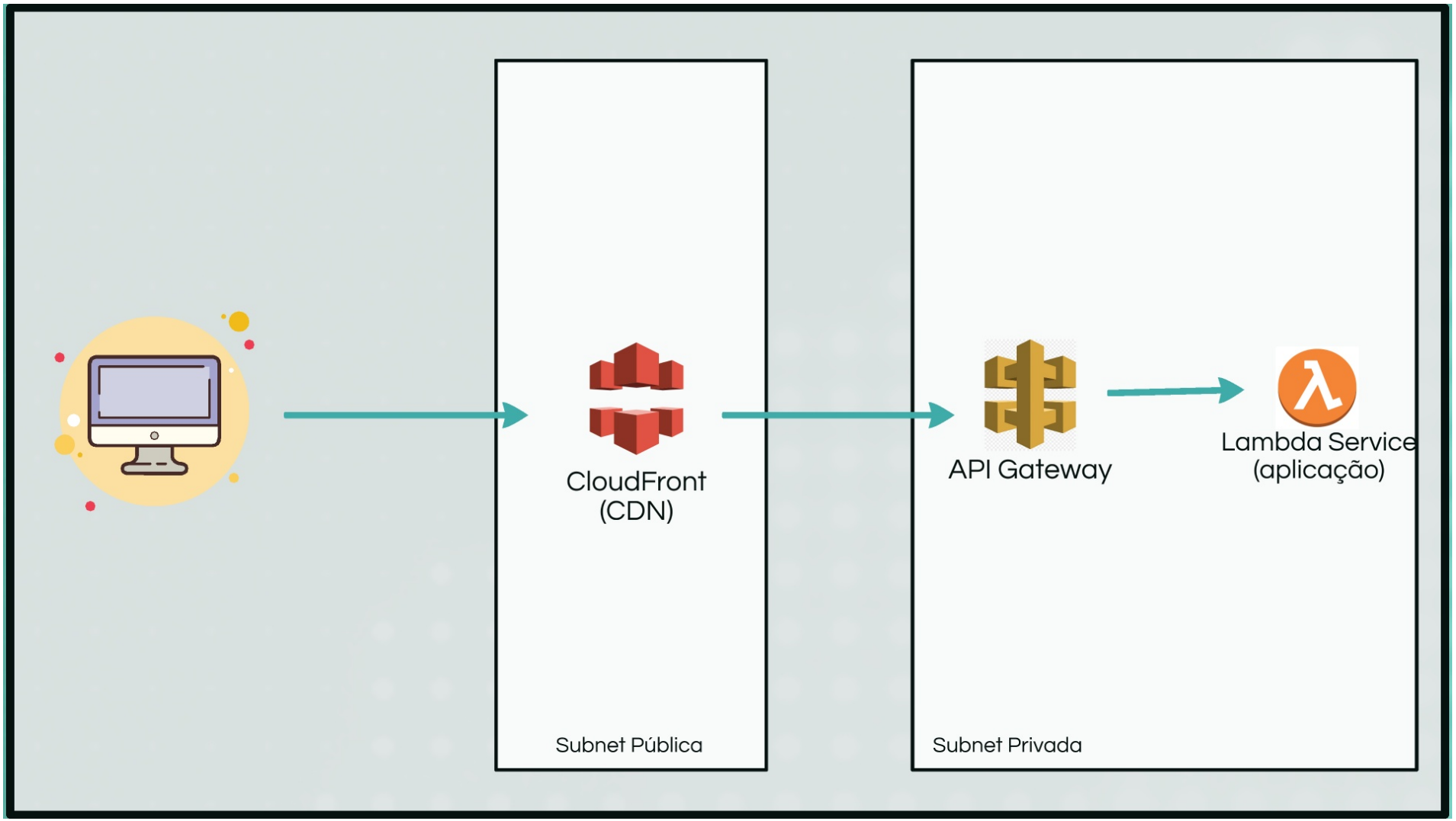



API Gateway
Subnet Pública
ELB
(load balancer)
instâncias EC2
(aplicação)
containers ECS
(aplicação)
Lambda Service
(aplicação)
Subnet Privada

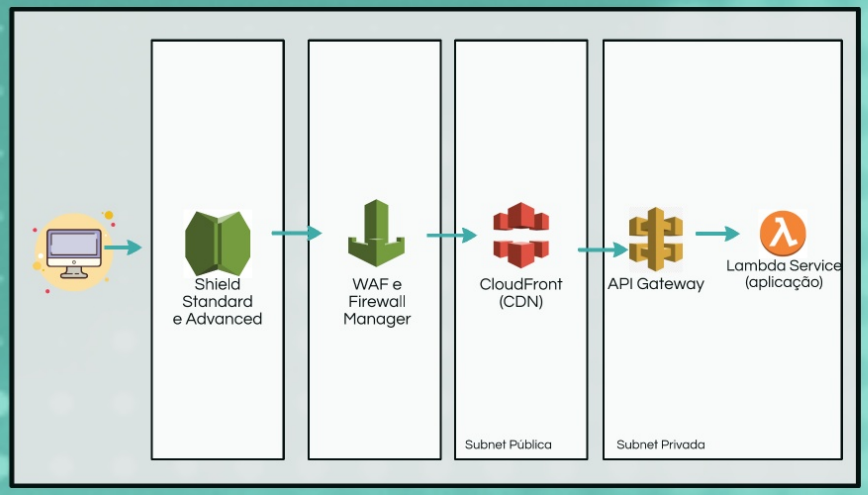
Arquitetura protegida

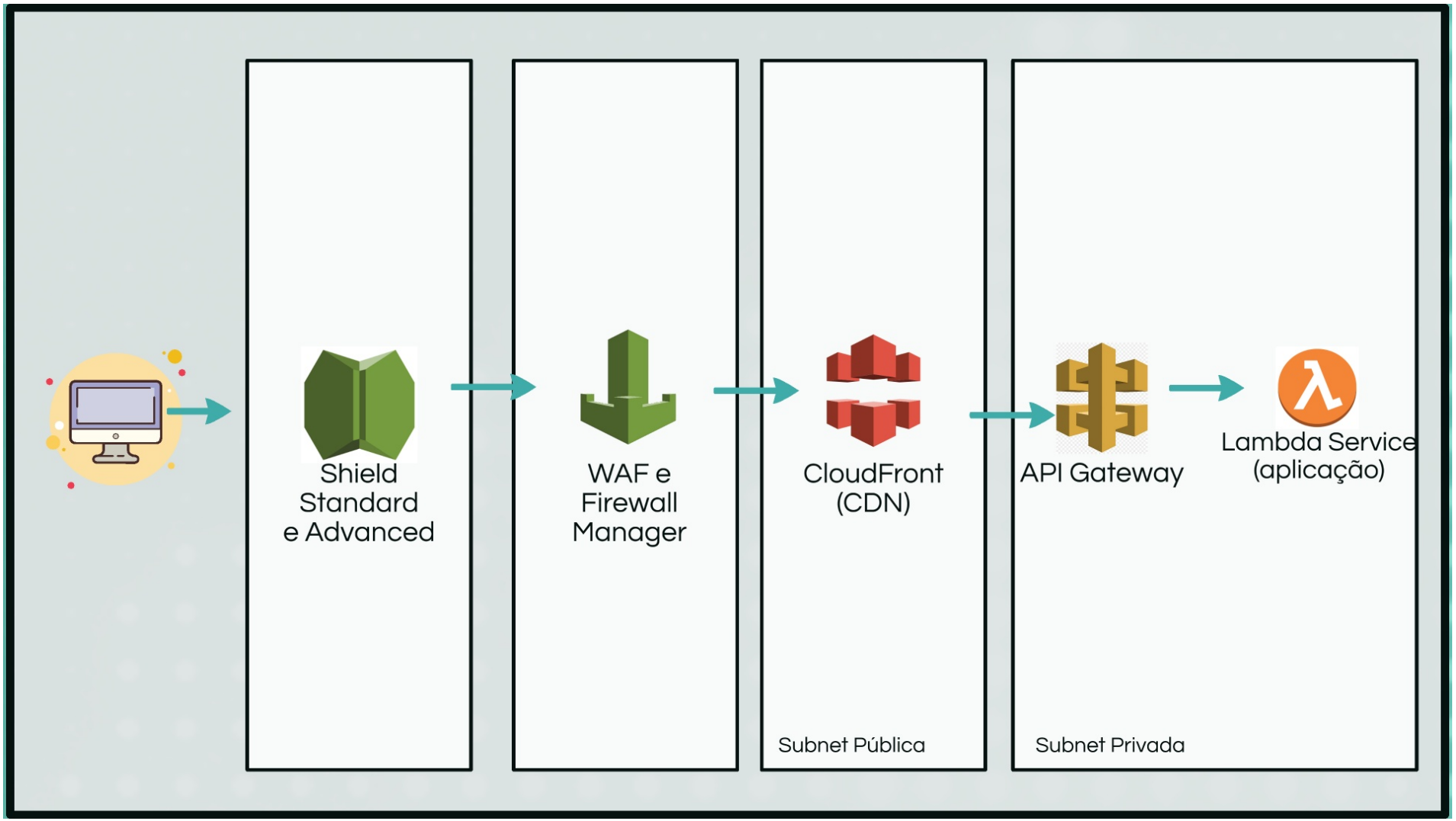
Protegendo e acelerando a aplicação




CloudFront
(CDN)
API Gateway
Lambda Service
(aplicação)
Subnet Pública
Subnet Privada

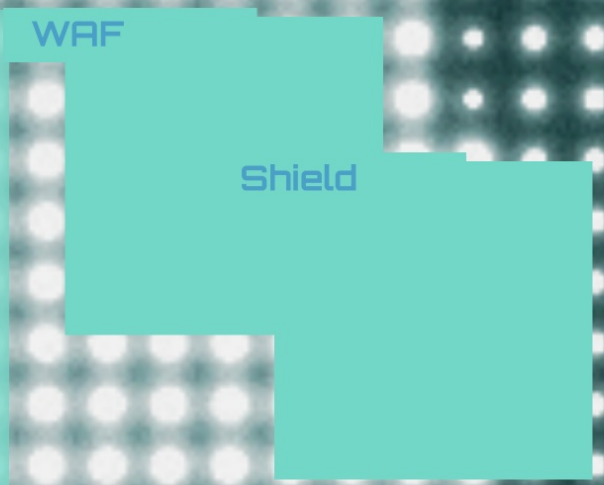
Proteção avançada




Shield
Standard
e Advanced
WAF e
Firewall
Manager
CloudFront
(CDN)
API Gateway
Lambda Service
(aplicação)
Subnet Pública
Subnet Privada

WAF e Shield

- criação de recursos de segurança
- combinados para criar uma solução abrangente de segurança



WAF

Funcionamento

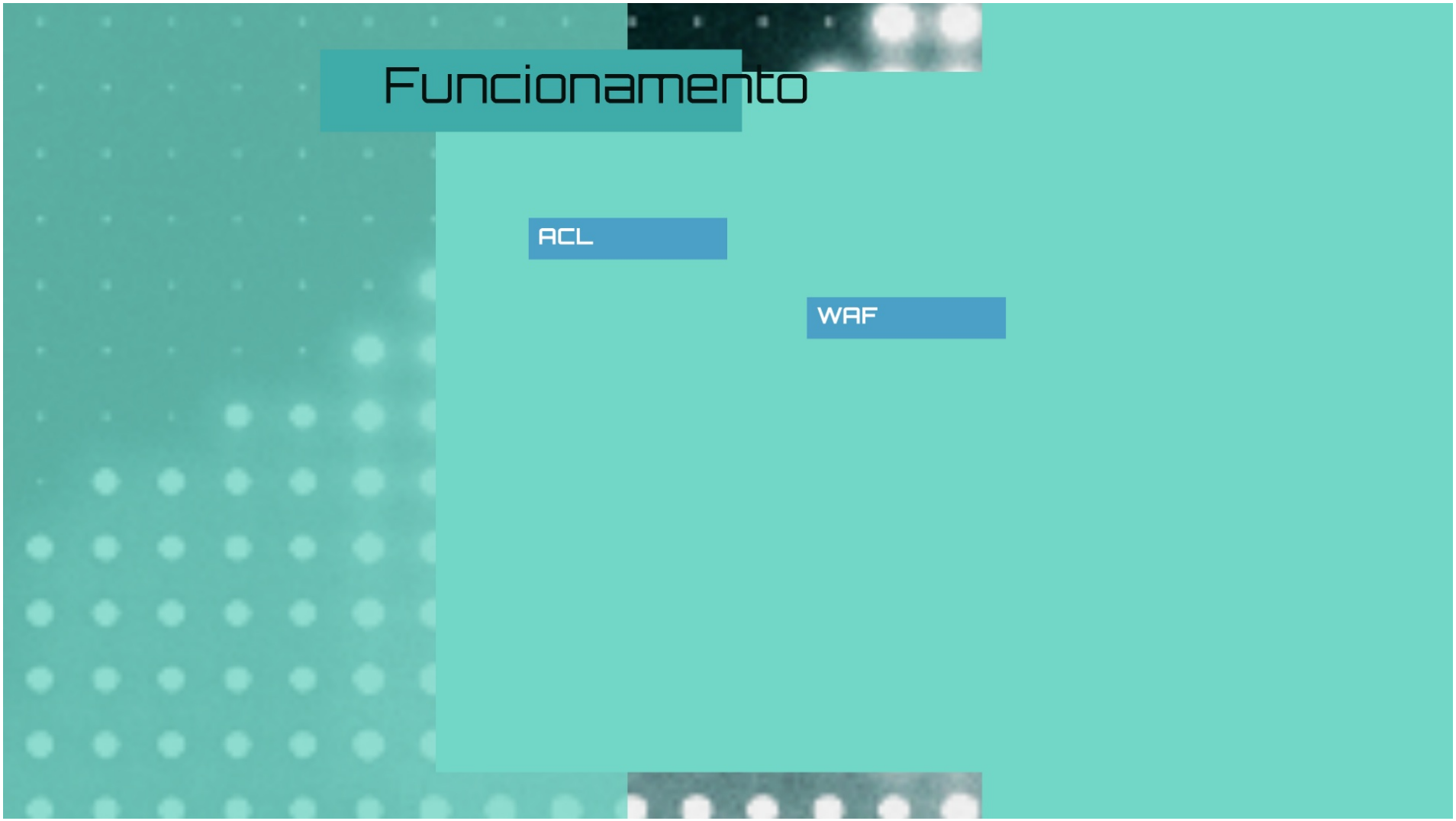
Controle granular sobre a proteção que é adicionada aos seus recursos

Monitorar as solicitações HTTP e HTTPS

- API do Amazon API Gateway
- Amazon CloudFront
- Balanceador de carga de aplicações

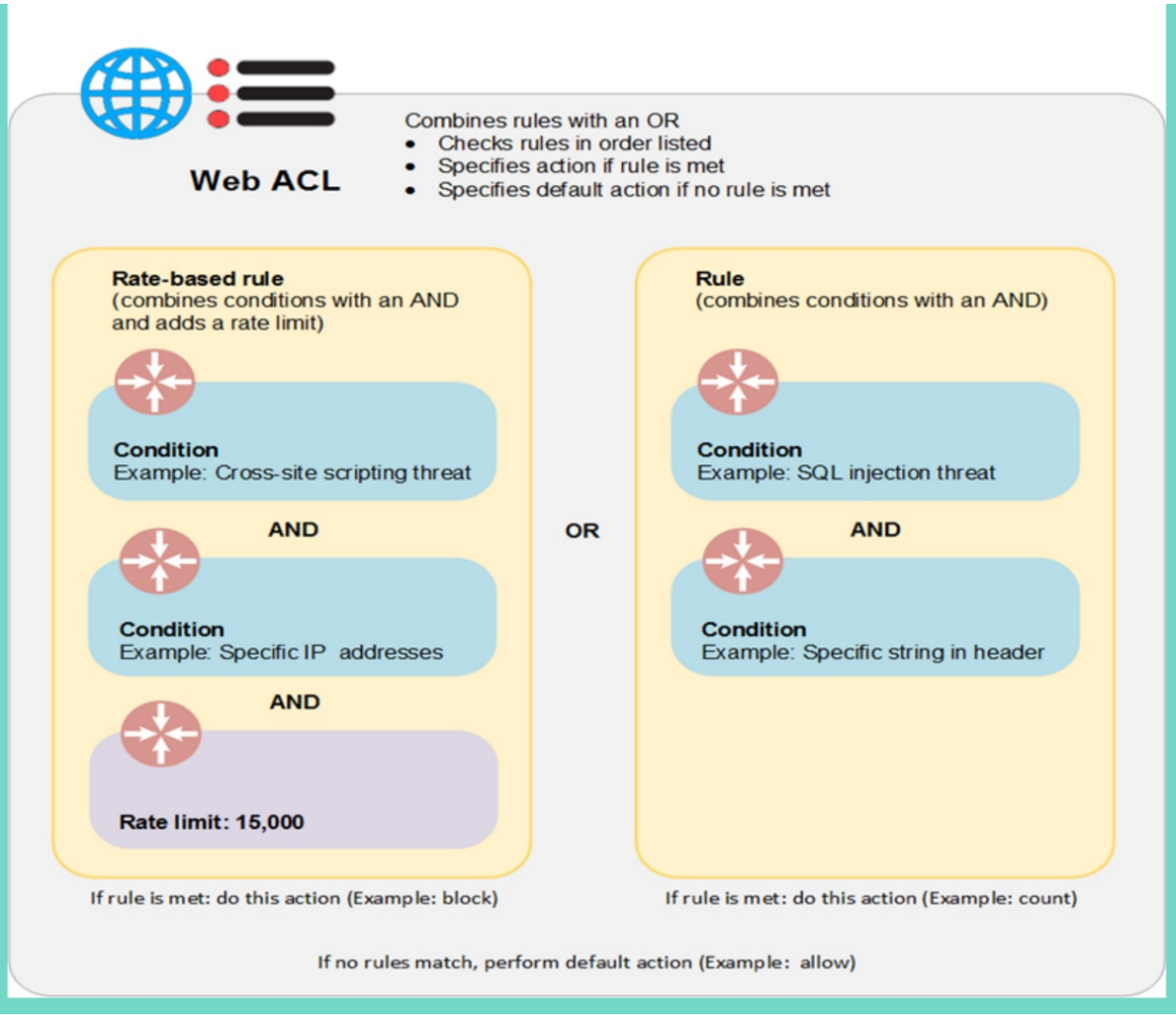
Responde as requisições maliciosas com status 403 (proibido)

Benefícios


Funcionamento
ACL
WAF

ACL - Access Control List

Lista de permissões de acesso a um recurso de um sistemas


Web ACL
Combines rules with an OR
Checks rules in order listed
Specifies action if rule is met
Specifies default action if no rule is met
Rate-based rule
(combines conditions with an AND and adds a rate limit)
Condition
Example: Cross-site scripting threat
AND
Condition
Example: Specific IP addresses
AND
Rate limit: 15,000
If rule is met: do this action (Example: block)
OR
Rule
(combines conditions with an AND)
Condition
Example: SQL injection threat
AND
Condition
Example: Specific string in header
If rule is met: do this action (Example: count)
If no rules match, perform default action (Example: allow)

Benfícios

Proteção adicional contra ataques da web

- Endereços IP origem
- País de origem
- Padrões de expressão regular
- Tamanho das solicitações.
- Presença de código SQL
- Presença de script que provavelmente mal-intencionado

Métricas em tempo real e solicitações

Shield

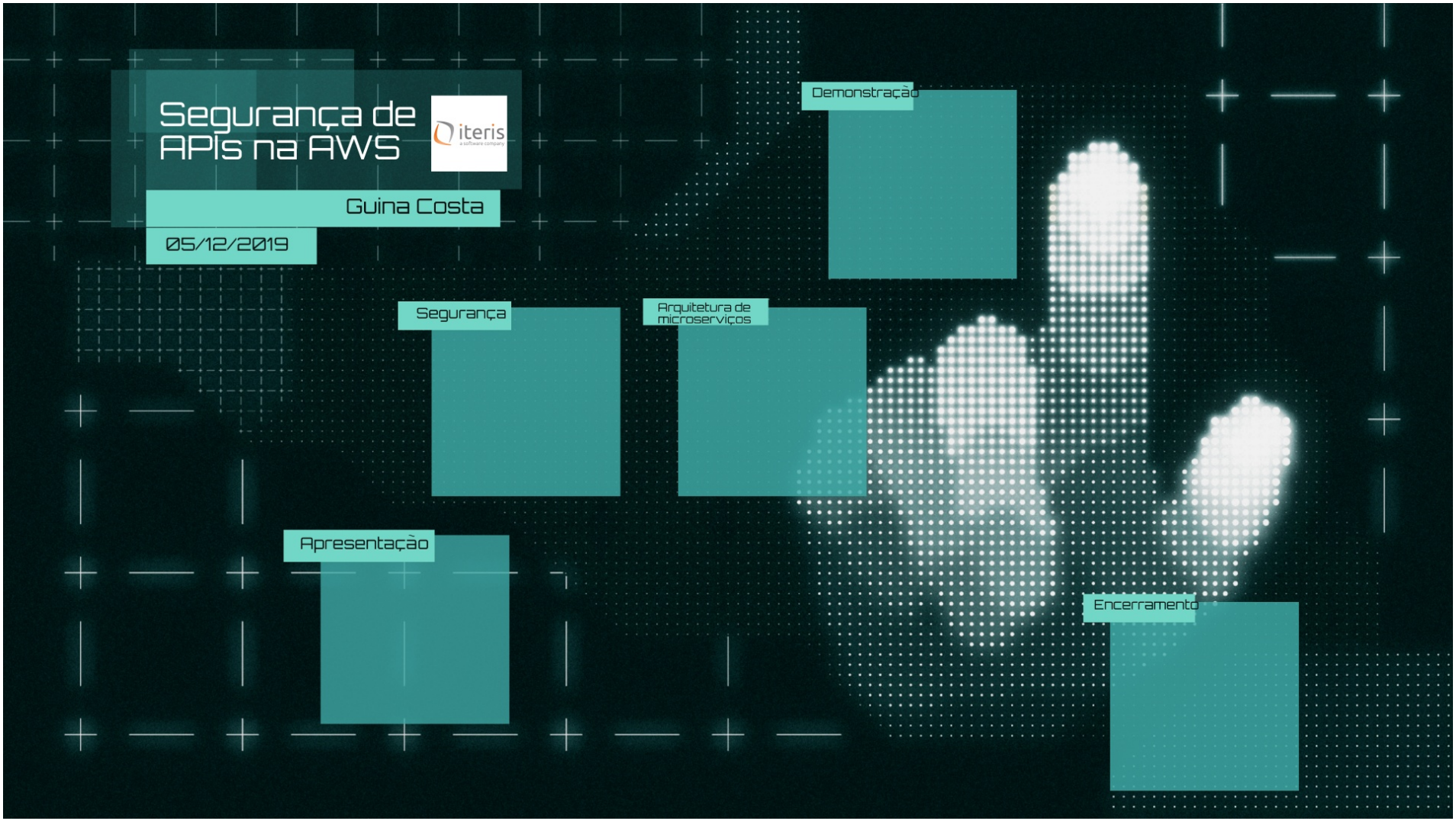
Standard

Advanced

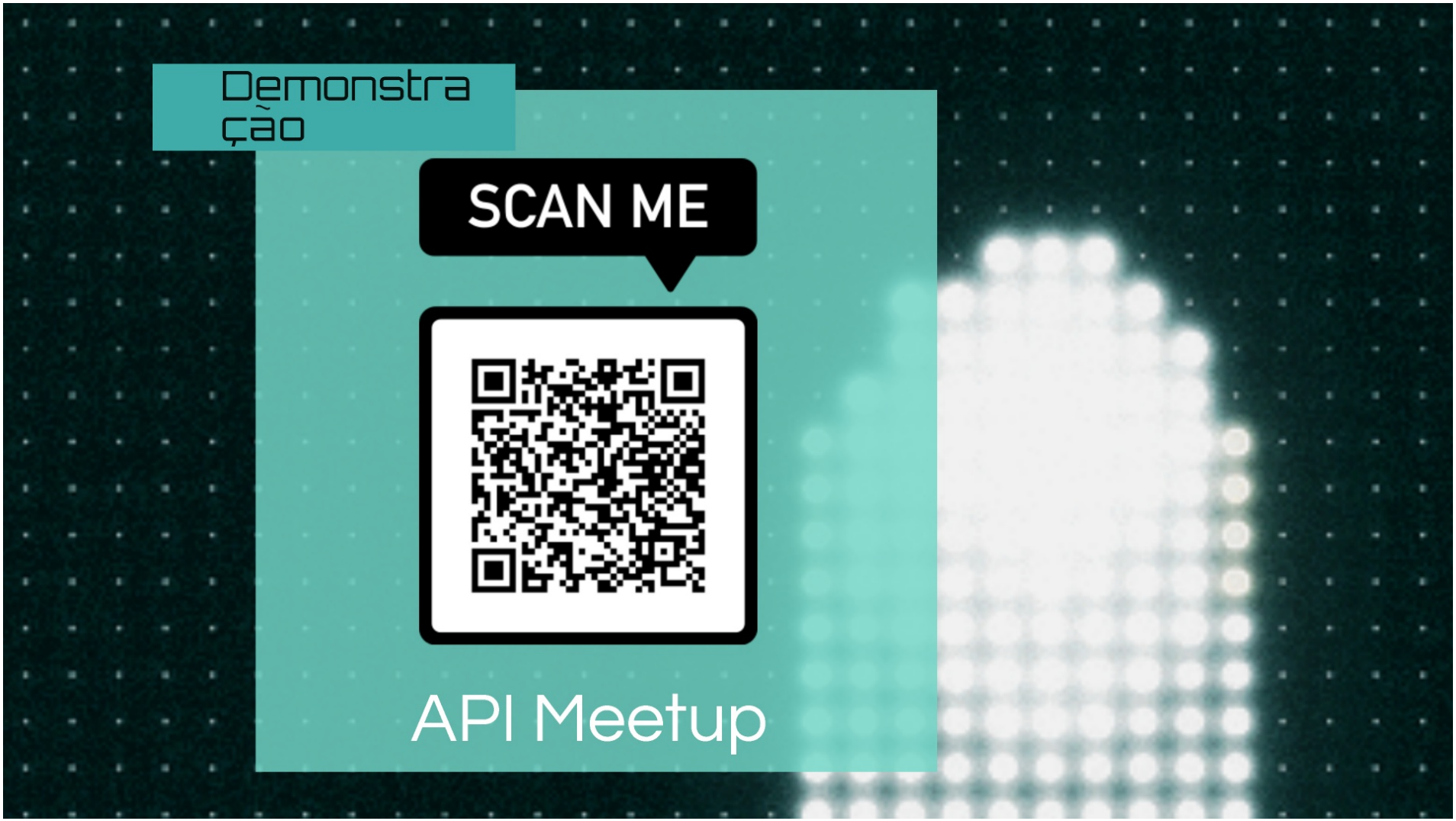
Ataque Distributed Denial of Service (DDoS – ataques distribuídos de negação de serviço)


Standard
Sem custos adicionais para todos os clientes da AWS
Protege contra os ataques DDoS mais comuns e frequentes
Sem visibilidade dos bloqueios realizados por logs


Advanced
Suporte dedicado da DDoS Response Team (DRT)
Níveis mais altos de proteção contra ataques direcionados
Inclui detecção inteligente e atenuação de ataques DDoS
Clientes inscrito no plano Business Support ou Enterprise Support
$$$$$$$
US$3.000/mês


Segurança de APIs na AWS
iteris
Guina Costa
05/12/2019
Demonstração
Segurança
Arquitetura de microserviços
Apresentação
Encerramento


Demonstra
ção
SCAN ME
WhatsMyIP?
Demonstraçao
Links de Apoio

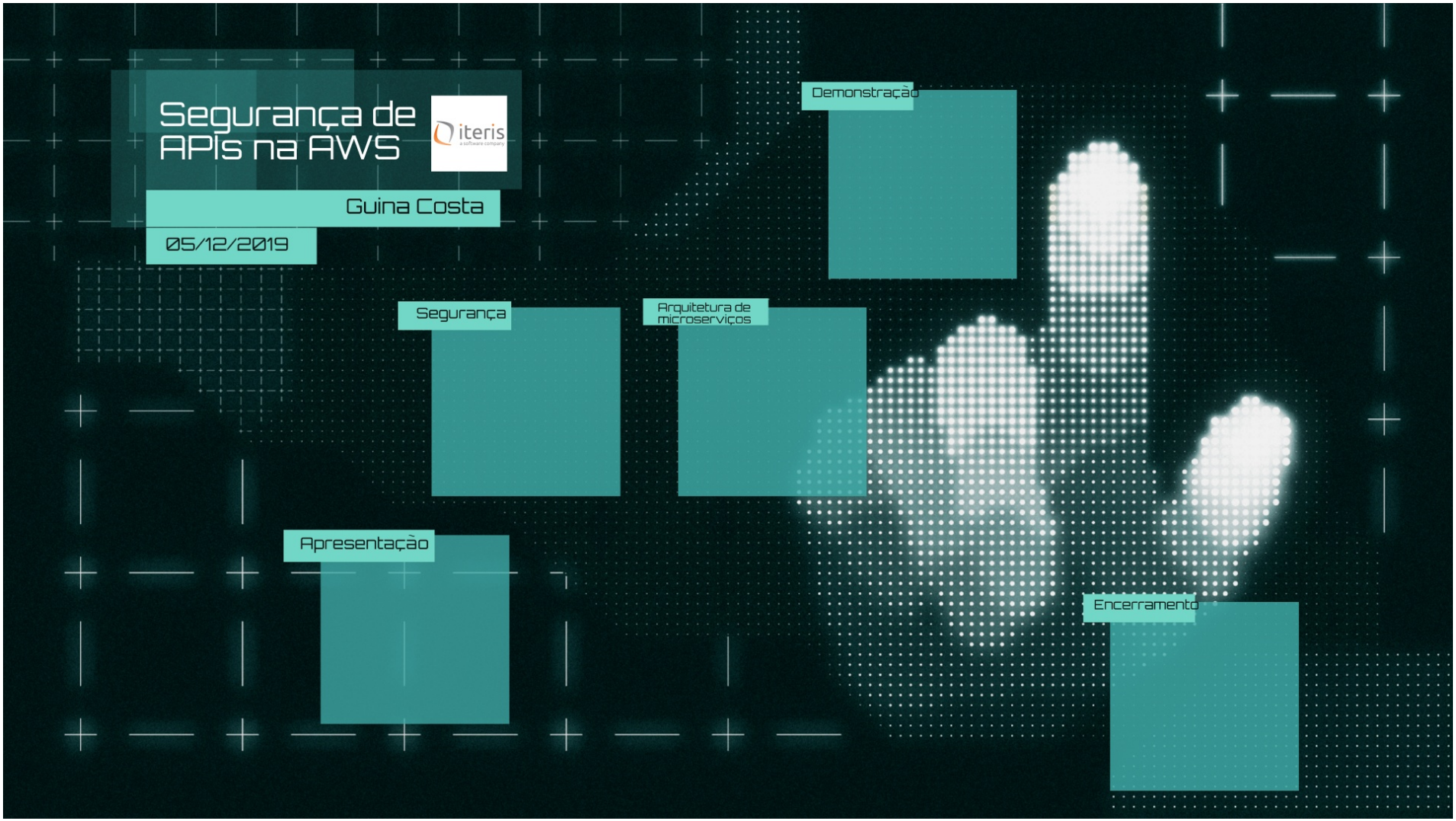

Demonstra
ção
SCAN ME
API Meetup

Links

https://www.whatismyip.com/

https://d3q00fif8i4vmp.cloudfront.net/securitymeetup?TableName=SecurityMeetup

https://console.aws.amazon.com/cloudwatch/home?region=us-east-1#dashboards:name=evil-intention-us-east-1


Segurança de APIs na AWS
iteris
a software company
Guina Costa
05/12/2019
Demonstração
Segurança
Arquitetura de microserviços
Apresentação
Encerramento

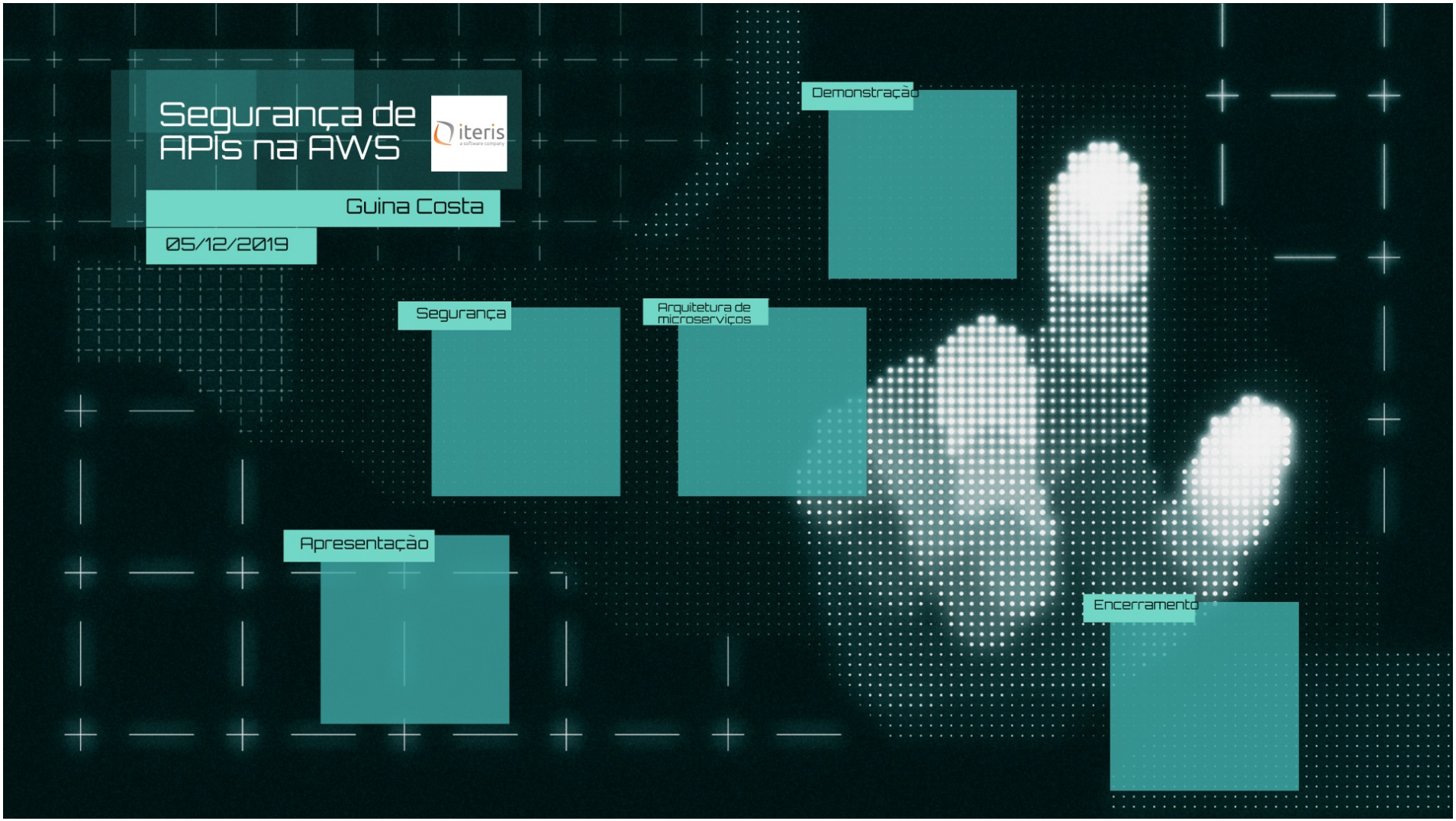
Dúvidas?

Obrigadoo!

Obrigado!

LinkedIn: agnaldocosta

iteris
a software company


Segurança de APIs na AWS
iteris
a software company
Guina Costa
05/12/2019
Demonstração
Segurança
Arquitetura de microserviços
Apresentação
Encerramento