DevOps, Governance & DDOS

A talk about best practices

Rodrigue Vitini
Global Solutions Architect
Amazon Web Services

Part I
Modern DevOps practices

Drop the baggage: DevOps can be simplified to 4 practices

THE 4 A'S OF MODERN DEVOPS

1

Accountability

By bringing development and operations closer together; no “throw it over the wall” silo’ed culture

2

Automation

To speed up delivery and reduce human interaction and errors

3

Awareness

Of the state of your systems at all times

4

Autonomy

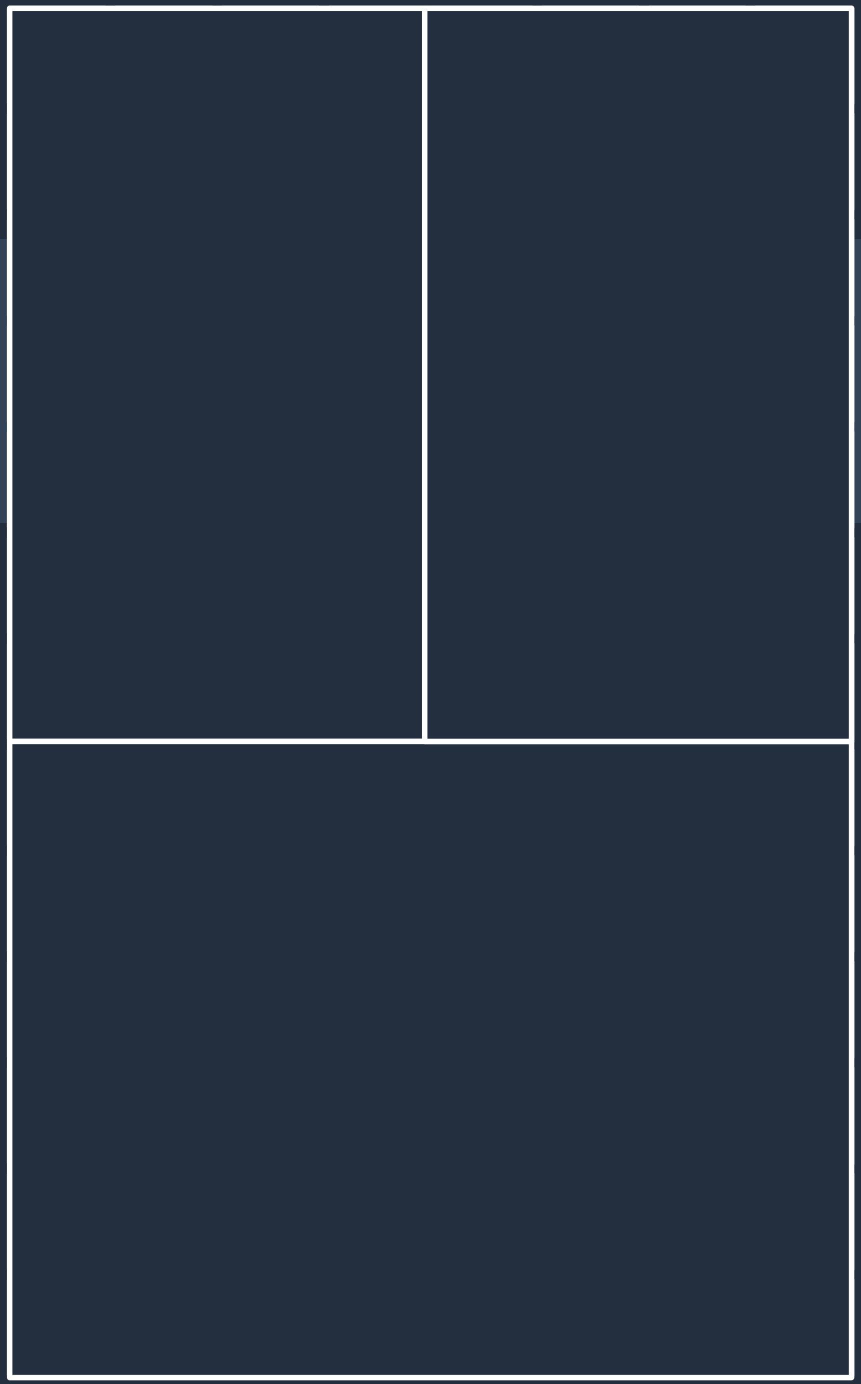
Enabled via centrally enforced standards and governance

Breaking things down

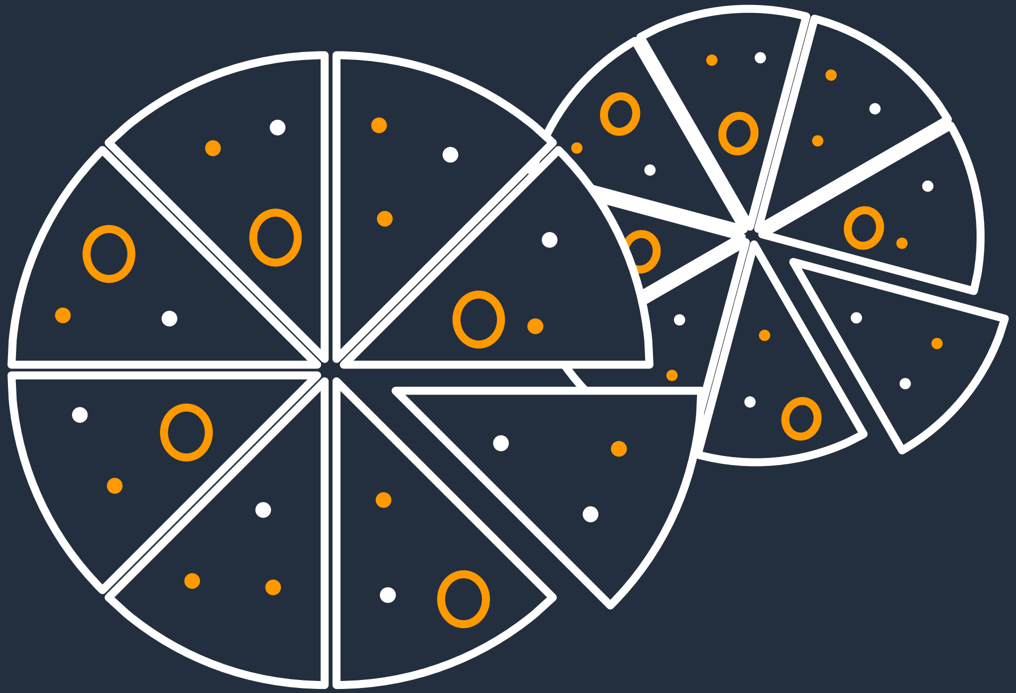
Principles

- Make units a small as possible (Primitives)
- Create data domains
- De-couple based on scaling factors, not functions
- Each service operates independently
  “Communication is terrible!” —Jeff Bezos
- APIs (contracts) between services

✓ **This led to changes in organization**



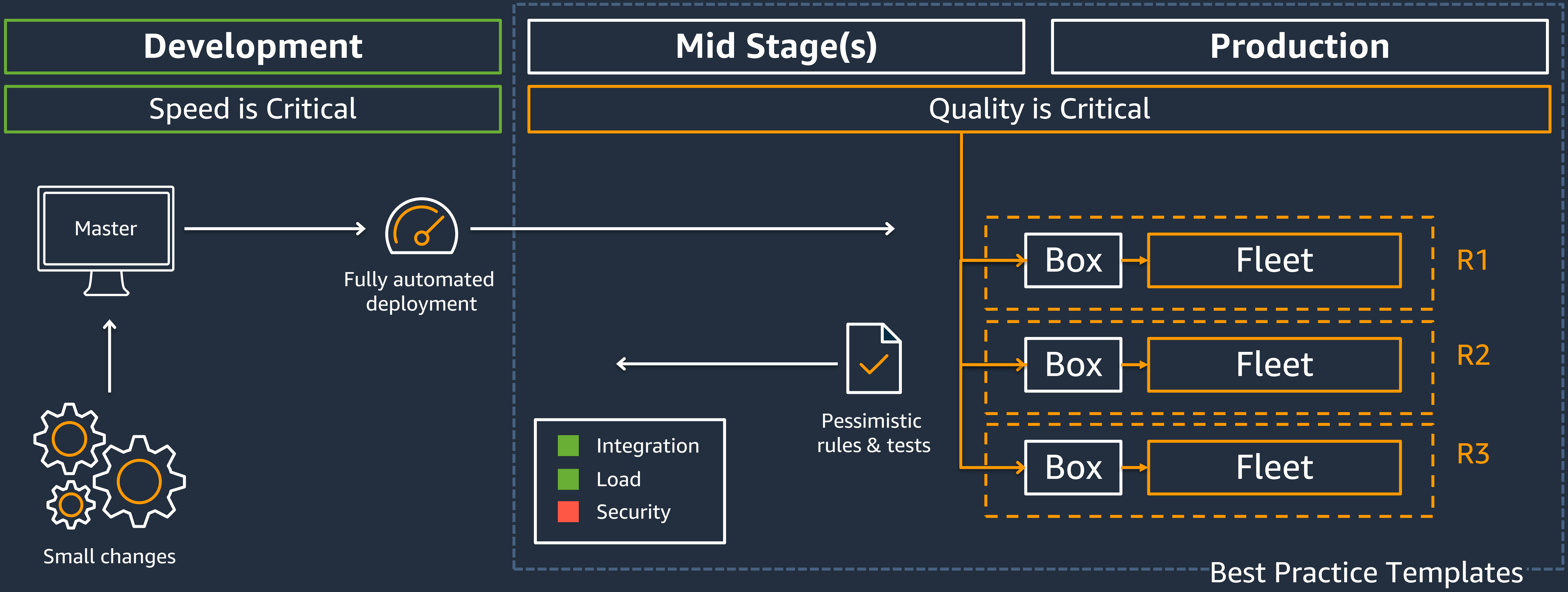
Getting (re)organized



“Two-pizza” teams

- Own a service
- Minimizes social constraints (Conway’s law)
- Autonomy to make decisions

Automate everything



What does Success mean to you?

Business metrics

- Growth
- Usage
- Feedback

Operational metrics

- Errors
- Throttling
- Failed deployments
- Performance

Input goals

- Features
- Use cases
- Performance
- Features

Enablement

- Principal reviews
- Security training
- Ops training
- Measuring Success!

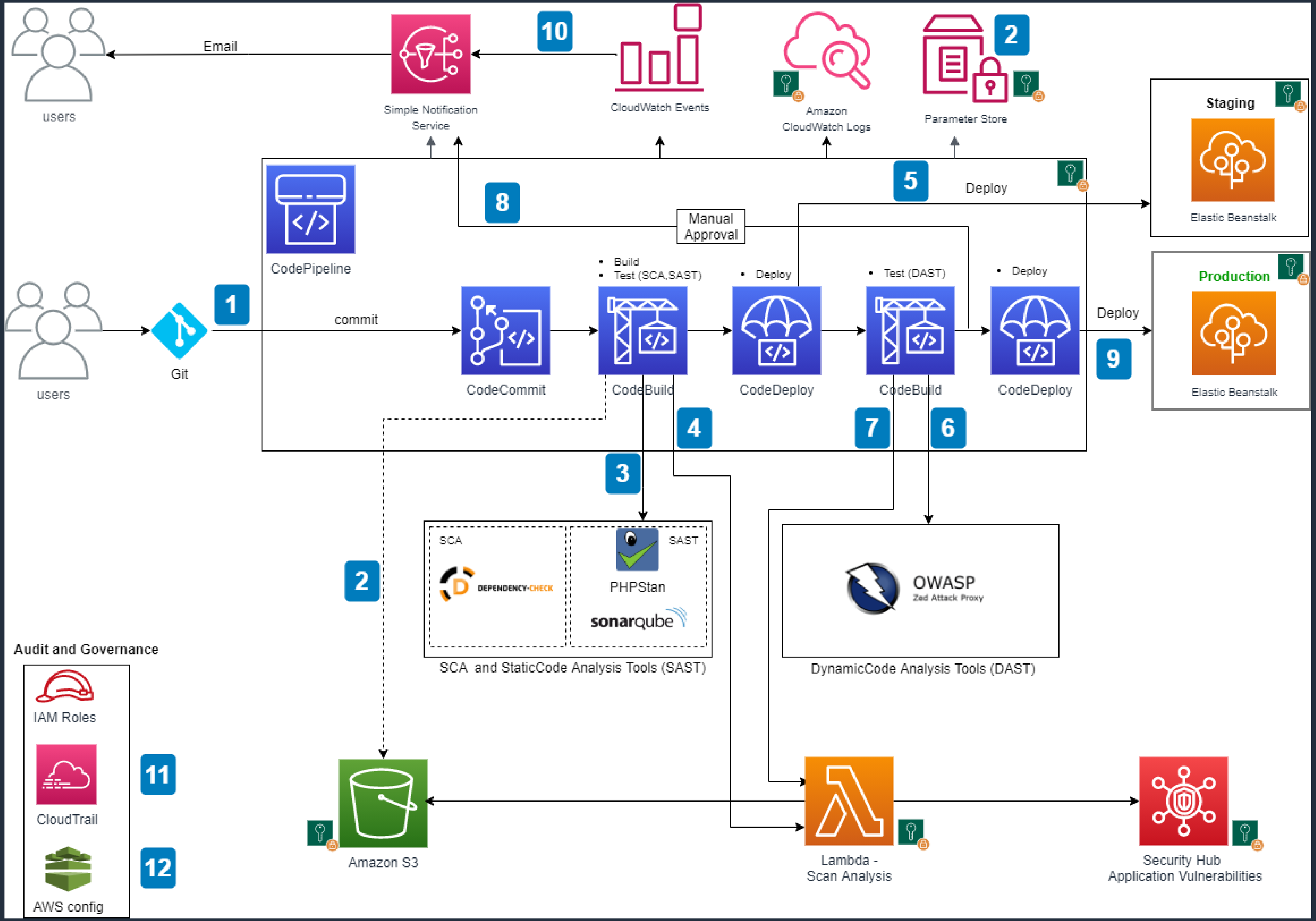
Example of a code pipeline architecture

Continuous testing, logging, monitoring, auditing & governance

Integration with various open-source scanning tools

Aggregation of vulnerability findings

DevSecOps pipeline available as a code



aws

Before…

Move fast **OR** Stay secure

Now…

Move fast AND Stay secure

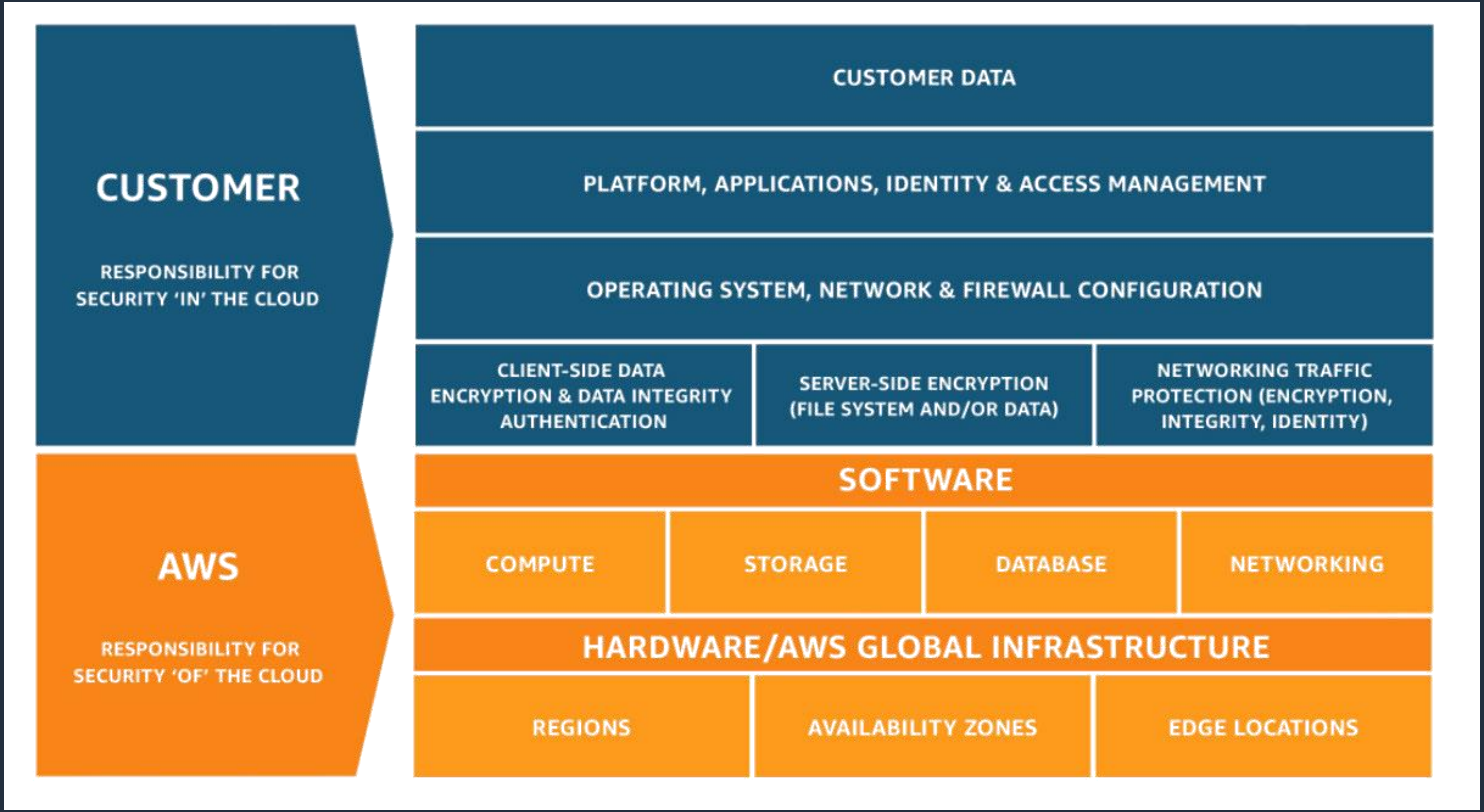
Part II
Governance and DDoS Mitigation

Why is on-premises security traditionally challenging?

Lack of visibility

Low degree of automation

AWS shared responsibility model



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

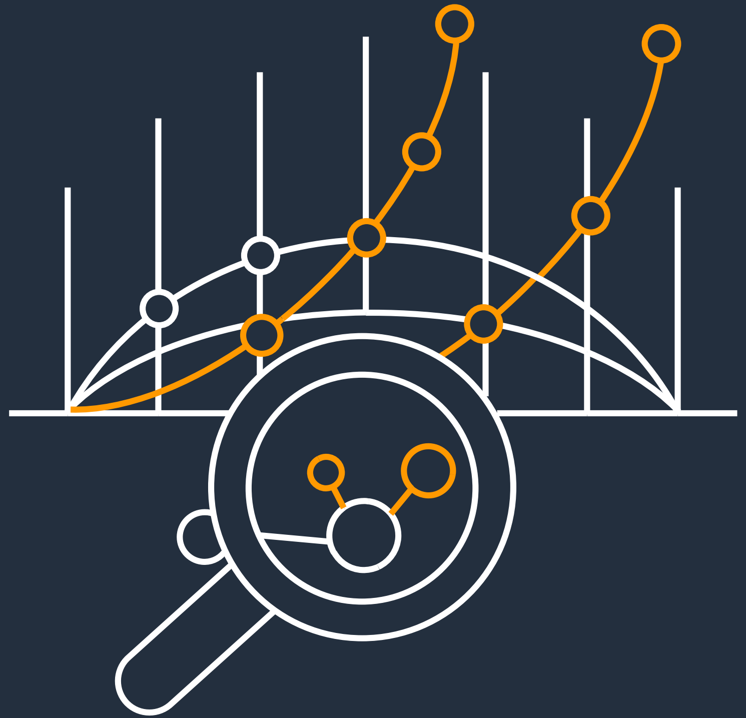
SOFTWARE

COMPUTE	STORAGE	DATABASE	NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS

Scale with superior visibility and control



Control where your data is stored and who can access it

Fine-grain identity and access controls so users and groups have the right access to resources

Reduce risk via security automation and continuous monitoring

Integrate AWS services with your solutions to support existing workflows, streamline ops, and simplify compliance reporting

DDoS Mitigation in the Cloud

Challenges of scale

Many possible points of ingress for Internet traffic

Monitoring on a very large network

Destination endpoint capacity varies (a lot)

Distinguishing legitimate traffic from the malicious

Picking the best mitigation strategy

Some data points

~1 million DDoS attacks per year

Exabytes of data analyzed every minute

1,000s of DDoS attacks mitigated every day

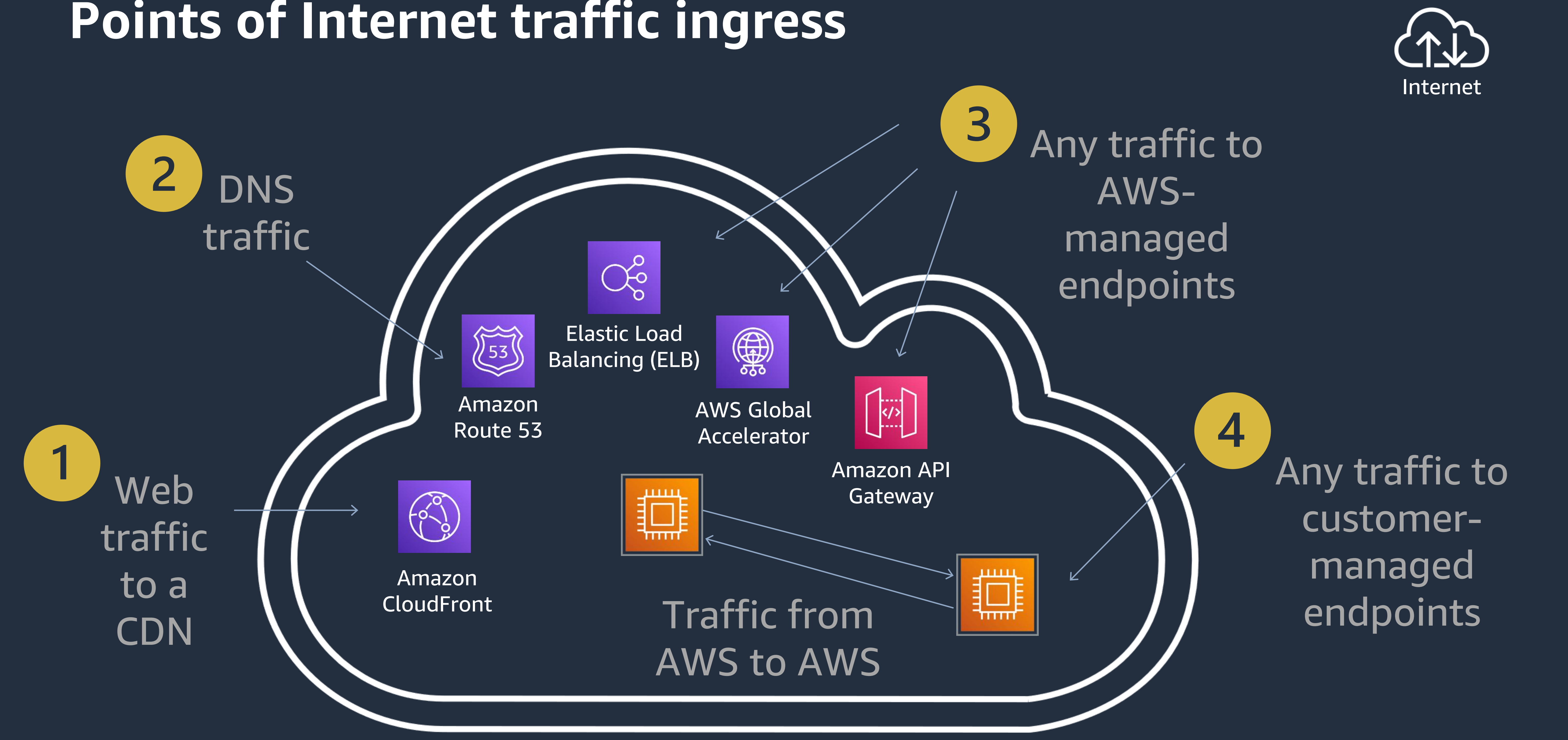
100+ billion AWS Managed Rules requests processed per day

300 GB of flow logs ingested every second

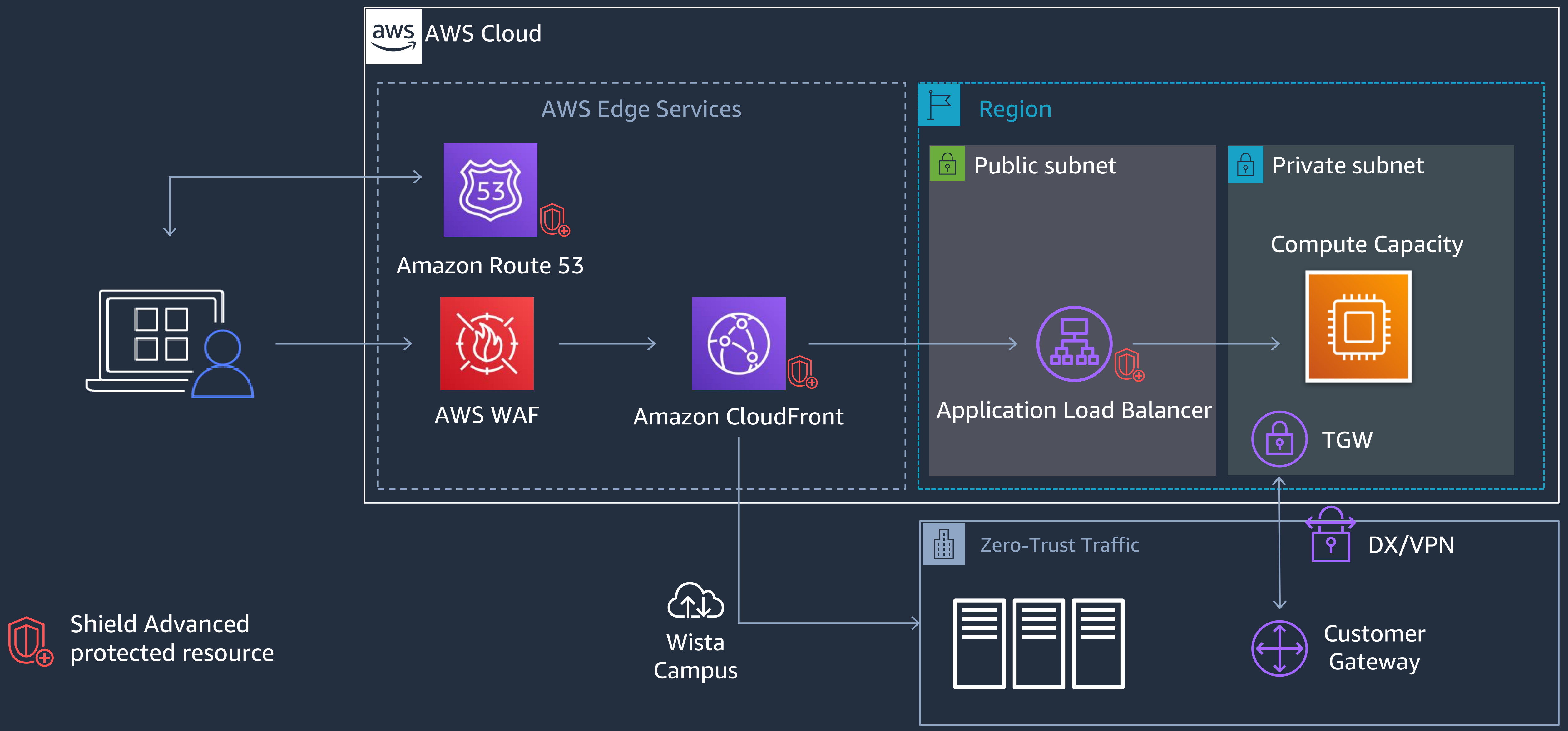
Network and Application layers

<table>
<tr><th>OSI model</th><th>TCP/IP model</th><th colspan="6">IP protocol stack</th></tr>
<tr><td>Application layer</td><td rowspan="3">Application layer</td><td rowspan="3">HTTP
TCP/80</td><td rowspan="3">HTTPS
TCP/443</td><td rowspan="3">DNS
TCP/53 or UDP/53</td><td rowspan="3">QUIC
UDP/443</td><td rowspan="3">SIP, SMPP, RTP, RSVP, etc.</td><td rowspan="3">SMTP, TELNET, FTP, RIP, etc.</td></tr>
<tr><td>Presentation layer</td></tr>
<tr><td>Session layer</td></tr>
<tr><td>Transport layer</td><td>Transport layer</td><td colspan="3">TCP</td><td colspan="3">UDP</td></tr>
<tr><td>Network layer</td><td>Internet layer</td><td colspan="6">IP</td></tr>
<tr><td>Data link layer</td><td rowspan="2">Network access layer</td><td colspan="6" rowspan="2">Ethernet, ATM, frame relay, etc.</td></tr>
<tr><td>Physical layer</td></tr>
</table>

Points of Internet traffic ingress



Protecting on-premise applications



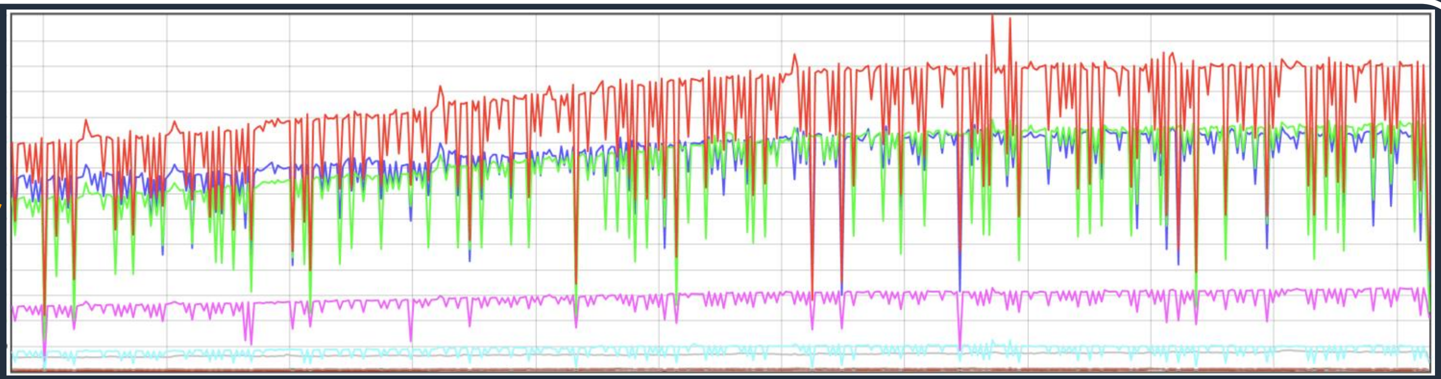
L7 auto mitigation with AWS Shield Advanced

Internet traffic

AWS WAF

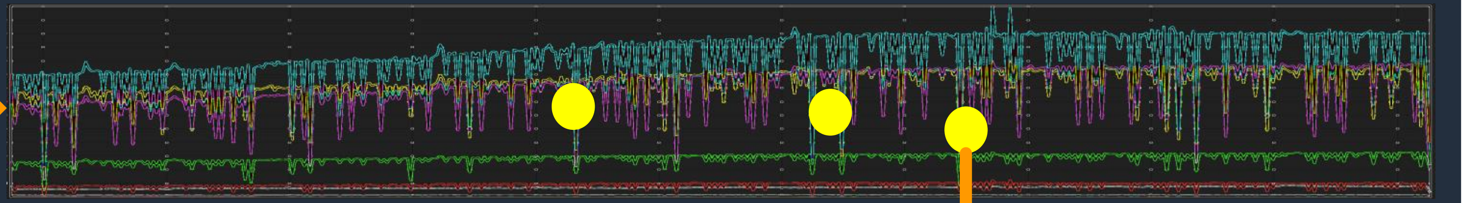
Automatic application-layer DDoS mitigation

Request logs

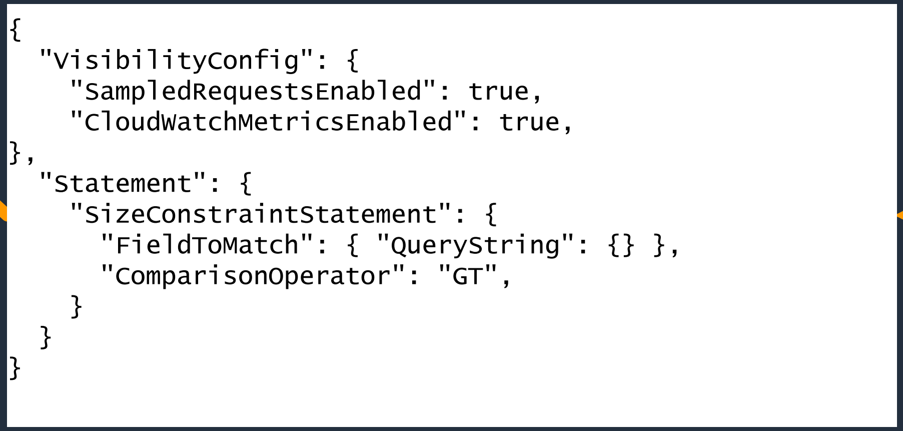


Per-resource baseline

Request logs

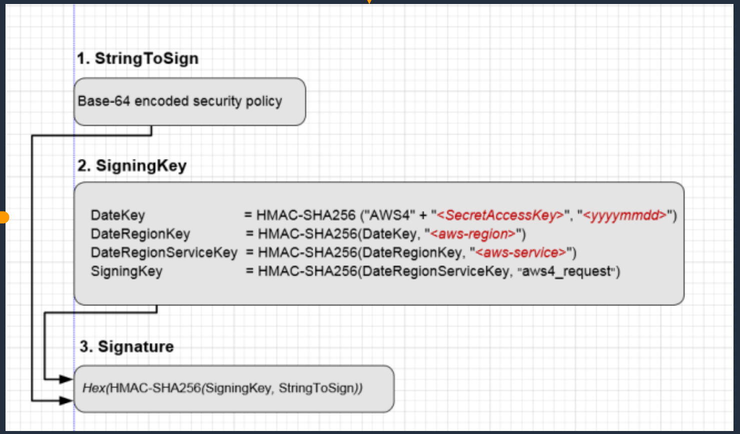


Continuous anomaly detection



```
{
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
},
  "Statement": {
    "SizeConstraintStatement": {
      "FieldToMatch": { "QueryString": {} },
      "ComparisonOperator": "GT",
    }
  }
}
```

Builds AWS WAF rules

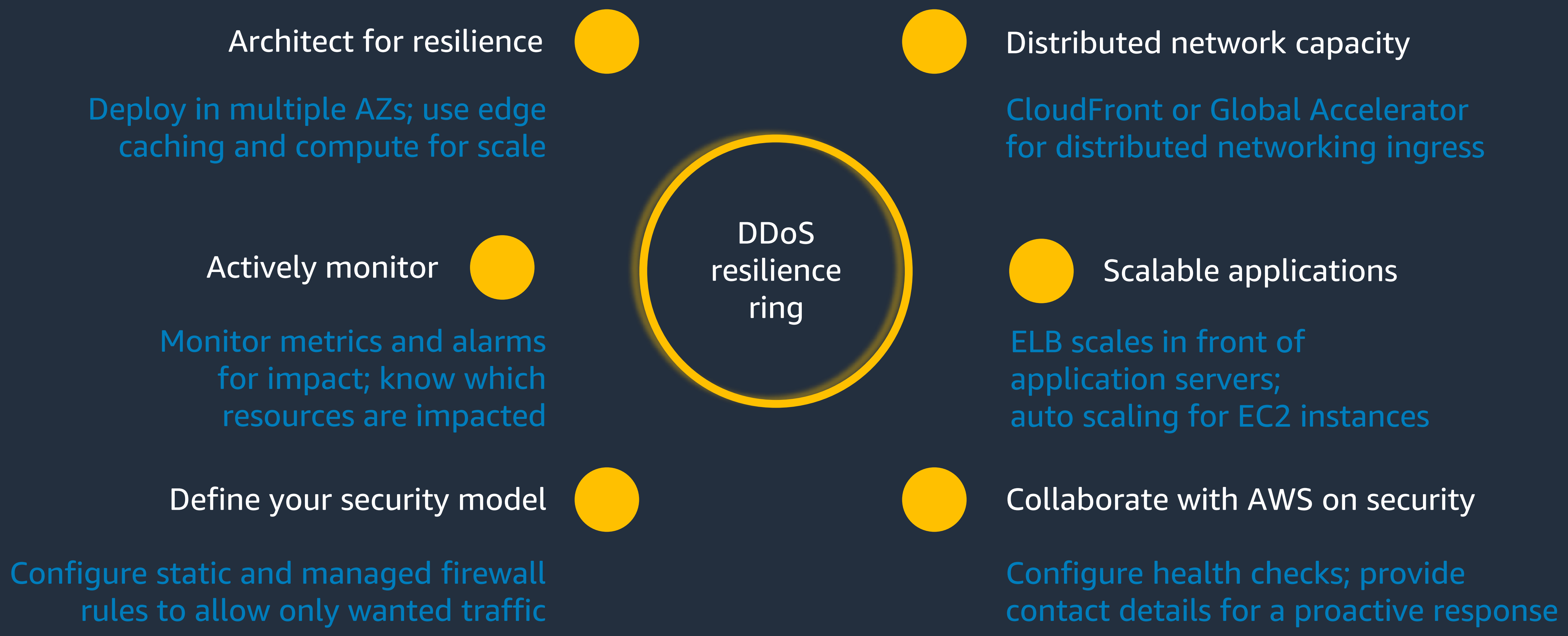

1. StringToSign
Base-64 encoded security policy
2. SigningKey
DateKey = HMAC-SHA256 ("AWS4" + "<SecretAccessKey>", "<yyyymmdd>")
DateRegionKey = HMAC-SHA256(DateKey, "<aws-region>")
DateRegionServiceKey = HMAC-SHA256(DateRegionKey, "<aws-service>")
SigningKey = HMAC-SHA256(DateRegionServiceKey, "aws4_request")
3. Signature
Hex(HMAC-SHA256(SigningKey, StringToSign))

Attack signatures

Auto-placed

AWS WAF rules can be applied in count mode to verify effectiveness or block mode to protect legitimate traffic

Framework for DDoS resilience best practices



DDoS resilience ring

Architect for resilience

Deploy in multiple AZs; use edge caching and compute for scale

Actively monitor

Monitor metrics and alarms for impact; know which resources are impacted

Define your security model

Configure static and managed firewall rules to allow only wanted traffic

Distributed network capacity

CloudFront or Global Accelerator for distributed networking ingress

Scalable applications

ELB scales in front of application servers;
auto scaling for EC2 instances

Collaborate with AWS on security

Configure health checks; provide contact details for a proactive response

AWS Shield Response Team has a time machine

Some resources to follow-up

https://aws.amazon.com/blogs/devops/

https://catalog.workshops.aws/sec4devs/en-US

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html?secd_intro1

https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/

https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

https://www.youtube.com/watch?v=5cfVebJ8wTo&pp=ygURcmVpbnZlbnQgZGRvcyBhd3M%3D

https://aws.amazon.com/blogs/networking-and-content-delivery/how-to-enhance-cloudfront-origin-security-of-on-premise-web-servers-using-third-party-firewalls/ .

https://aws.amazon.com/blogs/devops/building-end-to-end-aws-devsecops-ci-cd-pipeline-with-open-source-sca-sast-and-dast-tools/

Thank you!

Rodrigue Vitini

vitini@amazon.com

https://www.linkedin.com/in/rodriguevitini/