Accelerating Progress With Automation

George White

FBI CJIS - CIAU

Unit Chief

2020 / VIRTUAL ISO/ACADEMY

Topics

- Progress Highlights Since June of 2018
- Automated Cloud Security Assessment (ACSA)
- Challenges
- Keys to Success
- Lessons Learned
- Q&A

Progress

- 2018 Status
  - Measured Transition
  - Secure Transport
  - Account Roles Validation
  - Security Controls Inheritance
  - Manual Security Assessments of Cloud Services
  - Lock-Down of Internet Gateways
  - NGI – early stages
  - Replicating Object Store
  - Performance Testing
  - Learning what Automation Really Means

Progress…

- 2020 Status
    - Scaled Agile Framework for Lean Enterprises (SAFe)
        - Agile Teams
            - DevOPS ->SecDevOPS
        - Transparency
        - Fail Forward
    - CI/CD Pipeline
    - Automation
        - Push-button NGI -> Push-button Everything
        - Automated Cloud Security Assessment (ACSA)

SME Quote

"With the move from on-premises physical and virtual datacenters to our cloud environment, Microsoft Azure Government in this case, we have seen a greater need for automation and continuous integration / continuous delivery (CI/CD). As we have adopted DevOps and DevSecOps practices with CI/CD automation our time to availability for a new server has dropped from weeks/months to under 10 minutes. This change in pace has required us to rethink how we do all of our processes, from change management, to security, to patching and compliance. All of our actions that constitute the delivery of a functional, secure server have required changes. We now push patches faster and with greater automation than ever before. We perform security scans as part of our baseline builds. This has impacted us, positively, in so many ways. And in the end it has helped us to drive other areas of the CJIS mission to automate and retool our thinking. Cloud has forced us to become innovators and those who can't automate or innovate are getting left behind."

Josh Staley – CJIS Division

Progress…

- 2020 Status Continued...
  - In the GOV Cloud
    - 40-50% of Windows Server Environment
    - High Percentage of Storage
    - CITRIX
    - Operating in all Gov-Cloud Regions/Locations

Progress…

- 2020 Status Continued...
  - In the GOV Cloud
    - Business Sytems in the Cloud
      - NGI – LFR, IdFP/RISC, FRS, eDO (prod)
      - NGI – MBA, EFCON, IRIS (Pre-Prod)
      - NDEX – IDOL Search Engine
      - NDEX – Novetta Entity Resolution (Pre-Prod)
      - NCIC – Proof-of-Concept (Pre-Prod)
      - UoF – Pre-Prod
      - UCR – NIBRS Portal (Prod)
      - UCR – (Pre-Prod)
      - NICS – (Pre-Prod)
      - TIPS – (Pre-Prod)
      - LEEP – (Pre-Prod)

SME Quote

"For NGI, containers and container adjacent technologies (such as Kubernetes and Gitlab pipelines in our case) are useful because they remove the debris from the road of development. This allows our developers to further abstract themselves from infrastructure and at the same time relieve system administrators from (some of) the burden of infrastructure management, freeing them up to work more towards efficiency and enhancement versus firefighting. For a specific example, Using our new infrastructure we were able to deploy the new Face Algorithm in a third of the amount of time (3-4 months versus 1 year). Using containers, kubernetes, and AWS aren't the entire reason for decrease in deployment time but there are the driving force behind it. "

Dan Rubenstein – CJIS Division

Progress…

- 2020 Status Continued...
  - In the GOV Cloud
    - Shared Services in the Cloud
      - Transit
      - Sharepoint
      - Back-Office
      - Infrastructure Security Stack
      - Security Assessment Tools
      - Logging
      - Asset Management
      - Config Management
      - Encryption
      - Authentication/Federation

Automated Cloud Security Assessment (ACSA)

- Combination of Service Evaluation and Code Development
- Overcomes massive levels of manual assessment required to bridge cloud native service gap
- Developed by CJIS (python for AWS; PS for Azure)
- Cloud Security Matrix identifies controls in play
- Repeatable
- Sustainable – with infusion of SME manpower

ACSA…

- Evaluate the Gov Cloud FEDRAMP High service to determine what FISMA controls are in play
- Determine which of the controls can be inherited
- Determine required configuration settings for controls not inherited
- Write code for automation and reporting
- Run ACSA against service to determine compliance
- Plug-in the automation to execute ACSA at spin-up

ACSA… Approved Services (AWS)

Amazon API Gateway

Amazon CloudWatch

Amazon CloudWatch Logs

Amazon CloudWatch Events

Amazon DynamoDB

Amazon Elastic Block Store (EBS)

Amazon ElastiCache

Amazon Elastic Compute Cloud (EC2)

Amazon Elastic File System (EFS)

Amazon Elasticsearch Service

Amazon Elastic MapReduce

Amazon Glacier

Amazon Kinesis Data Streams

Amazon Kinesis Data Firehose

Amazon Redshift

Amazon RDS (MariaDB)

Amazon RDS (MySQL)

Amazon RDS (Oracle)

Amazon RDS (Postgres)

Amazon RDS (SQL Server)

Amazon Simple Notification Service (SNS)

Amazon Simple Queue Service (SQS)

Amazon Simple Storage Service (S3)

Amazon Simple Workflow Service (SWF)

Amazon Virtual Private Cloud (VPC)

AWS Auto Scaling

AWS CloudFormation

AWS CloudTrail

AWS Database Migration Service

AWS Identity & Access Management (IAM)

AWS Key Management Service (KMS)

AWS Lambda

AWS Snowball

Elastic Load Balancing

ACSA… Top 10 Prioritization for AWS & Azure

Amazon Web Services

1. Amazon Aurora (Postgres & MySQL)
2. AWS Step Functions
3. Amazon Elastic Container Registry (ECR)
4. Amazon Elastic Container Service (ECS)
5. Amazon Redshift
6. Amazon Workspaces
7. AWS Secrets Manager
8. AWS Systems Manager (EC2 feature)
9. AWS Trusted Advisor
10. Amazon GuardDuty

Microsoft Azure

1. Azure Web Apps (revisit)
2. Azure Functions
3. Azure Event Hubs
4. Azure Load Balancer
5. Azure API Management
6. Azure Cognitive Search
7. Azure Container Registry
8. Azure Container Instances
9. Azure Kubernetes Service (AKS)
10. Azure Application Gateway

Security Challenges - Automation & Containers

- Automation
  - Reliance on dynamic testing using ACSA for cloud based Infrastructure as Code (IaS)
  - Still learning hot to static test IaC as we haven’t focused our efforts on developing linting tools (static code analyzer) to analyze code as it’s merged into DevOps pipelines
  - Security staff generally has limited experience with DevOps and our DevOps teams generally aren’t security aware
- Containers
  - Testing of the virtualized environment has moved to the left in most cases, but haven't yet implemented the tools to move us up the container stack or into the container stack.
    - e.g. SonaBouy, AquaSecurity, Clair and others conduct analysis “up the container stack”
  - Little knowledge of the impact of deploying plug-ins like Helm and Calico that can enhance container environments, but can also increase the risk of exploit if not configured correctly.

Input for this slide from Warren LaClair – FBI Certifying Authority

Security Challenges... success story

- CASPR (CJIS Automated Security Platform and Resources) tool
  - Automated run of all available security tools
  - Captured in common vulnerability repo (CodeDX)
    - Nessus Vulnerability Scans
    - Nessus Compliance Scans
    - OpenSCAP
    - AWS-ACSA
    - OWASP Dependency Check
    - OWASP Zap Web Scanner
    - Arachni Web Scanner
    - Fortify Static Code Analyzer
    - SonarQube Static Code Analyzer
    - Ansible Lint
    - Python Lint
  - Working to expand the capabilities of CASPR to generate Jira Issues from scan results that will land in the work back log
    - Synopsis Black duck (container scanning, dependency check)
    - Synopsis Coverity (static code analysis scanning)
    - IBM AppScan (web scanner)

Input for this slide from Jake Brozenick – Lead N3G Security Engineer

Keys to Success - Migration and Sustainment

- SecDevOps via Agile Development Teams
- Transport is King
- Automate Everything
- Centralize Account Management
- Migration Center
- Federation
- Cost Optimization
- Training

Lessons Learned

- Cloud Services Vary in Complexity – Work with partners to prioritize
- Native Services Don’t Always Fit Needs – Homegrown Solutions
- Tendency to Overestimate Compute Needs – Careful of long-term deals
- Automation and Containerization are Double-Edged – Blind Spots
- SecDevOPS Works - With Teamwork and Collaboration
- Demand for Services Outpace Ability to Assess - Consistent Prioritization

Open Q&A

George White

Unit Chief

FBI CJIS - CIAU