Welcome and Opening Remarks

Mike Watson

Sept. 2
• Mike Watson, Opening & Welcome Remarks

• David Raymond, Virginia Cyber Range

• Peter Smith, Zscaler

• Milty Brizan, Amazon Web Services
Virginia Cybersecurity Education – Leading the Nation!

David Raymond, Ph.D.
Director, Virginia Cyber Range
draymond@virginiacyberrange.org
Cybersecurity Talent Shortfalls

National level

<table>
<thead>
<tr>
<th>TOTAL CYBERSECURITY JOB OPENINGS</th>
<th>SUPPLY OF CYBERSECURITY WORKERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>504,316</td>
<td>Very Low</td>
</tr>
</tbody>
</table>

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

997,058

SUPPLY/DEMAND RATIO

National average

2.0
Cybersecurity Talent Shortfalls

Virginia

TOTAL CYBERSECURITY JOB OPENINGS
49,669

TOTAL EMPLOYED CYBERSECURITY WORKFORCE
88,166

SUPPLY OF CYBERSECURITY WORKERS
Very Low

CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO

VA: 1.8
National average: 2.0
How do we solve this?
Making Virginia a National Resource for Cybersecurity Education
Virginia Higher Ed Cybersecurity Education: Recent Developments

• Rapid increase in NSA-certified Centers for Academic Excellence in Cybersecurity Education (CAE)
  • Virginia has doubled the number of CAEs since 2016, from 11 to 22
• George Mason University Cybersecurity Engineering Department
  • Unique in the nation!
• Radford IMPACT program
  • Online, competency-based programs in cybersecurity
  • Workforce development for cybersecurity and geospatial intelligence
  • Includes cybersecurity certificate program for Virginia K12 teachers
Commonwealth Cyber Initiative

• Collaborative effort among academia and industry, started in 2018
  • 21 Universities; 320 Faculty
  • $99M+ in sponsored research
  • 5G Testbed
  • AI Assurance research
• $20M annual investment from the state
• Led by Virginia Tech
  • Dr. Luiz DaSilva – Executive Director

“Building an engine for research, innovation, and commercialization of cybersecurity technologies”

Four Regional Nodes
• Northern Virginia
  • GMU
• Central Virginia
  • VCU
• Coastal Virginia
  • ODU
• Southwest Virginia
  • VT
### VDOE Cybersecurity Career Pathway Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>6302</td>
<td>Cybersecurity Fundamentals</td>
</tr>
<tr>
<td>6304</td>
<td>Cybersecurity Software Operations</td>
</tr>
<tr>
<td>8338</td>
<td>Health Informatics</td>
</tr>
<tr>
<td>8628</td>
<td>Cybersecurity Systems Technology</td>
</tr>
<tr>
<td>8499</td>
<td>Cybersecurity in Manufacturing</td>
</tr>
<tr>
<td>6306</td>
<td>Cybersecurity Software Operations, Advanced</td>
</tr>
<tr>
<td>8629</td>
<td>Cybersecurity Systems Technology, Advanced</td>
</tr>
<tr>
<td>8630</td>
<td>Cybersecurity Network Systems</td>
</tr>
<tr>
<td>8000</td>
<td>Cybersecurity in Food and Agriculture Industry</td>
</tr>
<tr>
<td>8200</td>
<td>Cybersecurity in Family and Work Life</td>
</tr>
<tr>
<td>8100</td>
<td>Cybersecurity in Digital Marketing</td>
</tr>
</tbody>
</table>

*The Cybersecurity Fundamentals course (Year 1) serves as the “core” for all Year 2 courses in the coherent sequence.*
Virginia Cyber Range
What is a Cyber Range?

- Isolated network
  - Activity will appear malicious
  - Actual malware sometimes used
- Usually virtualized
  - Allows for maximum configurability
  - Scripted network environment creation
- Used for:
  - Hands-on cybersecurity training
    - Defensive AND offensive
    - Classroom exercises
    - Capture-the-flag and red/blue CTFs
  - Device and software testing
2016 Executive Budget Document, Item 224, Paragraph J:
“Out of this appropriation, [two years of funding will be] designated to support a cyber range platform to be used for cyber security training by students in Virginia's public high schools, community colleges, and four-year institutions. Virginia Tech shall form a consortium among participating institutions, and shall serve as the coordinating entity for use of the platform. The consortium should initially include all Virginia public institutions with a certification of academic excellence from the federal government.”
Governance:
Executive Committee

- Danville Community College
- George Mason University
- Germanna Community College
- James Madison University
- Longwood University
- Lord Fairfax Community College
- Norfolk State University
- Northern Virginia Community College
- Old Dominion University
- Radford University
- Southwest Virginia Community College
- Thomas Nelson Community College
- Tidewater Community College
- University of Virginia
- Virginia Commonwealth University
- Virginia Tech
- Virginia Western Community College
Leveraging the Public Cloud

Design Requirements:
- Scale to support thousands of students
- Up and running quickly
- Completely automatable
- Cost effective
- Short-term surge capacity
- Available state-wide (or anywhere?)
- Web portal for access to content
  - Role-based access
  - Login to see user-specific content
  - Students just need a web browser and internet connection!

Why the Cloud?
- Unlimited scalability!
- Quick start-up phase
- Low capital investment
- Rapid scalability
- Surge capacity
- Location independent
- Highly automated
- Available anywhere
Courseware Repository
- Courses, modules, and exercises for use in HS, CC, and university cybersecurity curricula
  - Instructors/professors can select course content in full or a la carte
- Grants offered for courseware development

Exercise Area
- Menu of per-student, isolated exercise environments for use in cybersecurity courses
- Instructors provision for their students – no delays waiting for administrators
- Capture-the-Flag infrastructure for cybersecurity competitions

Community of Purpose
- Consortium governance
- Convene workshops and conferences to “teach the teachers” and share best practices
- Helping to expand NSA/DHS CAE certification among Virginia colleges and universities
Making Virginia a National Resource for Cybersecurity Education
Step 1: Create Course

CFRS 660 Network Forensics

- John Doe
- 1 exercise
- 9 students

Step 2: Enroll Students

People

- Instructor: John Doe
- TA: Jane Smith
- Student: David White
- Student: Erin Brown
- Student: Sandra Black
- Student: Thomas Green
- Student: Russel Teal
- Student: Lolita Gray
- Student: Ellen Jade
- Student: Chris Gold
- Student: Amy Melon

Step 3: Provision Environments
Capture the Flag!

• Just deployed new CloudCTF platform to the Virginia Cyber Range

• Players solve “challenges” across a variety of categories, including networking, cryptography, web, exploitation, and reconnaissance.

• Great to introduce newbies to cybersecurity, and to challenge experts!

• Used for:
  • In-class gamification and topic reinforcement
  • Cybersecurity clubs and teams
  • Conferences and other outreach events
Exercise Area Stats

Cumulative # of users

- 258 Spring '17
- 440 Fall '17
- 678 Spring '18
- 3,009 Fall '18
- 4,544 Spring '19
- 9,313 Fall '19

Virtual Classrooms Created

- Spring '17: 3
- Fall '17: 128
- Spring '18: 178
- Fall '18: 272
- Spring '19: 247
- Fall '19: 332

20,000 Virtual Machines Provisioned in Fall 2018
Schools Supported

We support **220** high schools, **21** community colleges, and **13** public universities in Virginia.

* Each dot represents a different Virginia high school, community college, or university.
Community

Teacher Camps and Live Conference Workshops

Online "Weekly Workshops (Recorded)"
Annual Virginia Cybersecurity Education Conference

• 2 Days in July/Aug
  • Day 1: Workshops and keynote
  • Day 2: Talks and panels
US Cyber Range

- Providing Cyber Range as a Service
  - Schools outside of Virginia
  - Private schools in Virginia
  - Government and industry nationwide
  - 33 Customers in 20 states
- Customer organizations contract with Virginia Tech
  - “Service Center” within the university
  - Cost reimbursement model
- Students and teachers access cloud-based network infrastructure and CTFs via web portal
How Can *You* Help?

• Partner with Commonwealth Cyber Initiative and other orgs to support and expand cyber education in Virginia
  • More info here: [https://cyberinitiative.org/](https://cyberinitiative.org/)

• Support continued high school cybersecurity courses in your district
  • Reach out to Career and Technical Education (CTE) departments and offer your expertise

• Be a CyberPatriot team mentor
  • Go to [https://www.uscyberpatriot.org/](https://www.uscyberpatriot.org/) to register
“The Virginia Cyber Range has enabled me to teach a Cybersecurity class without needing expensive hardware and software.”

“Without this environment, my students would have only learned theory and seen pictures of what a professional might use in this work.”

“The Virginia Cyber Range is a definite game changer!”

“There are a variety of big-ticket range products out there that are just unwieldy and hard to implement. This is quick, easy, and to the point!”
Questions?

Making Virginia a national resource for cybersecurity education.

CONNECT WITH US
@VaCyberRange
virginiacyberrange.org
Microsegmentation
Powered By Zero Trust

Peter Smith
VP, Zscaler Workload Segmentation
Agenda

Why microsegmentation?

Limitations of existing approaches

A new approach based on zero trust and automation

Demo

Q&A
Flat Networks Allow Too Many Attack Paths

87% Allowed network paths unused within large segments
Experts Recommend Improve Segmentation And Use Zero Trust

<table>
<thead>
<tr>
<th>THREAT</th>
<th>IMPACT</th>
<th>EXPERTS RECOMMEND</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation State (Gov. agency)</td>
<td>21.5M PII records</td>
<td>“Zero trust model” US-HCOGR</td>
</tr>
<tr>
<td>APT (Financial services)</td>
<td>146M PII records</td>
<td>“Enhance network segmentation”</td>
</tr>
<tr>
<td>Ransomware (Logistics co.)</td>
<td>$300M, 29k systems</td>
<td>“... least privilege” US CERT</td>
</tr>
<tr>
<td>Insider Threat (Healthcare co.)</td>
<td>18K PHI records</td>
<td>&quot;Network segmentation&quot; SecurityMetrics</td>
</tr>
</tbody>
</table>

Gartner: “Identity-based segmentation” is a core protection strategy for cloud workloads.
Shrinking Segments Is Complex and Time Consuming
Shrinking Segments Is Complex and Time Consuming

Despite your investment, threats continue to move laterally through traditional controls.
Automating Segmentation Using Zero Trust
Impossibly simple microsegmentation with Zero Trust security

- Eliminate Attack Paths
- Provable Security
- Immediate Results
- Zero Touch Management

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION

Securing your cloud transformation
Automating Segmentation Using Zero Trust

Impossibly simple microsegmentation with Zero Trust security
Fully Automated Microsegmentation

All policy management tasks automated to radically simplify operations
1-Click Simplicity ➔ Provable Outcomes
Measurable return on your security investment
Don’t Change Your Network, Change Your Security
Overlay microsegmentation delivers identity-based protection with no change to your network
Microsegmentation as a Service
Zero Trust Identity
Patented technology driving Zero Trust Auto-Segmentation

Zero Trust Identity Policies
Authorizes communications by verifying software- and machine- identity

ZTID™ FINGERPRINT

SOFTWARE
Hash (SHA256)
Fuzzy Hash (LSH)
Process Signing
PE Header Values
Process Identifiers

USER
SID/User ID

CONTAINER
Container ID
Image ID

HOST OS
Racial Learning
Provisioned Hostname
BIOS UUID
CPU Serial Numbers
Network Namespace

NETWORK
Address, Port, Protocol

RISK
Software Reputation
Behavioral Scoring
Capabilities Classification
Zero Trust Identity Verification
Delivers the strongest protection in untrusted networks

- **Resilient Identity**
  - ZT Identities are resilient to software upgrades and CI/CD deployments

**ZTID Fingerprint**
- **Software**
  - SHA256: BA7816BF8F01CFEA41440DE...
  - LSH: 50FDE99373B04363727400AE98A...
  - PE Signer: Demo Company, Co.
  - PE Product Name: User Manager
  - PE Original Name: user_mgr.jar
  - Reputation: Good
  - Capabilities: Single Function

- **Host**
  - Hostname: winusrmgr01.prod.company.co
  - BIOS UUID: 75D64596-53F8-426C-903B...
  - CPU Serials Hash: 18EE24150DCB1D967...

**ZTID Fingerprint**
- **Software**
  - SHA256: ED2456914E48C1E17B7BD922...
  - LSH: BF6F9792B2A5EAA331426E8523...
  - PE Signer: Microsoft Corporation
  - PE Product Name: MS SQL Server 2016
  - PE Original Name: sqlsrv.exe
  - Reputation: Good
  - Capabilities: Single Function

- **Host**
  - Hostname: winusrdb01.prod.company.co
  - BIOS UUID: 062ef0f-4b04-4d17-a638-d...
  - CPU Serials Hash: 32CFAD293016DFF08...
Policy Automation Engine
Machine Learning generated policies for identity-based protection and 1-click simplicity

ZERO TRUST
IDENTITY™

REVEAL RISK

BUILD POLICY

AUTO-SEGMENT

SHRINK TIME TO VALUE
✓ Models applications
✓ Analyzes attack paths
✓ Classifies path risk

DRIVE IT EFFICIENCY
✓ Builds application segments
✓ Builds identity-based policies
✓ Optimizes policies

GAP-FREE PROTECTION
✓ Single-click segmentation
✓ Only verified apps communicate
✓ Adapts to change

72 hrs
Initial Learning Time

99%
Policy Confidence

99.9%
Policy Coverage

25x
Policy Compression
Securing your cloud transformation

**The Machine Learning Advantage**

**FIREWALL**
- 15B NET EVENTS
- 1.7M NET EVENTS UNIQUE

**EDGEWISE**
- 267K APP EVENTS
- 40K APP EVENTS ML REDUCED
- 100’s POLICIES ML CREATED

**ML REDUCED APPLICATION EVENTS**
Evaluating network vs. application identity attributes for automated rule generation.

- Compresses data by >6 orders of magnitude
- Reduces computational time
- Increases policy accuracy
Demo
Fully Automated Microsegmentation
All policy management tasks automated to radically simplify operations

1. BUILDING SEGMENTS
2. CREATING POLICIES FOR COMMUNICATION
3. ADDING/REMOVING HOSTS
4. UPGRADE APPLICATIONS
5. DEPLOYING NEW APPLICATIONS
One Platform, Complete Zero Trust Protection
Protection made easy for workloads. No changes to applications or the network

- **Deploy in minutes**
  Lightweight agents automatically installed

- **Measure network exposure risk**
  Visualize app topology and attack paths, and quantify reduction in risk

- **Simulate microsegmentation**
  Segments and policies automatically built by machine learning

- **Enforce policies & manage updates**
  Zero trust protection that adapts to changes in the environment
Thank you. Q&A
Managing Security on AWS

Milty Brizan
Solutions Architect, WWPS, State and Local Government, AWS
Security is our top priority

- Designed for security
- Constantly monitored
- Highly automated
- Highly available
- Highly accredited
Benefits of AWS Security

- Keep Your Data Safe
- Meet Compliance Requirements
- Save Money
- Scale Quickly
AWS Security Tools & Features

- Identity & Access Control
- Data Encryption
- Infrastructure Security
- Monitoring & Logging
- Inventory & Configuration
- AWS Partner Solutions
Economies of Scale Apply to Security and Compliance

Tough scrutiny, robust capabilities, constant improvements, and a world-class AWS security team benefit the whole client community.

The stringent demands of a few…

Set a higher standard for everyone

Everyone’s Systems and Applications

Amazon Web Services Security Infrastructure
What does this mean?

- You benefit from an environment built for the most security sensitive organisations
- AWS manages a multitude of security controls so you don’t have to
- You get to define the right security controls for your workload sensitivity
- You always have full ownership and control of your data
AWS Shared Responsibility Model
With AWS, Security Is a Shared Responsibility

Customers concentrate on systems and apps while AWS manages infrastructure.

Security expertise is a scarce resource; AWS oversees the big picture, letting your security team focus on a subset of overall security needs.
AWS Shared Responsibility Model

- Will one model work for all services?
Shared Responsibility Model - Infrastructure

- **Managed by AWS Customers**
  - CUSTOMER DATA
  - PLATFORM & APPLICATION MANAGEMENT
  - OPERATING SYSTEM, NETWORK, & FIREWALL CONFIGURATION
    - CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
    - SERVER-SIDE ENCRYPTION (File System and/or Data)
    - NETWORK TRAFFIC PROTECTION (Encryption / Integrity / Identity)
  - OPTIONAL - OPAQUE DATA: In transit/at rest

- **Managed by Amazon Web Services**
  - AWS ENDPOINTS
    - FOUNDATION SERVICES: COMPUTE, STORAGE, DATABASES, NETWORKING
    - AWS GLOBAL INFRASTRUCTURE: REGIONS, AVAILABILITY ZONES, EDGE LOCATIONS

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Shared Responsibility – Container Services

- **Customer Data**
  - Client-side data encryption & data integrity authentication
  - Network traffic protection: Encryption / Integrity / Identity
  - Optional – Opaque Data: OS and 1S (In transit/rest)

- **Platform & Application Management**

- **Operating System & Network Configuration**

- **AWS Global Infrastructure**
  - Regions
  - Availability Zones
  - Edge Locations

- **AWS Services**
  - Compute
  - Storage
  - Databases
  - Networking

Managed by AWS Customers

Managed by Amazon Web Services
Shared Responsibility – Abstracted Services

- **Customer Data**
  - Client-side data encryption & data integrity authentication
  - Server side encryption provided by the platform
  - Network traffic protection provided by the platform

- **Platform & Application Management**

- **Operating System, Network, & Firewall Configuration**

- **AWS Services**
  - Compute
  - Storage
  - Databases
  - Networking

- **AWS Global Infrastructure**
  - Regions
  - Availability Zones
  - Edge Locations

Managed by AWS Customers

Managed by Amazon Web Services
Benefiting from Abstracted Services:
Serverless Architectures
Benefits of Serverless Architectures

- Developers can focus on their core product
  - No server management
  - Flexible scaling
  - Automated high availability

- Let AWS manage the security of the underlying services
  - We do the undifferentiated heavy lifting

- Reduced overhead lets developers reclaim time and energy that can be spent on developing great products
Real-time File Processing
Mobile Back-end
AWS Lambda: Real-time voting application
Applying the Shared Responsibility Model

- **Security of the cloud**
  - Security measures that **AWS** implements and operates
  - AWS security standards shown by **certifications** & **attestations**

- **Security in the cloud**
  - Security measures that the **customer** implements and operates
  - **Certifications** and **attestations** can be used by customers when undertaking risk assessments or using **frameworks**
Security OF the Cloud
AWS Compliance

- Compliance **certifications** and **attestations** are assessed by a third-party, independent auditor and result in a **certification**, **audit report**, or **attestation of compliance**.
Accessing AWS Compliance Reports

- AWS Artifact:
  - On-demand access to AWS’ compliance reports
  - Globally available
  - Easy identification
  - Quick assessments
  - Continuous monitoring
  - Enhanced transparency
Assurance Programmes - Global

- **CSA**
  Cloud Security Alliance Controls
- **ISO 9001**
  Global Quality Standard
- **ISO 27001**
  Security Mgmt Controls
- **ISO 27017**
  Cloud Specific Controls
- **ISO 27018**
  Personal Data Protection

- **PCS DSS Level 1**
  Payment Card Standards
- **SOC 1**
  Audit Controls Report
- **SOC 2**
  Security, Availability & Confidentiality Report
- **SOC 3**
  General Controls Report
Assurance Programmes - Europe

C5 (Germany)
Operational Security Attestation

Cyber Essentials Plus (UK)
Cyber Threat Protection

ENS High (Spain)
Spanish Govt Standards

G-Cloud (UK)
UK Govt Standards

IT-Grundschutz (Germany)
Baseline Protection Methodology

And many more…

https://aws.amazon.com/compliance/
<table>
<thead>
<tr>
<th>Certifications / Attestations</th>
<th>Laws, Regulations, and Privacy</th>
<th>Alignments and Frameworks</th>
</tr>
</thead>
<tbody>
<tr>
<td>C5 [Germany]</td>
<td>CISPE</td>
<td>CIS</td>
</tr>
<tr>
<td>Cyber Essentials Plus [UK]</td>
<td>DNB [Netherlands]</td>
<td>CJIS</td>
</tr>
<tr>
<td>DoD SRG</td>
<td>EU Model Clauses</td>
<td>CSA</td>
</tr>
<tr>
<td>FedRAMP</td>
<td>FERPA</td>
<td>ENS [Spain]</td>
</tr>
<tr>
<td>FIPS</td>
<td>GLBA</td>
<td>EU-US Privacy Shield</td>
</tr>
<tr>
<td>IRAP [Australia]</td>
<td>HIPAA</td>
<td>FISC [Japan]</td>
</tr>
<tr>
<td>ISO 9001</td>
<td>HITECH</td>
<td>FISMA</td>
</tr>
<tr>
<td>ISO 27001</td>
<td>IRS 1075</td>
<td>G-Cloud [UK]</td>
</tr>
<tr>
<td>ISO 27017</td>
<td>ITAR</td>
<td>GxP (FDA CFR 21 Part 11)</td>
</tr>
<tr>
<td>ISO 27018</td>
<td>My Number Act [Japan]</td>
<td>ICREA</td>
</tr>
<tr>
<td>MTCS [Singapore]</td>
<td>VPAT / Section 508</td>
<td>MITA 3.0</td>
</tr>
<tr>
<td>PCI DSS Level 1</td>
<td>EU Data Protection Directive [EU]</td>
<td>MPAA</td>
</tr>
<tr>
<td>SEC Rule 17-a-4(f)</td>
<td>Privacy Act [Australia &amp; New Zealand]</td>
<td>NIST</td>
</tr>
<tr>
<td>SOC 1</td>
<td>PDPA - 2010 [Malaysia]</td>
<td>PHR</td>
</tr>
<tr>
<td>SOC 2</td>
<td>PDPA - 2012 [Singapore]</td>
<td>Uptime Institute Tiers</td>
</tr>
<tr>
<td>SOC 3</td>
<td>PIPEDA [Canada]</td>
<td>UK Cloud Security Principles</td>
</tr>
<tr>
<td></td>
<td>Spanish DPA Authorization</td>
<td></td>
</tr>
</tbody>
</table>
### Inherit controls from AWS

<table>
<thead>
<tr>
<th>Control #</th>
<th>Control Name</th>
<th>Control #</th>
<th>Control Name</th>
<th>Control #</th>
<th>Control Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.11.1.1</td>
<td>Physical security perimeter</td>
<td>A.11.2.1</td>
<td>Equipment siting and protection</td>
<td>A.11.2.7</td>
<td>Secure disposal or reuse of equipment</td>
</tr>
<tr>
<td>A.11.1.2</td>
<td>Physical entry controls</td>
<td>A.11.2.2</td>
<td>Supporting utilities</td>
<td>A.11.2.8</td>
<td>Unattended user equipment</td>
</tr>
<tr>
<td>A.11.1.3</td>
<td>Securing offices, rooms and facilities</td>
<td>A.11.2.3</td>
<td>Cabling security</td>
<td>A.11.2.9</td>
<td>Clear desk and clear screen policy</td>
</tr>
<tr>
<td>A.11.1.4</td>
<td>Protecting against external and environmental threats</td>
<td>A.11.2.4</td>
<td>Equipment maintenance</td>
<td>A.17.2.1</td>
<td>Availability of information processing facilities</td>
</tr>
<tr>
<td>A.11.1.5</td>
<td>Working in secure areas</td>
<td>A.11.2.5</td>
<td>Removal of assets</td>
<td>A.13.1.2</td>
<td>Communications security</td>
</tr>
<tr>
<td>A.11.1.6</td>
<td>Delivery and loading areas</td>
<td>A.11.2.6</td>
<td>Security of equipment and assets off-premises</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security IN the Cloud
Access a deep set of cloud security tools

### Networking & Security
- Amazon GuardDuty
- Amazon VPC
- AWS Direct Connect
- VPN connection
- Security Groups
- AWS Firewall Manager
- Flow logs
- AWS Shield
- AWS WAF
- Route table

### Compliance & Governance
- AWS Service Catalog
- AWS Trusted Advisor
- AWS CloudFormation
- AWS CloudTrail
- AWS Systems Manager
- Amazon CloudWatch
- AWS Config
- AWS Artifact
- Amazon Inspector
- AWS OpsWorks

### Identity
- Amazon Cognito
- IAM
- AWS Directory Service
- AWS Organizations
- Active Directory integration
- Temporary Security credential
- SAML Federation

### Encryption
- AWS KMS
- AWS Secrets Manager
- AWS CloudHSM
- Client-side encryption
- AWS Certificate Manager
Asset Inventory / Management

Knowing, at every point in time, what’s running, where, and why

- **Everything is an API call**
  - Authenticated, signed, logged, whether it’s the GUI, CLI, or SDK
  - All resources are listed in the console and, for CLI users, one API call away

- **AWS Service Catalog**
  - Asset inventory, ownership, responsibility, and access management

- **AWS Systems Manager**
  - Asset inventory, management and automation (including on premises assets)
  - Manage VMs without logging in (RunCommand): immutable infrastructure
  - Patch Management, and configuration checks
Network Segmentation

- **Virtual Private Cloud (VPC)**
  - Private and Public subnets
  - Security Group and NACLs
  - VPC Flow Logs for network monitoring and analysis

- **Range of connectivity options**
  - Internet access
  - IPsec VPN (over Internet)
  - Private Network Connectivity (Direct Connect)

- **Infrastructure as code**
Configuration and Change Management

- **AWS Config and AWS Config Rules**
  - Configuration history and Security rules enforcement
  - Extensive set of built-in rules and you can create your own (security as code)

- **CloudFormation**
  - Configuration management, with a unique source of truth

- **AWS Inspector and AWS Trusted Advisor**
  - Best practices and vulnerability management

- **AWS CloudWatch Events**
  - Respond quickly to notifications from AWS resources delivered in near-real-time

Controlled, monitored, and managed change – in an Agile context
Security by Design

Security by Design (SbD) is a security assurance approach that formalises AWS account design, automates security controls, and streamlines auditing.

Instead of relying on auditing security retroactively, SbD provides security control built in throughout the AWS IT management process.

https://aws.amazon.com/compliance/security-by-design/
Automate Security Operations

Security by Design allows you to automate deployments, provisioning, and configurations of AWS environments.
Advantages to the API

- **Authoritative** – the interface to, and between, AWS services
- **Auditable** – always know what, and who, is doing what
- **Secure** – verified integrity, and no covert channels
- **Fast** – can be read and manipulated in sub-second time
- **Precise** – defines the state of all infrastructure and services
- **Evolving** – continuously improving
- **Uniform** – provides consistency across disparate components
- **Automatable** – enables some really cool capabilities
Automated Remediation: Amazon CloudWatch Events
Automated Remediation: Example

• Customer wants to make sure that there is no Internet access available within a secure VPC
  • IAM policies should provide the first defense
  • The customer would like to be notified in the event that an Internet Gateway does get attached

• Automated remediation: automatically remove the Internet Gateway attachment at the same time as sending the notification

• How could we do this?
Amazon CloudWatch Events

• Delivers a **near real-time** stream of **system events** that **describe changes** in Amazon Web Services (AWS) resources
  • Use simple rules to match events and route them to target function(s)
  • Schedule automated actions that self-trigger at certain times using cron or rate expressions

• Common **use cases** for CloudWatch Events
  • Responding to operational changes
  • Sending notifications
  • Automating corrective actions
Key concepts

- **Event**: indicates a change in your AWS environment
  - Generated from other AWS services
  - Generated on a schedule
  - Generated from custom application-level events

- **Target**: processes events
  - Example targets include AWS Lambda, Kinesis Streams, Step Functions

- **Rule**: matches incoming events and routes them to targets for processing
  - Single rule can match to multiple targets
  - Rules are processed in parallel
Amazon CloudWatch event bus

- Allows the sending of CloudWatch Events to other AWS account(s)
  - Allows for centralised CloudWatch Events within/between organisations
- Receiving accounts can receive events from
  - Whitelisted AWS accounts, or
  - Any AWS account
- Some additional points to consider
  - Chained events aren’t supported (e.g. Acct A → Acct B → Acct C)
  - The sending account is charged for the event; the receiving account is not
  - Rules can be scoped to specific AWS account(s)
Implementation

• Create an Amazon CloudWatch event rule:
  • Trigger the event when an ec2:AttachInternetGateway API call is made
  • Target an SNS topic to notify the security team when this happens

• Test the CloudWatch Events rule
  • Navigate to the VPC console, Internet Gateways section
  • Attach the unattached IGW to the Data VPC
  • You should receive an email notification within 5 minutes

• Automated remediation: hook up a custom Lambda function as a second trigger to CloudWatch Events, to detach the IGW automatically
CloudWatch Events Rule

Create rules to invoke Targets based on Events happening in your AWS environment.

Event Source
Build or customize an Event Pattern or set a Schedule to invoke Targets.

Event Pattern
Service Name: EC2
Event Type: AWS API Call via CloudTrail

Build event pattern to match events by service

Targets
Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.

SNS topic
Topic: alerts

Lambda function
Function: testFunction

Add target
Where to start?
So many services… where do I start?

- AWS provides:
  - Continuous innovation of products and services
  - AWS Quick Starts
  - AWS Answers
  - AWS blogs
  - Comprehensive documentation
  - Extensive partner network
Continuous Innovation
AWS Certificate Manager – Private CA
AWS Firewall Manager

Prerequisites for using AWS Firewall Manager

- Your AWS account must be part of the full feature set enabled. Learn more
- This AWS account must be enabled

Choose an option

- Create an AWS Firewall Manager policy and add existing rule groups.
- Create an AWS Firewall Manager policy and add a new rule group.

Choose a region

The service will create the policy and any associated conditions, rules, and route tables that you choose. The policy will protect only the resources in that region.

Region: US East (N. Virginia)

If the policy will apply to CloudFront distributions, choose CloudFront (CloudFront).

Define policy scope

Specify condition to identify which resources to protect

Region:
- US East (N. Virginia)

Select resource types that will be protected*

- CloudFront distribution
- ELB Application Load Balancer

Use tags to include/exclude resources (optional)

Apply policy?

- Create and apply this policy to existing and new resources.
- Create but do not apply this policy to existing or new resources.

Status

- Noncompliant
- Noncompliant
- Noncompliant

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
AWS Secrets Manager

Store a new secret

Select secret type
- Credentials for RDS database
- Credentials for other database
- Other type of secrets (e.g. API key)

Specify the user name and password to be stored for this secret.

User name: ranman
Password: ********

Select the encryption key
- DefaultEncryptionKey

Select which RDS database this secret will access
- twitterapp2
- twitterapp2-us-east-1a

Configure automatic rotation
- Disable automatic rotation
- Enable automatic rotation

Select rotation interval
- Custom: 10 days

Use the secret that I provided in step 1
Use this option if you are storing a super user.

Use a secret that I have previously stored in AWS Secrets Manager
Use this option if you are sharing a user who will access the database programmatically. ASM will use a previously stored super user to execute rotation.
AWS Config Rules aggregation
Amazon GuardDuty

Enable GuardDuty
With a few clicks in the console, monitor all your AWS accounts without additional security software or infrastructure to deploy or manage

Continuously analyze
Automatically analyze network and account activity at scale, providing broad, continuous monitoring of your AWS accounts

Intelligently detect threats
GuardDuty combines managed rule-sets, threat intelligence from AWS Security and 3rd party intelligence partners, anomaly detection, and ML to intelligently detect malicious or unauthorized behavior

Take action
Review detailed findings in the console, integrate into event management or workflow systems, or trigger AWS Lambda for automated remediation or prevention

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
AWS Quick Starts
What are AWS Quick Starts?

• AWS Quick Starts are:
  • built by AWS solutions architects and partners
  • help you deploy popular solutions on AWS
  • based on AWS best practices for security and high availability

• Covers a wide range of topics
  • DevOps; Security & Compliance
  • Database & Storage; Big Data & Analytics
  • Microsoft & SAP

• [https://aws.amazon.com/quickstart/](https://aws.amazon.com/quickstart/)
Security-focused Quick Starts

- HIPAA
  - Reference architecture that helps support your HIPAA compliance program
  - Learn more | View guide

- NIST
  - AWS architecture that helps supports NIST, DoD, FedRAMP standards
  - Learn more | View guide

- NIST High-Impact
  - AWS architecture for NIST high-impact controls, featuring Trend Micro
  - Learn more | View guide

- PCI DSS
  - Standardized AWS architecture that helps support PCI DSS compliance
  - Learn more | View guide

- UK-OFICIAL
  - AWS architecture that supports the UK’s NCSC and CIS security controls
  - Learn more | View guide

- CIS Benchmark
  - Security configurations for the CIS AWS Foundations Benchmark
  - Learn more | View guide

- CJIS Security Policy
  - Standardized AWS architecture to help support CJIS Security Policy 5.6
  - Learn more | View guide

- Trend Micro
  - Deep Security
  - Security solution with intrusion prevention, anti-malware, host firewall
  - Learn more | View guide

- Sophos
  - Sophos web proxy
    - Sophos UTM and Outbound Gateway for outbound web filtering proxy on AWS
    - Learn more | View guide

- Symantec
  - Symantec Protection Engine
    - Content scanning, malware and threat detection
    - Learn more | View guide

- Security and analytics with Palo Alto Networks and Splunk
  - Palo Alto Networks VM-Series firewall and Splunk Enterprise on AWS
  - Learn more | View guide
CIS Benchmark on AWS

- Standardised architecture for the Center for Internet Security (CIS) AWS Foundations Benchmark.

- Deploys the following AWS services
  - AWS Config rules
  - CloudWatch alarms
  - CloudWatch Events
  - Lambda functions
  - AWS CloudTrail
  - AWS Config
NIST High-Impact on AWS
Building your own AWS Quick Start

- [https://aws-quickstart.github.io](https://aws-quickstart.github.io/)
- Advice on code design & deployment
- AMI configuration and regionalisation
- Parameterising CloudFormation
- Learn about best practices
AWS Answers
What is AWS Answers?

• Offers clear answers to common questions about architecting, building, and running applications on AWS
• Repository of instructional documents and solutions
• Outlines AWS best practices & provides prescriptive architectural guidance

• [https://aws.amazon.com/answers/](https://aws.amazon.com/answers/)
Examples of security-focussed AWS Answers

• Account security  
  • How do I ensure I set up my AWS account securely?  
  • How do I setup AWS IAM for my organisation?  
  • What are the native AWS security-logging capabilities?

• EC2 security  
  • What is the recommended EC2 baseline configuration?  
  • How do I control OS-level access to my EC2 instances?

• Application security  
  • How do I protect my applications from DDoS attacks?
Protecting web applications from DDoS attacks

- AWS provides flexible infrastructure and services that help customers implement strong DDoS mitigations and create highly available application architectures.
Centralised Logging

- Deploy a centralised logging solution using AWS CloudFormation
- Extend your logging capabilities beyond default AWS service logs.
- Control access to your dashboards
- Simplify data visualisation using built-in Amazon ES support for Kibana
AWS Blogs
What are AWS Blogs?

- New service / functionality announcements
- Best practice guidance
- Customer references and case studies
- Key blogs from a security perspective:
  - AWS Architecture: https://aws.amazon.com/blogs/architecture/

- https://aws.amazon.com/blogs/
Securing data on S3 using bucket policies

AWS Documentation

- AWS Documentation is now available in GitHub
- Accepting pull requests for content updates, errata, and code samples

https://github.com/awsdocs/
AWS Marketplace security partners
Recap

• In AWS, security is our TOP priority
• Shared Responsibility Model; security…
  • …OF the cloud: build on our security controls
  • …IN the cloud: use our extensive security features
• Use abstracted services to let you focus on applications
• Automation is your friend
• Make use of available AWS resources, docs, and examples
Key take-aways

• AWS Cloud:
  • Is the new normal, and security is still familiar
  • Improves security for nearly all customers
  • Simplifies the work of security and compliance
  • Delivers unprecedented visibility and control
  • Enables agility and speed through automation
Finally, some links to remember…

- https://aws.amazon.com/security/
- https://aws.amazon.com/compliance/
Thank you!
Upcoming events
Cybersecurity Awareness Month: Oct. 2020

DO YOUR PART.
#BECYBERSMART
Do Your Part. #BeCyberSmart

Helping to empower individuals and organizations to own their role in protecting their part of cyberspace.
Weekly themes

Oct. 1 and 2: Official NCSAM kick-off

Week of Oct. 5 (Week 1): If You Connect It, Protect It

Week of Oct. 12 (Week 2): Securing Devices at Home and Work

Week of Oct. 19 (Week 3): Securing Internet-Connected Devices in Healthcare

Week of Oct. 26 (Week 4): The Future of Connected Devices
• https://staysafeonline.org/cybersecurity-awareness-month/theme/
• https://www.dhs.gov/publication/dhs-speaker-request-form
• https://www.cisa.gov/cisa-cybersecurity-resources
IS Orientation
Sept. 30 at 1 p.m.
Presenter: Marlon Cole

Registration Link:
https://covaconf.webex.com/covaconf/onstage/g.php?MTID=e68b787865f20af9aaa799b14b366af31
COVITS 2020

VIRTUAL COVITS

September 9-10, 2020
Future ISOAG

Oct. 7, 2020

Speakers:

Randy Marchany, VT – Remote Security Threats

Dan Han, VCU – Dangers of using Teleconference & Online Classroom Training

ISOAG meets the first Wednesday of each month in 2020