TEK5530 - Measurable Security for the Internet of Things

L15-16 – Cloud security and IoT

György Kálmán,
DNB/UiO ITS
gyorgy.kalman@its.uio.no

Josef Noll
UiO ITS
josef.noll@its.uio.no

http://cwi.unik.no/wiki/TEK5530, #IoTSec, #IoTSecNO

TEK5530: Lecture plan

- 17.01 L1: Introduction
- 24.01
  - L2: Internet of Things
- 31.01
  - L3: Security of IoT + Paper list
- 07.02
  - L4: Smart Grid, Automatic Meter Readings
  - L5: Service implications on functional requirements
- 14.02
  - L6: Technology mapping
  - L9: Top 20 critical security controls
- 21.02 --- Winter holiday
  - «homework» see recording of
  L7: Practical implementation of ontologies
- 28.02
  - L8: Paper analysis with 25 min presentation
  - L10: Intrusion detection
- 07.03
  - L13: Communication and security in current industrial automation
  - L14: Cloud basics and cloud architecture
- 14.03
  - L11: Multi-Metrics Method for measurable Security
  - L12: Multi-Metrics Weighting of an AMR sub-system
- 21.03
  - L15: AWS Cloud security, Cloud monitoring, automation and incident response
  - L16: AWS IoT
- 28.03
  - L17: Wrap-up of the course ,
  Selected recent topics from IoT security
- 04.04 ---- No lecture, prepare for exam, consultation possibility
- 11.04 ---- group work presentation?
- 18.04 ---- Easter holiday, no lecture
- 25.04 ---- Exam

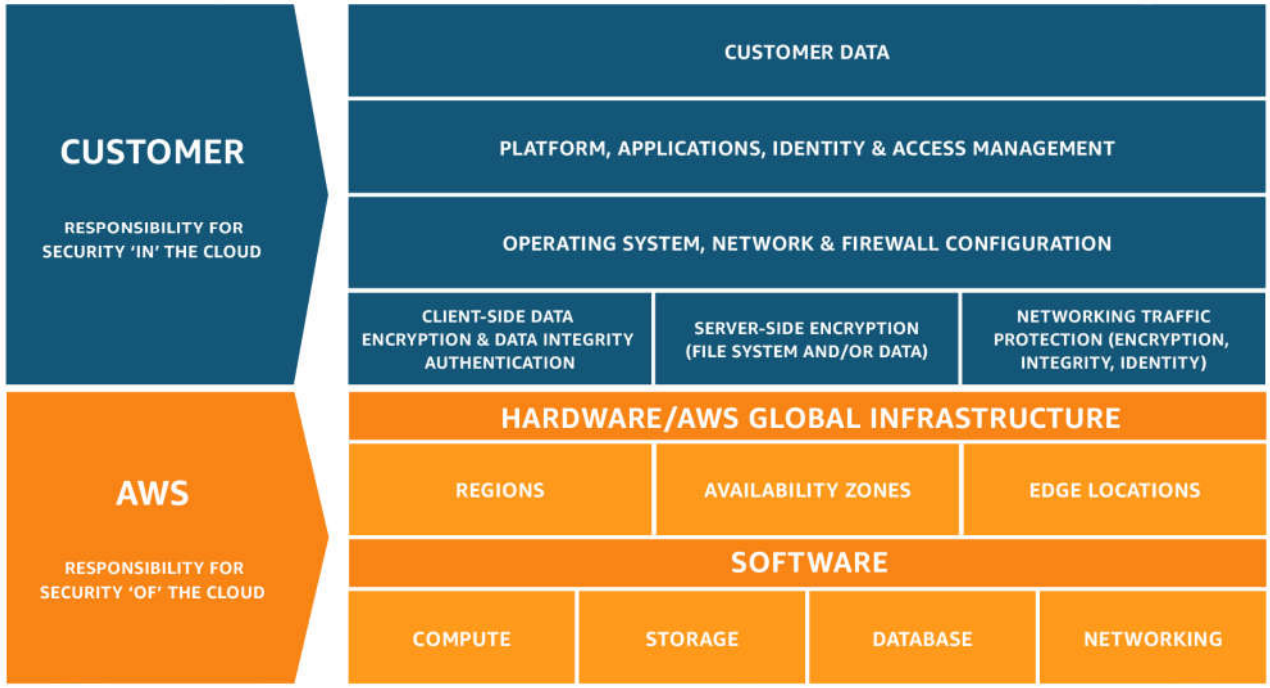
Cloud security, IoT and service examples

- Short recap on Cloud computing
- Cloud security
  - Implications of the shared responsibility model
  - Security infrastructure
  - Logging
  - Penetration testing
  - Managing your cloud

- IoT in cloud
  - AWS Greengrass

AWS Shared Responsibility Model

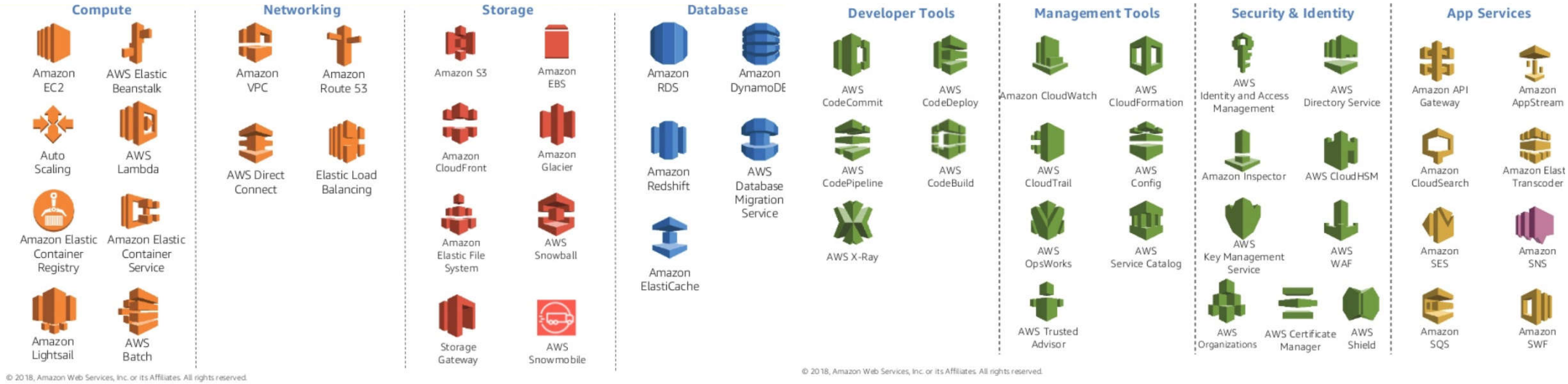
- AWS responsibility is to provide a reliable and secure infrastructure, where the customer services can be built on, a «foundation»
- Customer responsibility is determined by the services chosen
- Wide range of services
- And third party deliveries



https://aws.amazon.com/compliance/shared-responsibility-model/

AWS in a nutshell

- Launched in 2006, originally to utilize computing capacity investment for Christmas season
- More than 4000 features with around 1500 launched in ’17
- In Europe, Ireland is the main site and expanding rapidly, also in the Nordics



Based on https://www.slideshare.net/AmazonWebServices/awsome-day-nashville-2018training

Security infrastructure

- Principles and tools
- Identitiy and Access Management, Certificates
- Security services
  - Security Group, Internet gateway, NAT gateway
  - Network security: IDS, WAF, network functions
  - Vulnerability management
  - Data encryption and protection

Security infrastructure

- Isolation levels and possibilities:
  - Inside VPC: security groups, NACLs, IAM resource level constraints
  - Between VPCs: separate networks, peering, routing and IAM
  - Between accounts: treated as having no connection between «foreign network»

Security controls

- Remember the lecture on the 20 critical controls

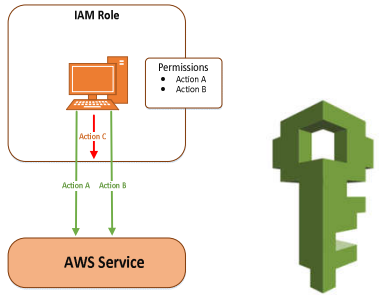
- Directive controls
  - AWS organizations and AWS IAM
- Preventive controls
  - Security Group, CloudFormation, OpsWorks, VPC, Shield, WAF
- Detective controls
  - CloudTrail,AWS Config, CloudWatch, Inspector, network flow logs
- Responsive controls
  - AWS Trusted Advisor, Amazon Config Rules,

Identity and Access Management

- Controls access to resources and services run on AWS
  - Manage and set up permissions for users and applications
  - Supports federation through standard interfaces
- Main components are: policy, role and group:
  - Policy defines the actions, resources and other options
  - Role is an identity with policies connected to it
  - Group is an entity, which can connec to mulitple common policies

Identity and Access Management

- Best practices:
  - Minimize root account use, mulit-factor authentication is a must for root, enable at first use, create own IAM role at once, root shall not be used for management
  - Create individual user accounts – that we have talked about already, when the situation allows, use personal accounts, helps both in forensics and keeping your users cautious
  - Use groups and roles, avoid granting an access rule directly to a user
  - Use own roles for applications e.g. run on EC2
  - Use AWS default policies if you can



Security services

- AWS Key Management System
- CloudHSM
  - Highly secure tamper resistant component for cryptographic operations
  - To my knowledge, the only actual physical device you can own in aws
- AWS Inspector
  - Automated compliance and vulnerability scanner for applications deployed in aws.
- AWS Certificate Manager
  - Provision, manage and deploy TLS certificates, supports ELB or CloudFront
- Security Groups

AWS Key Management Service

- Managed service for encryption key management
- Allows importing keys
- Easy integration with other AWS services
- AWS SDK available to integrate with your own application

- To support cryptograpic applicatons:
  - Encryption in transit and at rest
  - Disk volume encryption
  - Database encryption

Cryptographic services – storage and database

- S3 server side (encryption after data is recieved):
  - S3-managed keys: SSE-S3
  - AWS KMS managed keys: SSE-KMS
  - Customer-provided keys: SSE-C
- S3 client side (encryption before data is sent):
  - Use an AWS KMS-managed customer master key
  - Use a client side master key
- Database: server side with KMS, server side with HSM, client side, support depends on the actual database solution (most support for KMS)

Network security

- Secure DNS: Route 53
- GuardDuty – IDS
- AWS Shield (Advanced) – WAF
- Controlling in- and egress traffic: Internet Gateway, NAT Gateway, VPC, transit VPC, NACL, Security Groups

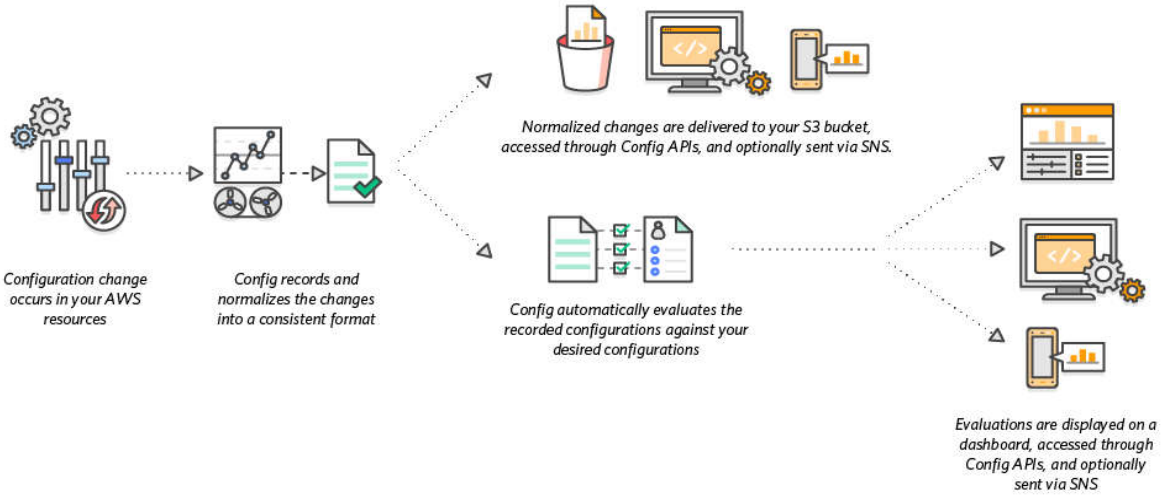
- DDoS: layer 3 and 4: using filtering, elasticity, routing, L7: Shield and WAF

Shield Advanced

- Paid service (free version available)
  - Visiblity into attacks
  - Custom mitigations
  - Post attack analysis
  - Instant rule updates and rule subscriptions

Management

- AWS Config
  - Resource inventory, configuration history and change notifications
  - Record, archive and compare
  - Secure against accidental exposure



Management

- Vulnerability management
  - Nessus or Qualys
  - Golden image creation with aws AMI
- AWS Inspector
  - Automatic assessment of applications for vulnerabilities and deviations from best practice
- AWS Macie
  - Accidental exposure, focuses on leaking personal information and other confidential information
- Amazon Config Rules:
  - Enforce best practice, automatic roll-back, trigger additional workflow
- AWS Trusted advisor: cost, performance, security and availability optimizations

Management – Infrastructure as Code

- With AWS CloudFormation
- Orchestrate changes across aws services
- JSON-based text file to describe infrastructure
- Resources created based on template
- Example: https://s3-us-west-2.amazonaws.com/cloudformation-templates-us-west-2/Windows_Single_Server_Active_Directory.template

Management – Trusted Advisor

- Checks available for all (some features free):
  - Security: security groups, IAM use, MFA for root, snapshots, S3 bucket permissions, CloudTrail,
  - Performance: are you within service limits (user plane vs management plane), EC2 with high load, database throughput
  - Cost optimization: EC2 reserved instances, Idle EC2, Idle LB, RDS idle
  - Fault tolerance: snapshots, Availability zones, VPN redundancy, auto scaling group resources, RDS backup and multi AZ
  - Service limits

Management

- Data protection in practice:
- S3: add metadata and set permissions, switch on native KMS-based encryption at rest, limit access (no public avail. -> e.g. Macie can find it)
- EBS (elastic block storage, volume type): restrict to be accessible only by creating account, only users in AWS IAM, integrates with KMS

Logging: monitoring, forensics and compliance

- Sources:
  - CloudTrail: records AWS API calls
  - CloudWatch logs and events (alarms)
  - Load balancer logs
  - S3 logs
  - AWS IAM
  - VPC flowlogs
    - This looks like e.g. a wireshark capture
- Splunk

Logging: monitoring, forensics and compliance

- Compliance:
  - AWS Artifact: access to aws compliance reports
  - AWS Macie
  - Amazon Config Rules

Penetration testing

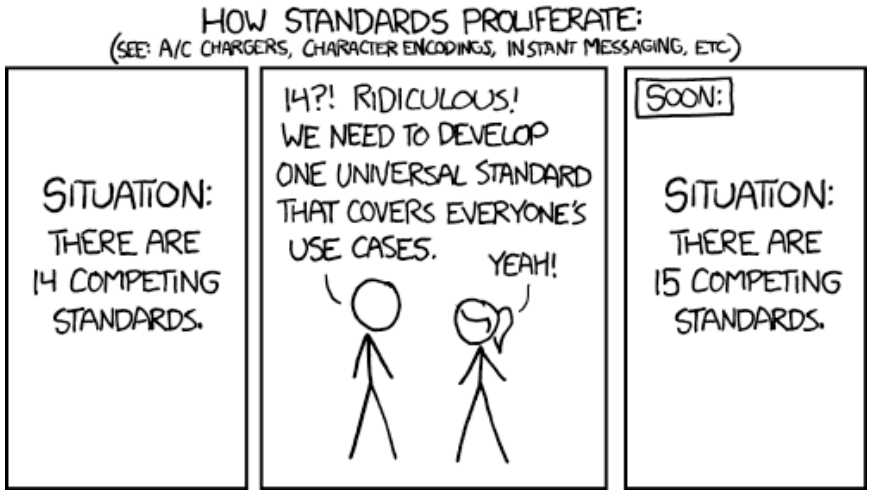
- Customers can execute tests agains 8 services without prior permission (new)
  - But not:
    - DNS zone walking via Amazon Route 53 Hosted Zones
    - Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS
    - Port flooding
    - Protocol flooding
    - Request flooding (login request flooding, API request flooding)

AWS IoT

- In general: exploit the global reach, flexible infrastructure

- Larger operations are especially interesting: predictive maintenance, traffic management, logistics, demand estimation
- Provides infrastructure to get information from the edge and process it with AWS services.
- An interesting feature is the Rules engine, which can be queried with SQL-like expressions
- Higher-level services built on the acquired data (e.g. traffic stats -> prediction)
- Device Shadow, use Lambdas

Standardization

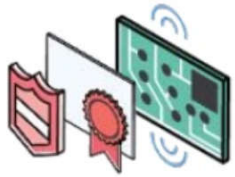


Main steps in AWS IoT

"Securely connect one or one-billion devices to AWS, so they can interact with applications and other devices"

1

Securely connect any physical device to AWS



Connect any device via MQTT/HTTP securely. Quickly get started with AWS IoT Starter Kits and Scale to billions of messages across millions of devices

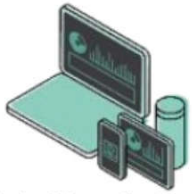
2

Respond to signals from your fleet of devices and take action with Rule Engine

Shift business logic from device to cloud and route data to AWS service of your choice for storage and analysis using rules engine.

3

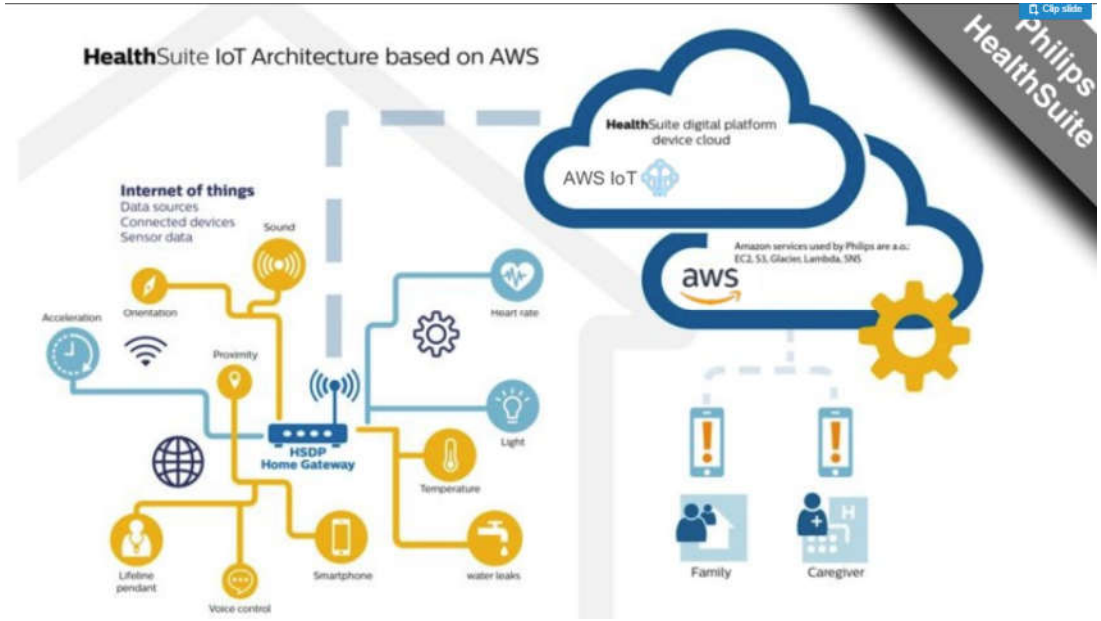
Create Web and Mobile Applications that Interact with Devices reliably at any time



Easily build applications on web and mobile that interact with devices, even when they are offline, with AWS SDK and Device Shadow.

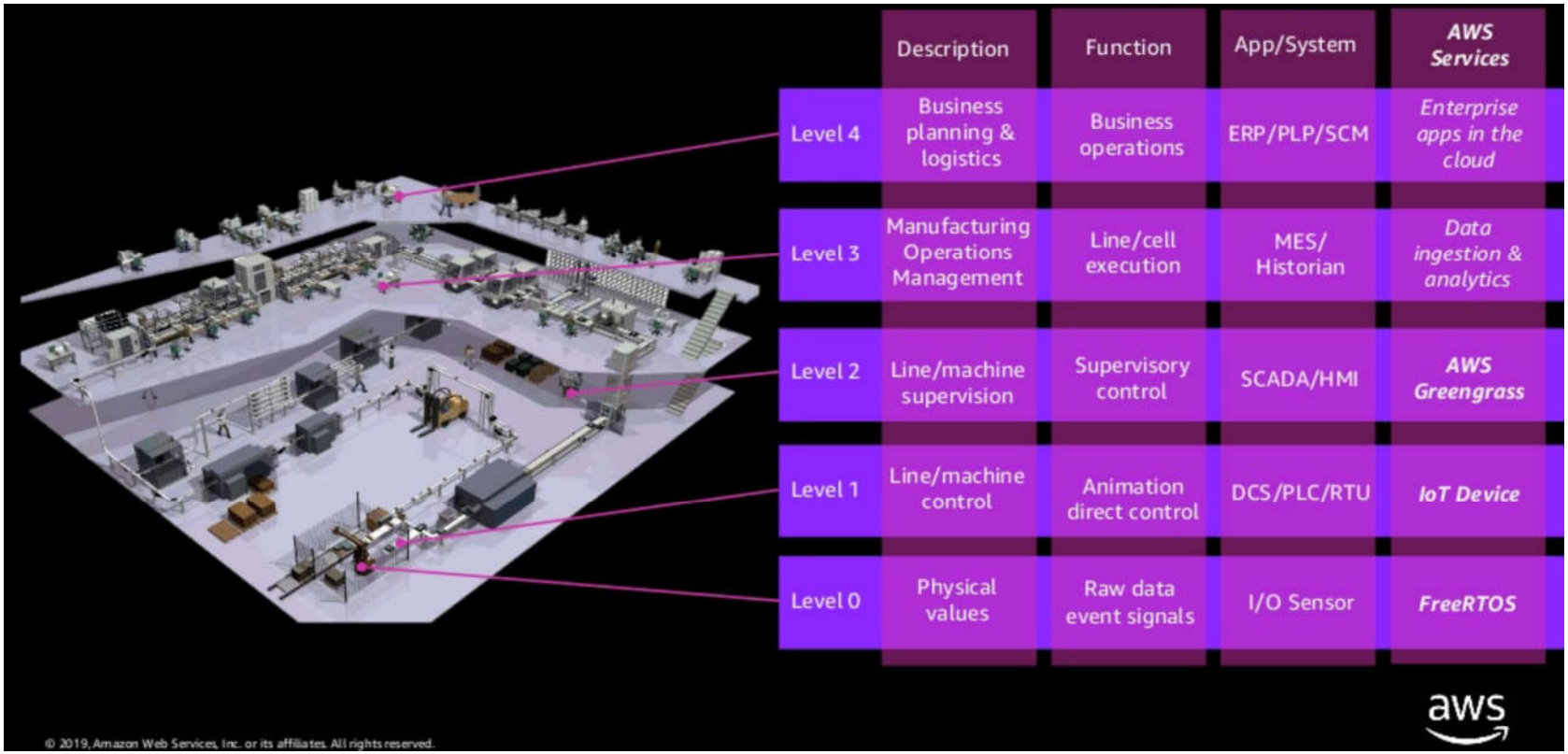
https://www.slideshare.net/AmazonWebServices/intro-to-aws-iot-80291679

Healthcare example



https://www.slideshare.net/AmazonWebServices/intro-to-aws-iot-80291679

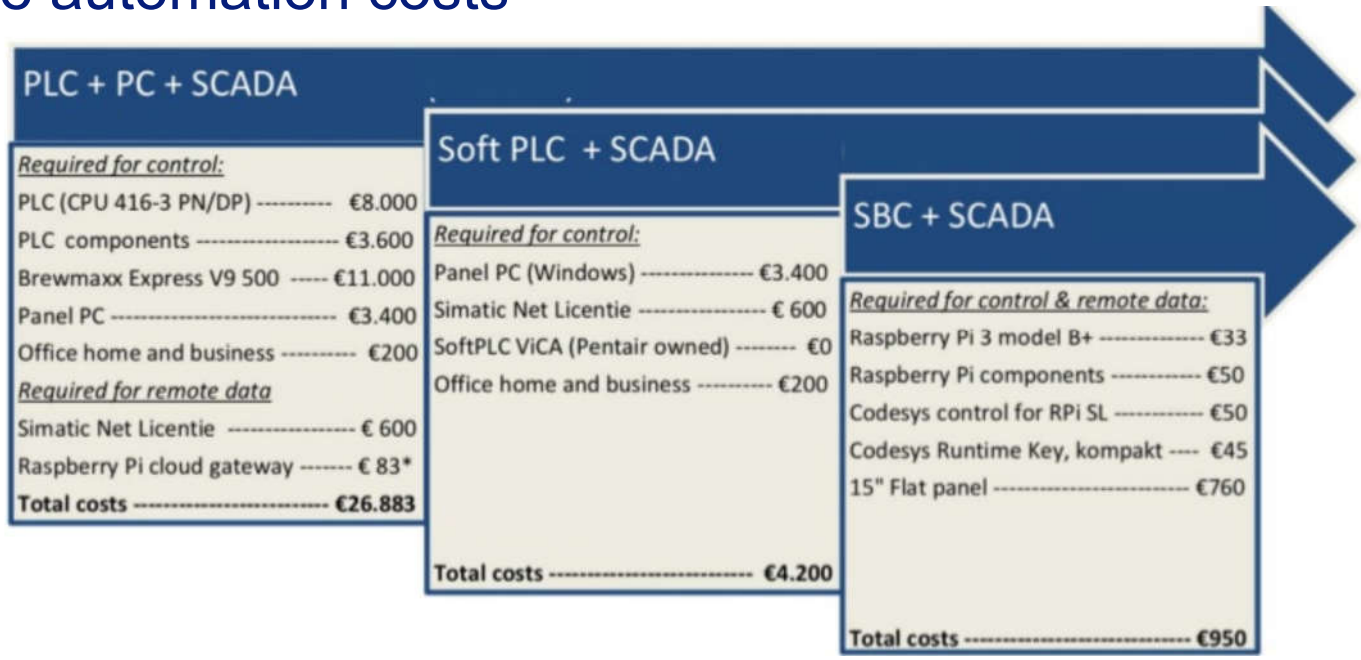
AWS in relation to ISA-95



https://www.slideshare.net/AmazonWebServices/aws-intelligent-at-edge-for-iot

Be careful!

- Slide from the same presentation as on the previous one
- One has to be careful: the system is getting cheaper, but the capabilities and the environment, where they can be operated is changing
- It is _not this easy_ to cut the automation costs

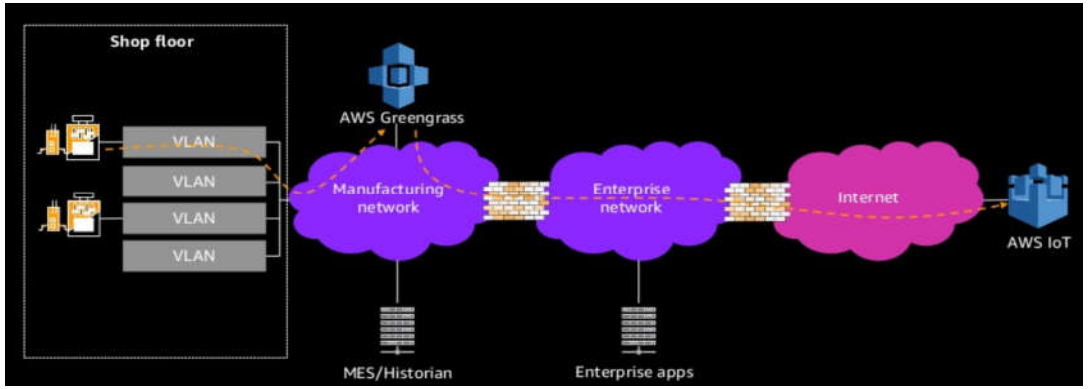


AWS FreeRTOS

- A free RTOS with extensions to connect to AWS services
  - Key importance for getting market share
  - OS is important in the budget of embedd projects
  - https://aws.amazon.com/freertos/

AWS Greengrass

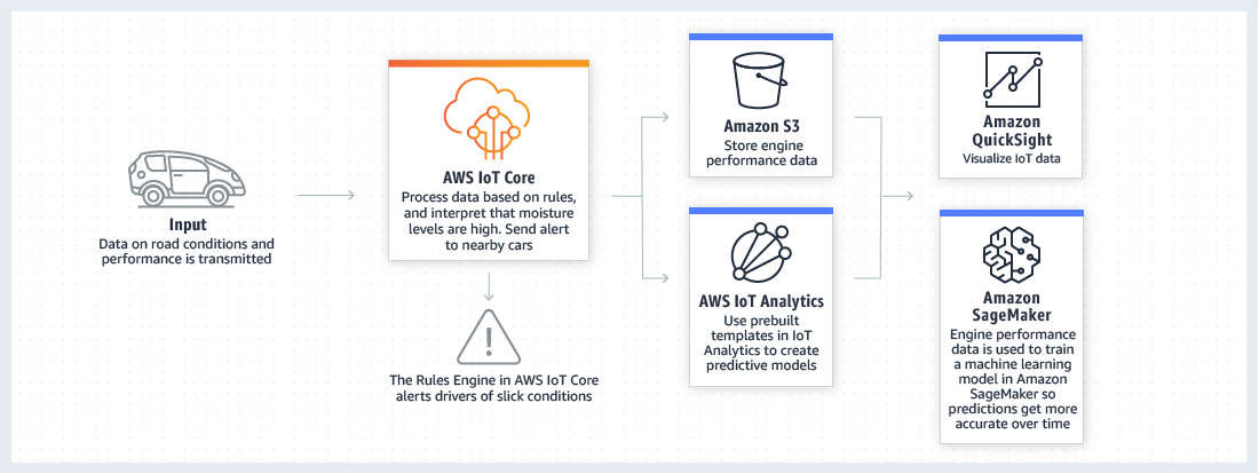
- Together with Amazon FreeRTOS: enable amazon IoT for a wider audience
- Offline operation with Lambda and device shadow support
- Local extraction, processing and reaction possiblity → QoS, criticality!
- Forwards information to AWS IoT core → which can then serve them as SaaS to Enterprise IT
- Secrets manager
- HW security

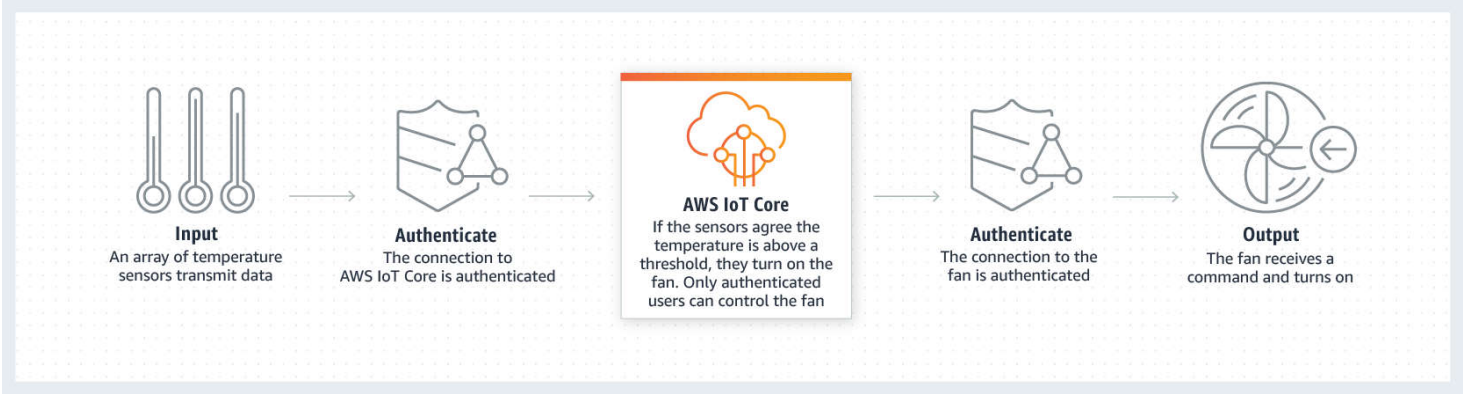


https://www.slideshare.net/AmazonWebServices/aws-intelligent-at-edge-for-iot

AWS IoT Core

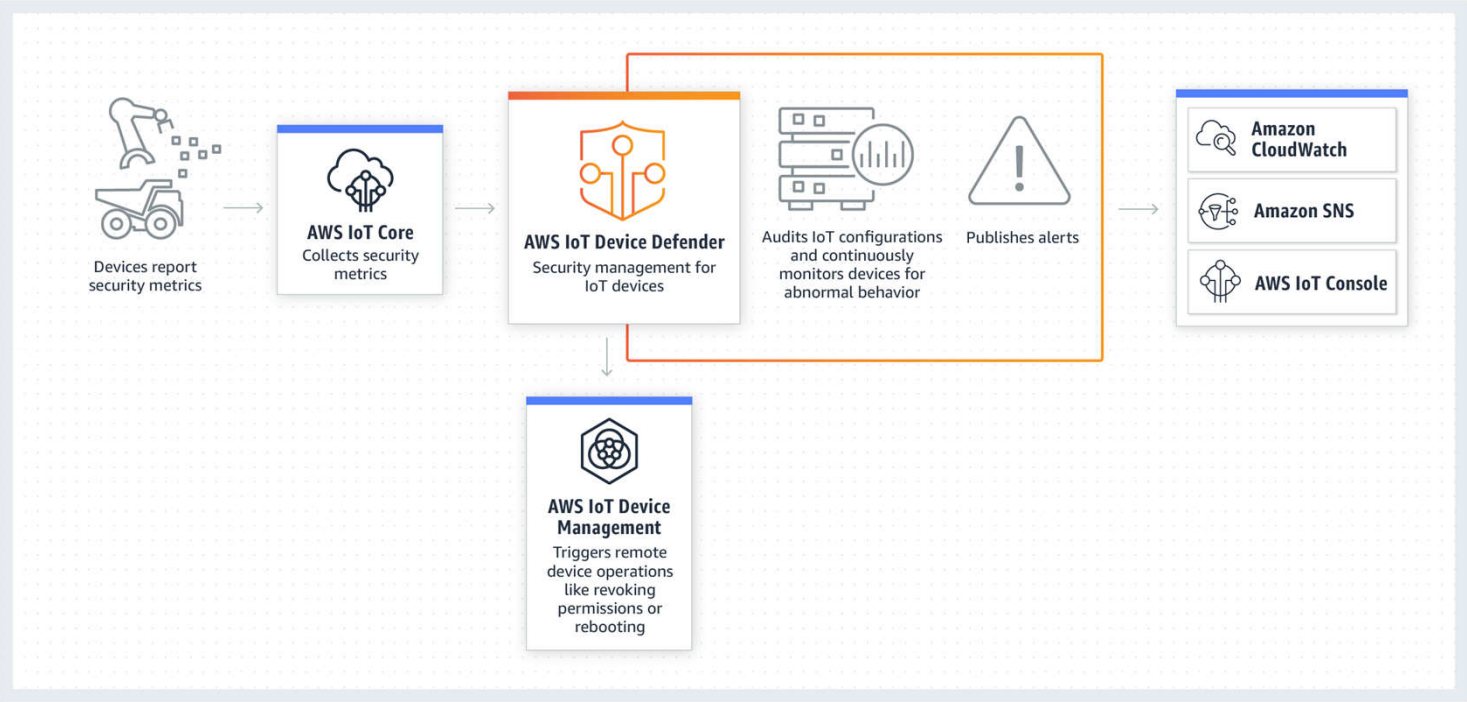
- Is a managed service to allow connectivity from the field to cloud services



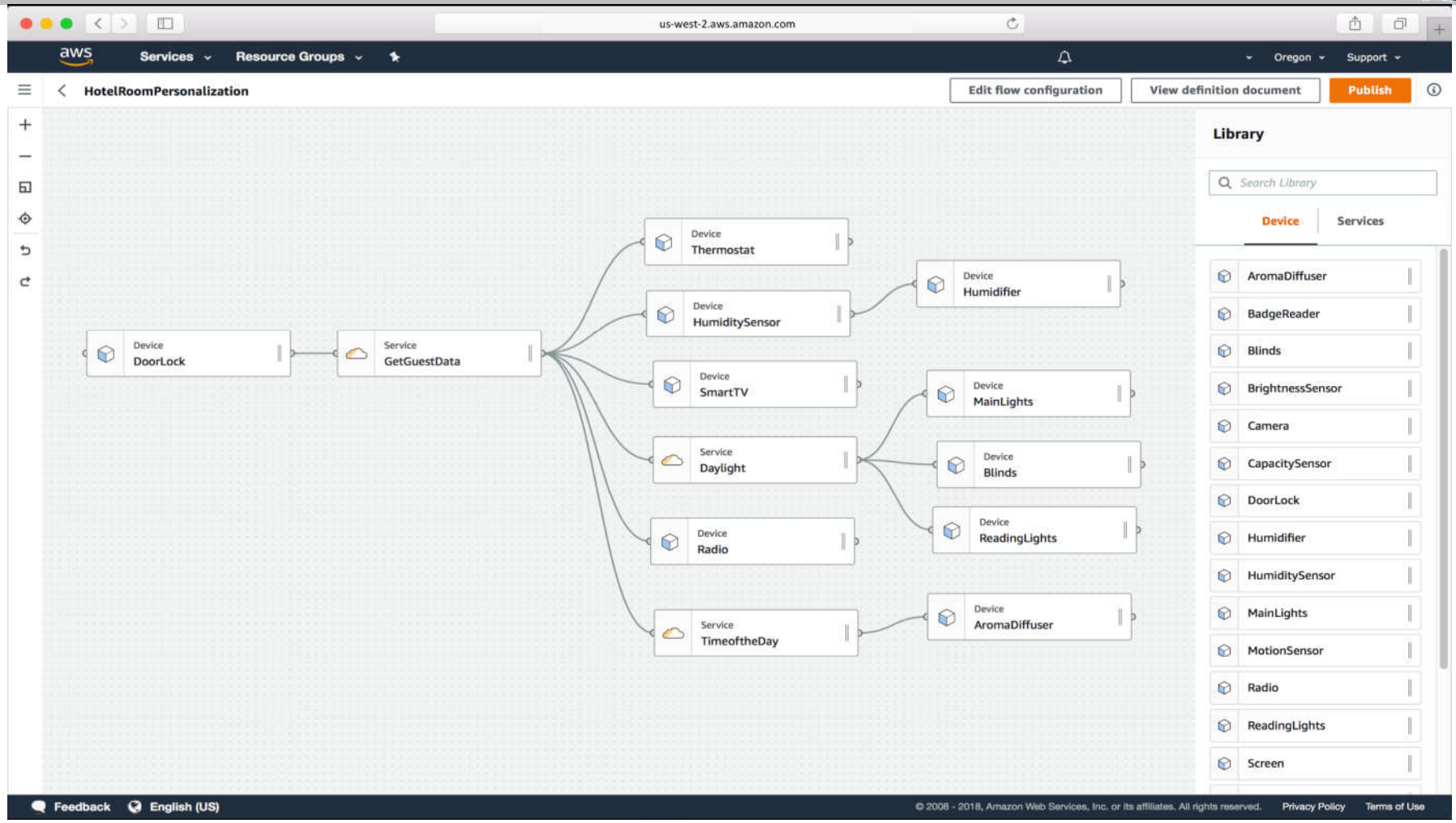


AWS IoT Device Defender

- Supports IoT Core with auditing the configuration against best practice and company policy
- Continous compliance, Attack surface evaluation, Threat impact analysis



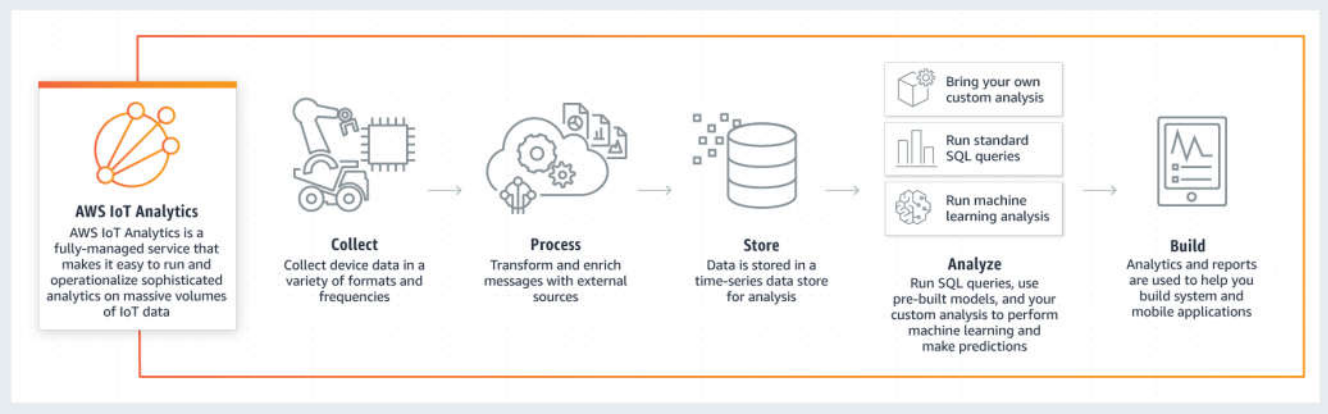
IoT ThingsGraph



IoT and analytics - SiteWise

- A combination of insight into IoT and processing power and analytics in cloud allows us to work on optimizations in different fields:
  - Classification
  - Route optimization
  - Anomaly detection
  - Prediction and forecast
  - Language processing
  - KPI identification

- Data lake: store unstructured data and run analytics on it



Security resources

- https://aws.amazon.com/security/videos/
- https://aws.amazon.com/security/penetration-testing/
- https://aws.amazon.com/blogs/security/videos-and-slide-decks-from-the-aws-reinvent-2017-security-compliance-identity-track/