2017 中国互联网安全大会
China Internet Security Conference

云上的安全自动化

杨 历

AWS China
合作伙伴解决方案架构师

目录

AWS云安全理念与技术合规

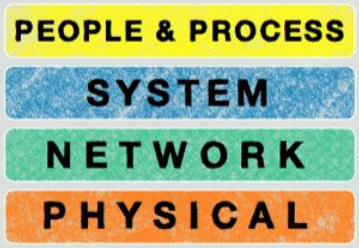
为什么需要安全自动化

如何实现安全自动化

示例

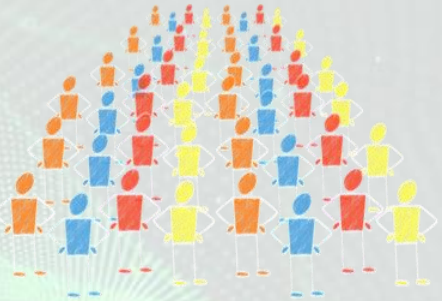
AWS云安全理念与技术合规

安全是第“零”项工作：Security is Job Zero



成熟的安全模型

被众多客户专家
验证和增强



所有客户受益

物理安全

网络安全

平台安全

人和过程

安全与合规是一种责任共担

客户

客户数据、内容

平台、应用、认证和授权管理，访问控制

操作系统，网络，防火墙配置

客户端数据加密 | 服务器端数据加密 | 网络流量保护

AWS 基础服务

计算 | 存储 | 数据库 | 网络

AWS 全球基础架构

可用区

区域

边缘节点

- ✓ AWS 最佳实践
- ✓ 业界标准
- ✓ AWS标准化架构
- ✓ 内部规章
- ✓ 服务文档
- ✓ AWS 工作手册
- ✓ AWS 技术资源

AWS众多技术确保云安全

网络

VPC

防火墙

加密

密码管理服务

Cloud HSM

加密

认证

IAM

SAML 联合

联合目录

合规

服务目录

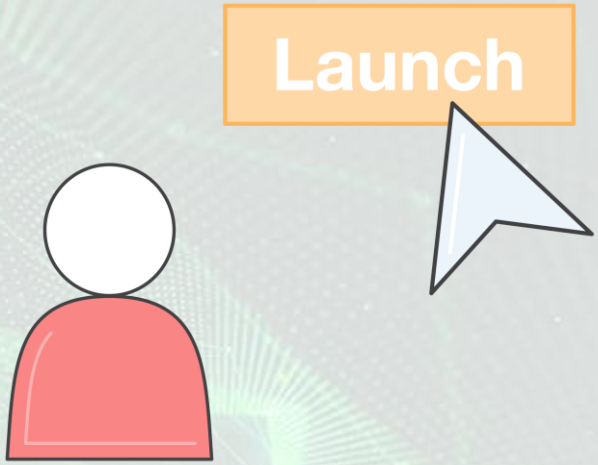
Cloud Trail

Config

为什么需要安全自动化

为什么需要自动化？

- 减少人为错误的风险

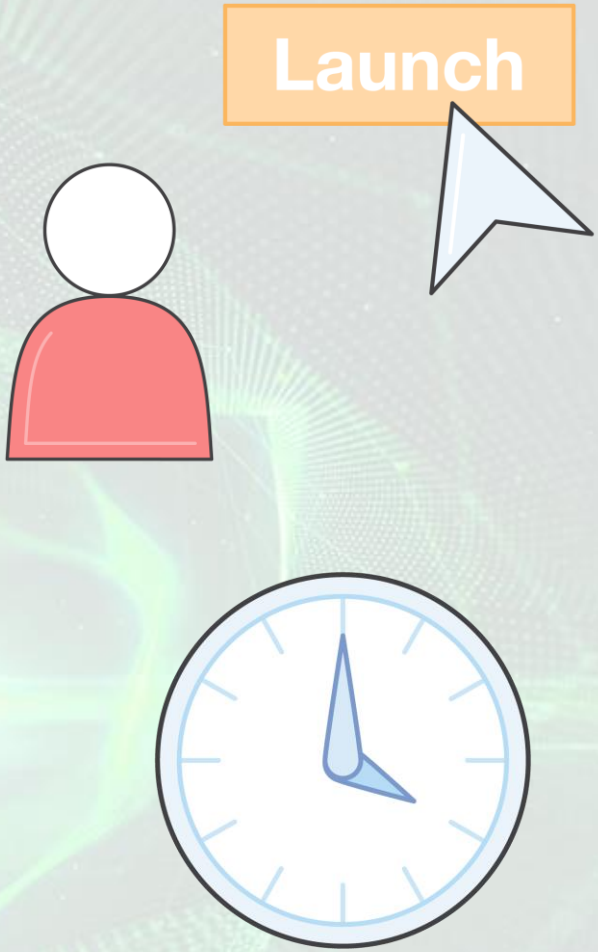


为什么需要自动化？

- 减少人为错误的风险
  - 自动化更有效

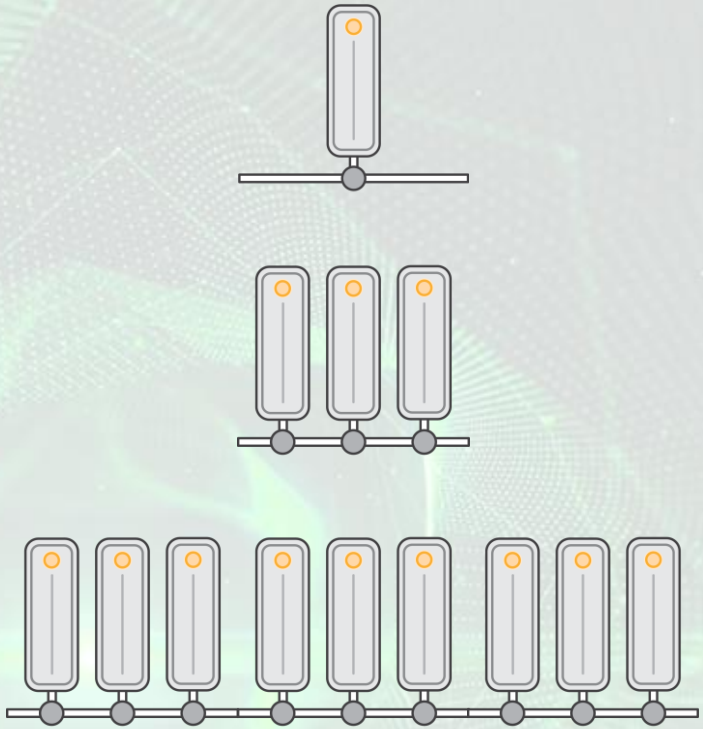
为什么需要自动化？

- 减少人为错误的风险
  - 自动化更有效
  - 自动化更可靠



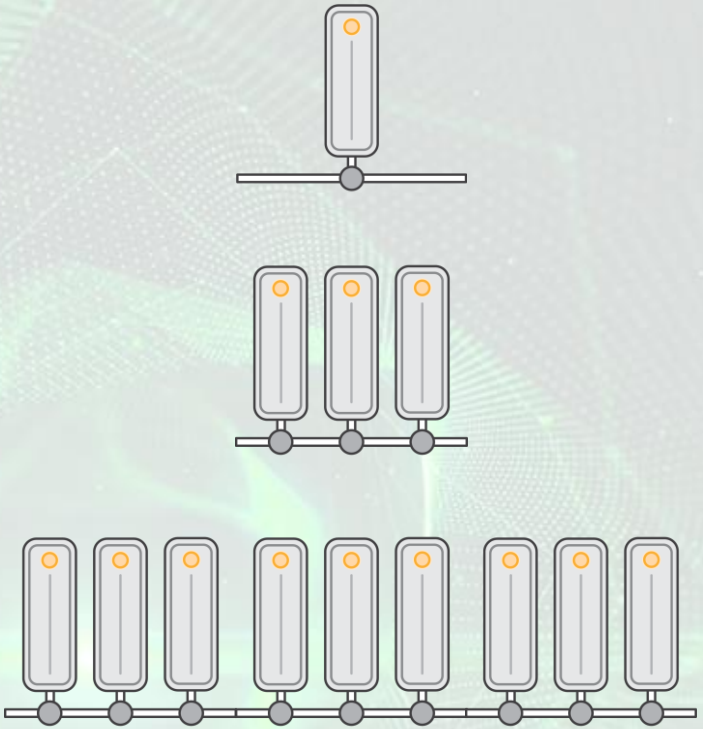
为什么需要自动化？

- 减少人为错误的风险
  - 自动化更有效
  - 自动化更可靠
  - 自动化更可扩展



为什么需要自动化？

- 减少人为错误的风险
  - 自动化更有效
  - 自动化更可靠
  - 自动化更可扩展
- 无需担心，依然需要人



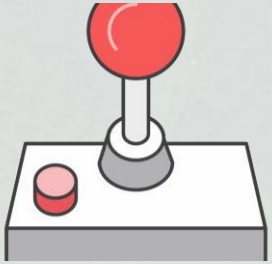
ISC 2017 中国互联网安全大会

360互联网安全中心

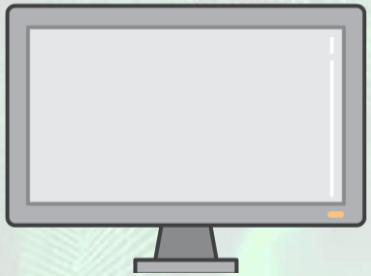
如何实现安全自动化

三个阶段

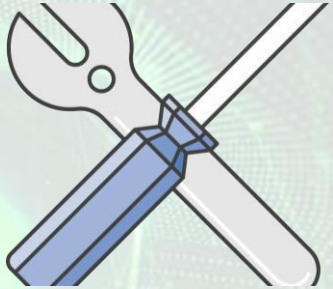
控制



监控



修复



阶段1 – 控制

- 防止可能带来问题的操作
  - AWS CloudFormation
  - Service Catalog
  - AWS IAM 策略
  - 禁止root密码
  - 检查GitHub是否泄漏访问密码

阶段2 – 监控

- 获取并监测所有元数据
  - AWS CloudTrail
  - AWS Config
  - Amazon CloudWatch Logs
  - VPC Flow Logs

阶段3 – 修复

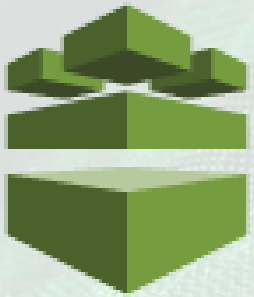
- 修复方式
  - 定位问题
  - 间接方式： tickets 或者 离线改正
  - 直接方式： 采取修正行动

自动化！

AWS帮助自动修复的服务

AWS Lambda

验证确定用户、组、角色、规则、行为是否合规。



AWS Config Rules

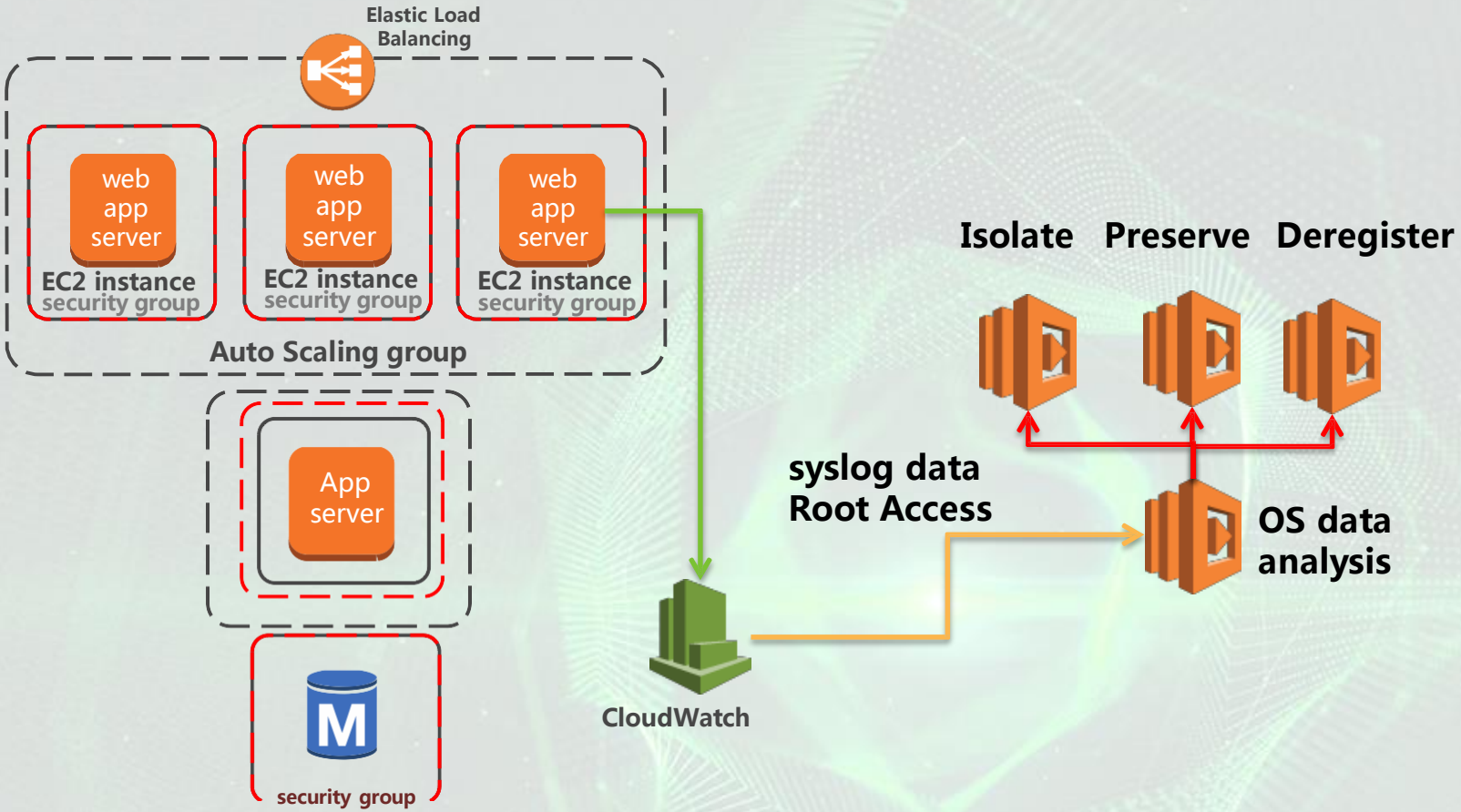
利用规则来验证、记录配置变更

Amazon SNS

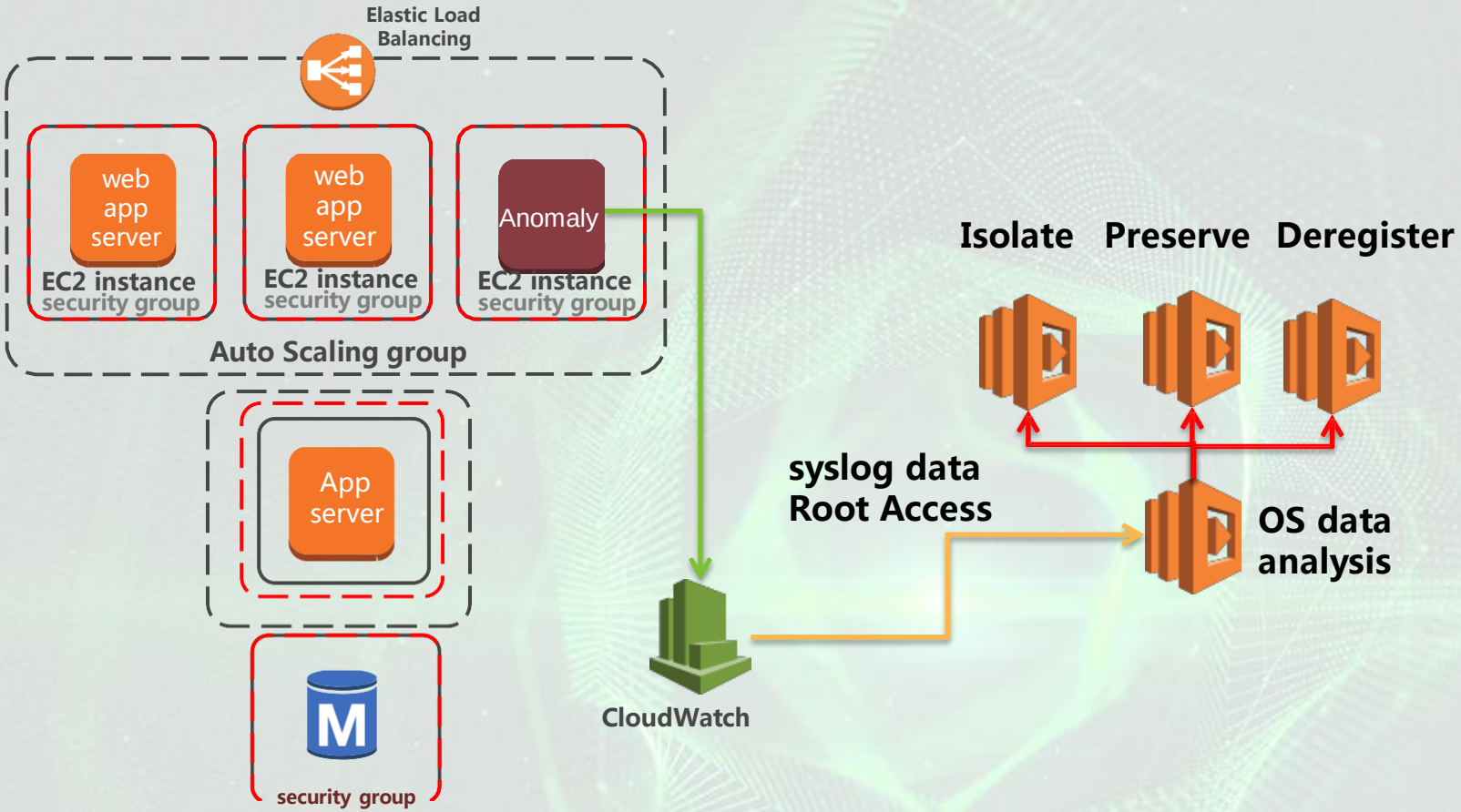
发现问题时通知

示例

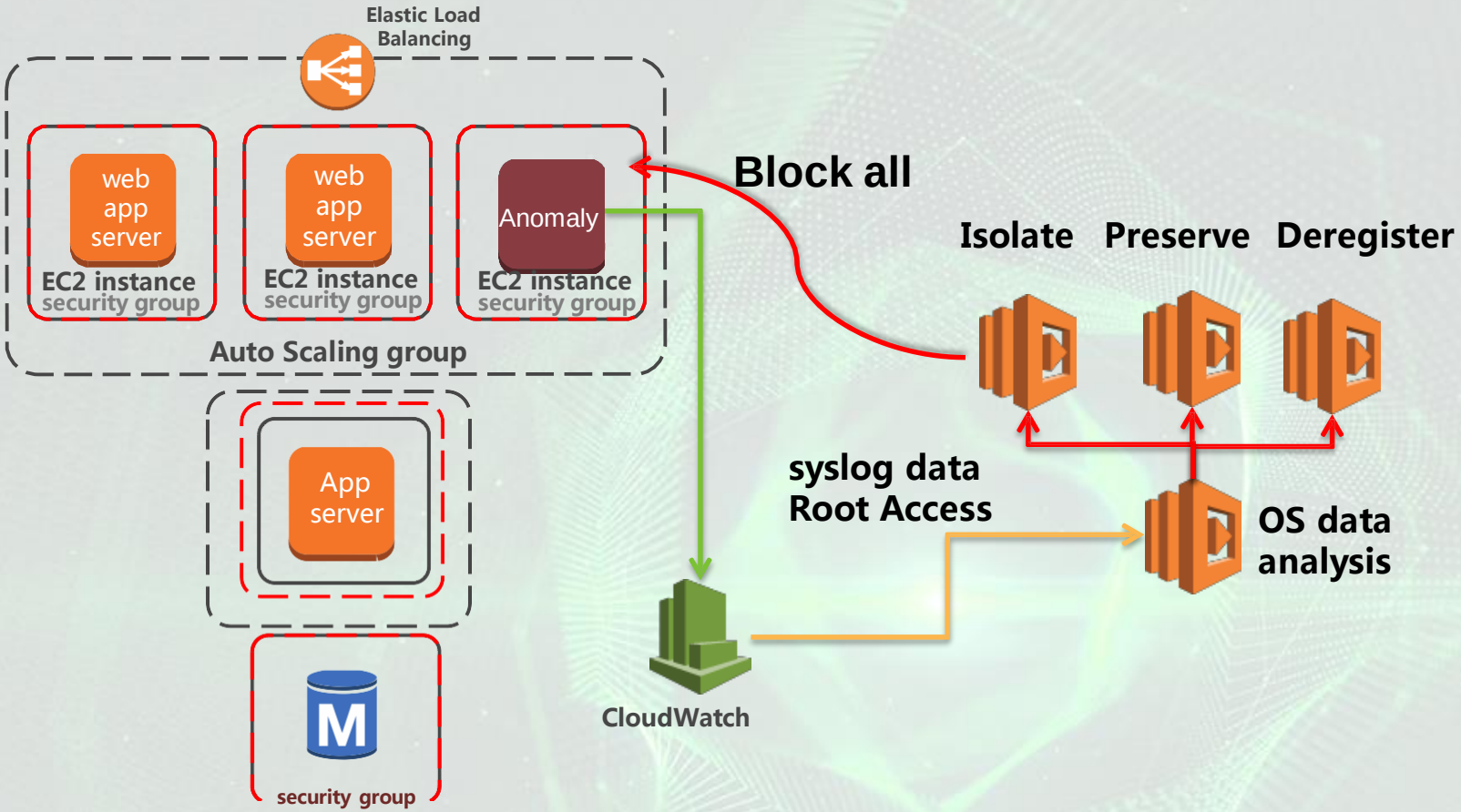
示例


Elastic Load Balancing
web app server
EC2 instance security group
web app server
EC2 instance security group
web app server
EC2 instance security group
Auto Scaling group
App server
security group
CloudWatch
Isolate
Preserve
Deregister
syslog data
Root Access
OS data analysis

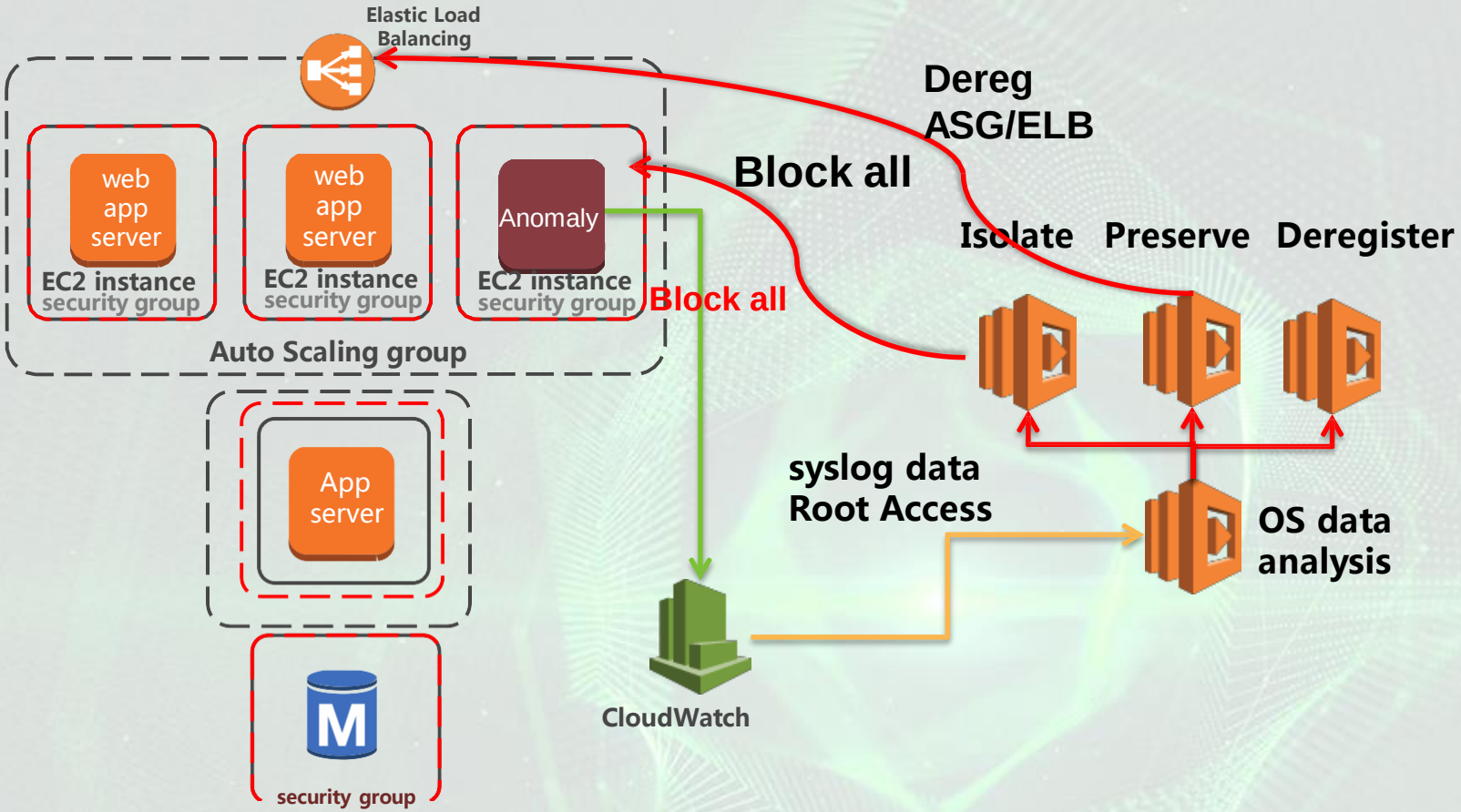
示例 – Cont 1


Elastic Load Balancing
web app server
EC2 instance security group
web app server
EC2 instance security group
Anomaly
EC2 instance security group
Auto Scaling group
App server
security group
CloudWatch
Isolate
Preserve
Deregister
syslog data
Root Access
OS data analysis

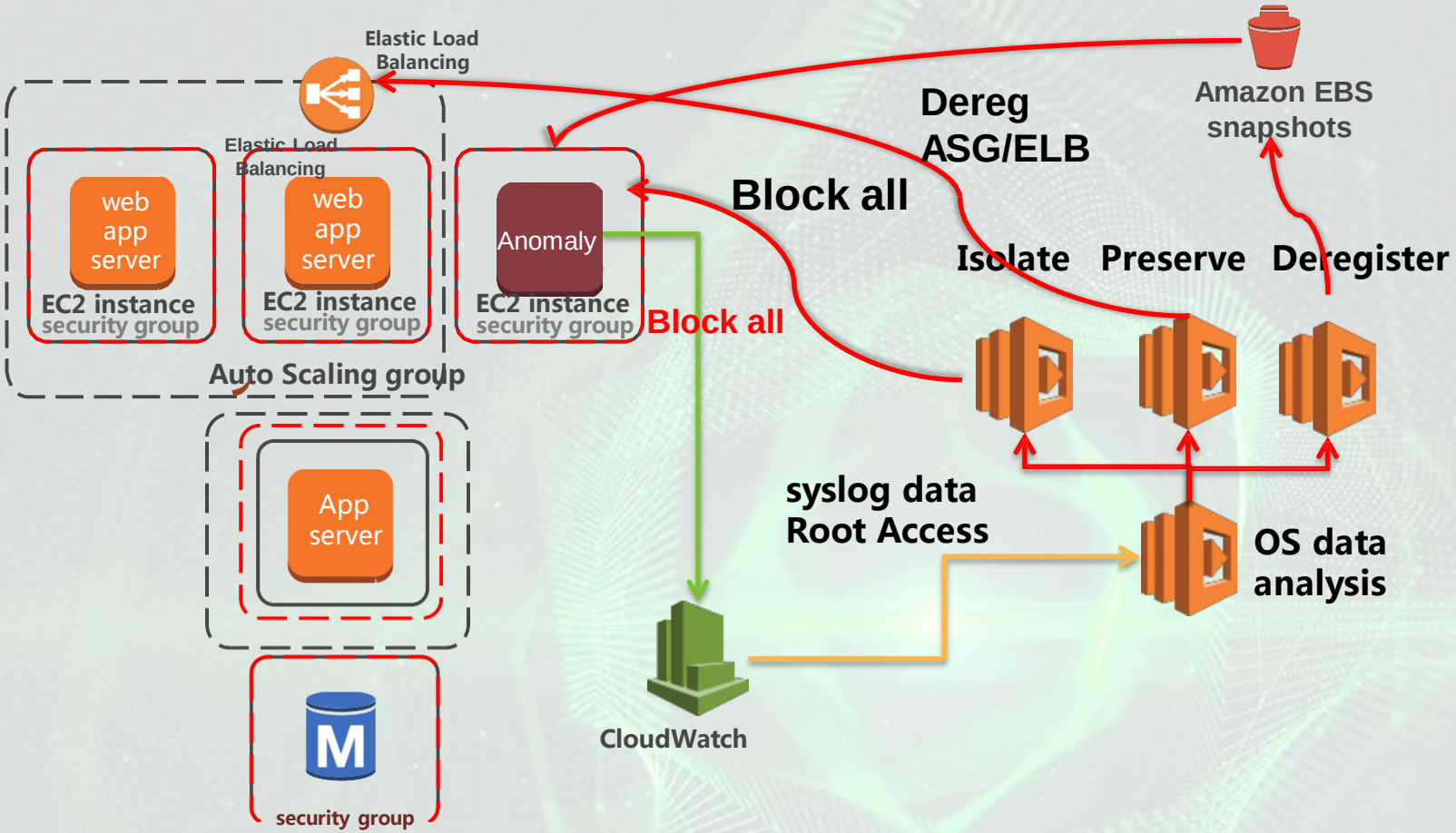
示例 – Cont 2


Elastic Load Balancing
web app server
EC2 instance security group
web app server
EC2 instance security group
Anomaly
EC2 instance security group
Auto Scaling group
App server
M
security group
Block all
Isolate
Preserve
Deregister
syslog data
Root Access
OS data analysis
CloudWatch

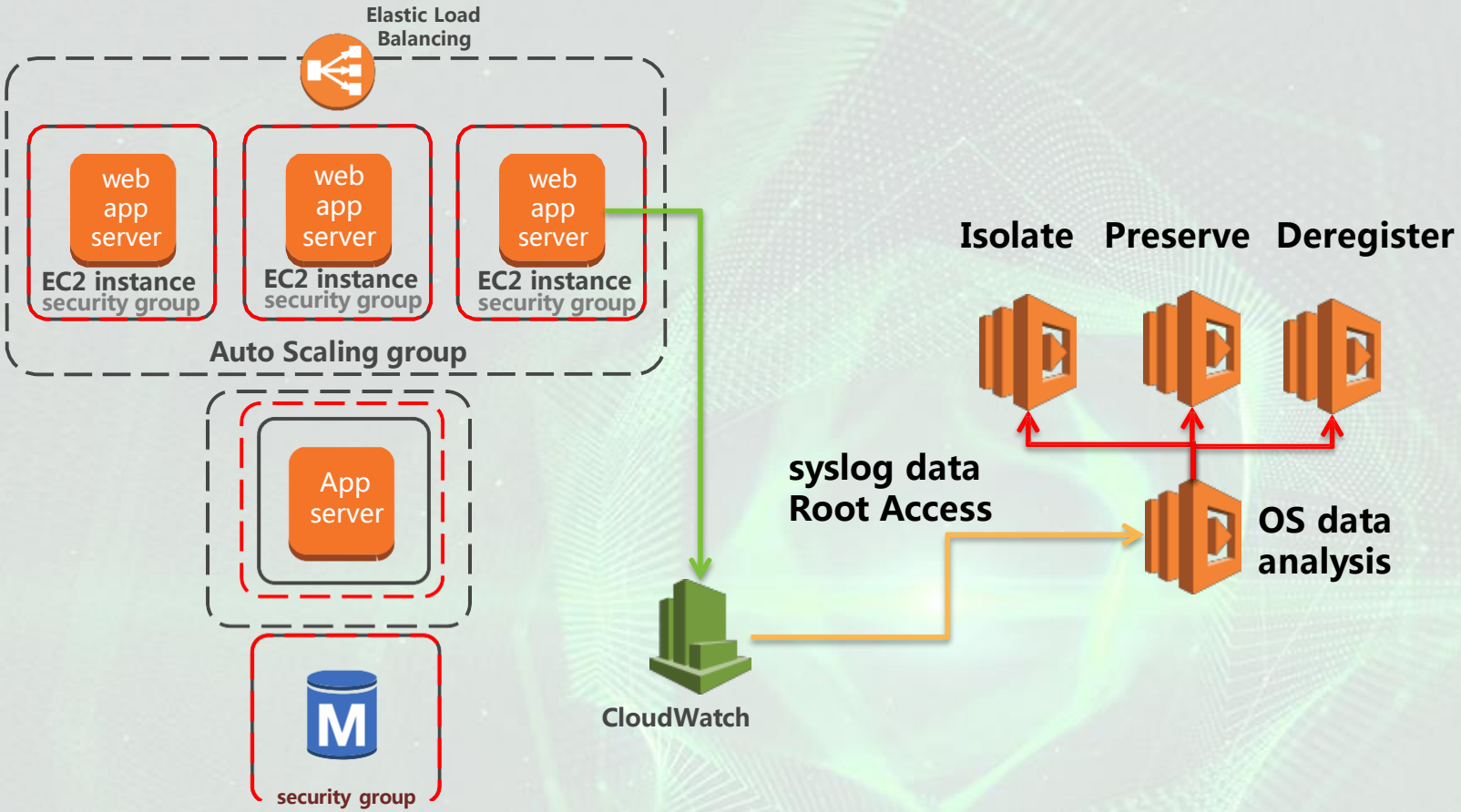
示例 – Cont 3


Elastic Load Balancing
web app server
EC2 instance security group
web app server
EC2 instance security group
Anomaly
EC2 instance security group
Auto Scaling group
App server
security group
Dereg ASG/ELB
Block all
Isolate
Preserve
Deregister
Block all
syslog data
Root Access
OS data analysis
CloudWatch

示例 – Cont 4


Elastic Load Balancing
Elastic Load Balancing
web app server
EC2 instance security group
web app server
EC2 instance security group
Anomaly
EC2 instance security group
Auto Scaling group
App server
security group
Block all
Dereg ASG/ELB
Block all
Amazon EBS snapshots
Isolate
Preserve
Deregister
syslog data
Root Access
OS data analysis
CloudWatch

示例 – Cont 5


Elastic Load Balancing
web app server
EC2 instance security group
web app server
EC2 instance security group
web app server
EC2 instance security group
Auto Scaling group
App server
security group
CloudWatch
Isolate
Preserve
Deregister
syslog data
Root Access
OS data analysis

众多AWS合作伙伴助力实现云安全

splunk>

ALERT LOGIC®
Security. Compliance. Cloud.

Flux7

VERIS GROUP

evident.io

ALLGRESS

CloudCheckr

TREND MICRO™

Symantec.

谢　谢


ISC
2017
5th
2017 中国互联网安全大会
China Internet Security Conference
万物皆变 人是安全的尺度
Of All Things Human Is The Measure