How Security Best Practices Enable a DevOps Security Transformation in the Cloud

Dan Wilson and Colleen Csech

Vulnerability Management and Remediation, Capital One Financial

Qualys Security Conference 2018

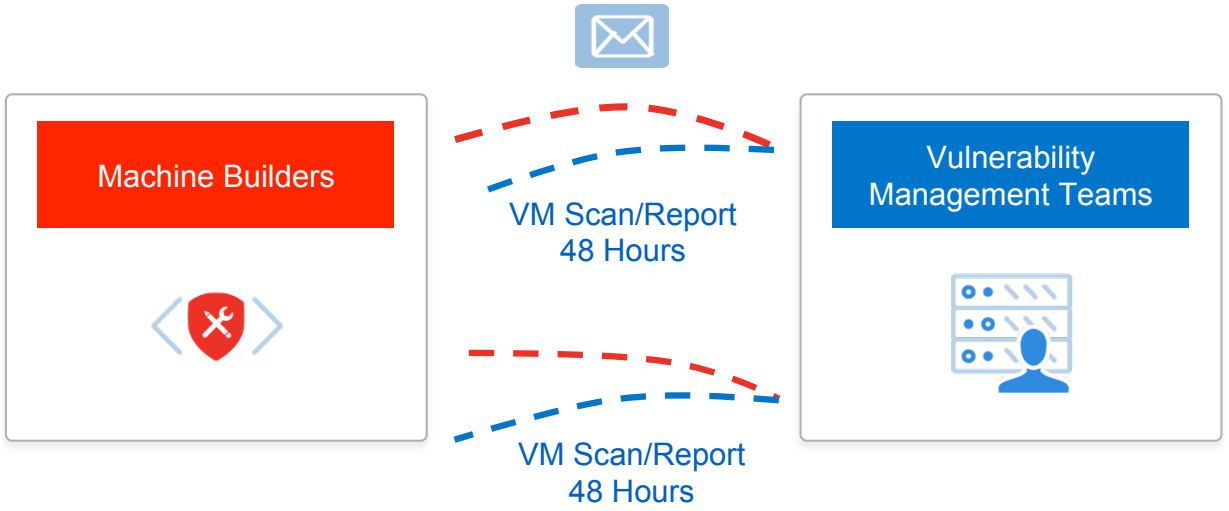
Capital One's Current Environment and Structure

- 2012 - Capital One owned and maintained 8 data centers
- Current day: 3 data centers remain and our shift to Co-locations is in full swing
- We are working to migrate Capital One infrastructure into the Cloud
- Focus: ensuring new assets spun up in the cloud are secure and free of Vulnerabilities and meeting configuration compliance requirements as defined by the CIS Benchmarks

Machine Shop: Baseline AMI Production

- Machine shop: centralized team that controls gold images that all EC2 hosts are provisioned from.
- Machine shop creates new AMIs
  - Includes both Linux and Windows flavors
  - Qualys scanner baked into AMIs
  - Removes security team from equation for DevOps
  - Automate vulnerability and compliance scans with APIs
  - Machine builders took ownership of certification process
  - Security team provides high-level oversight

Before: Lack of Security Automation Delays Release



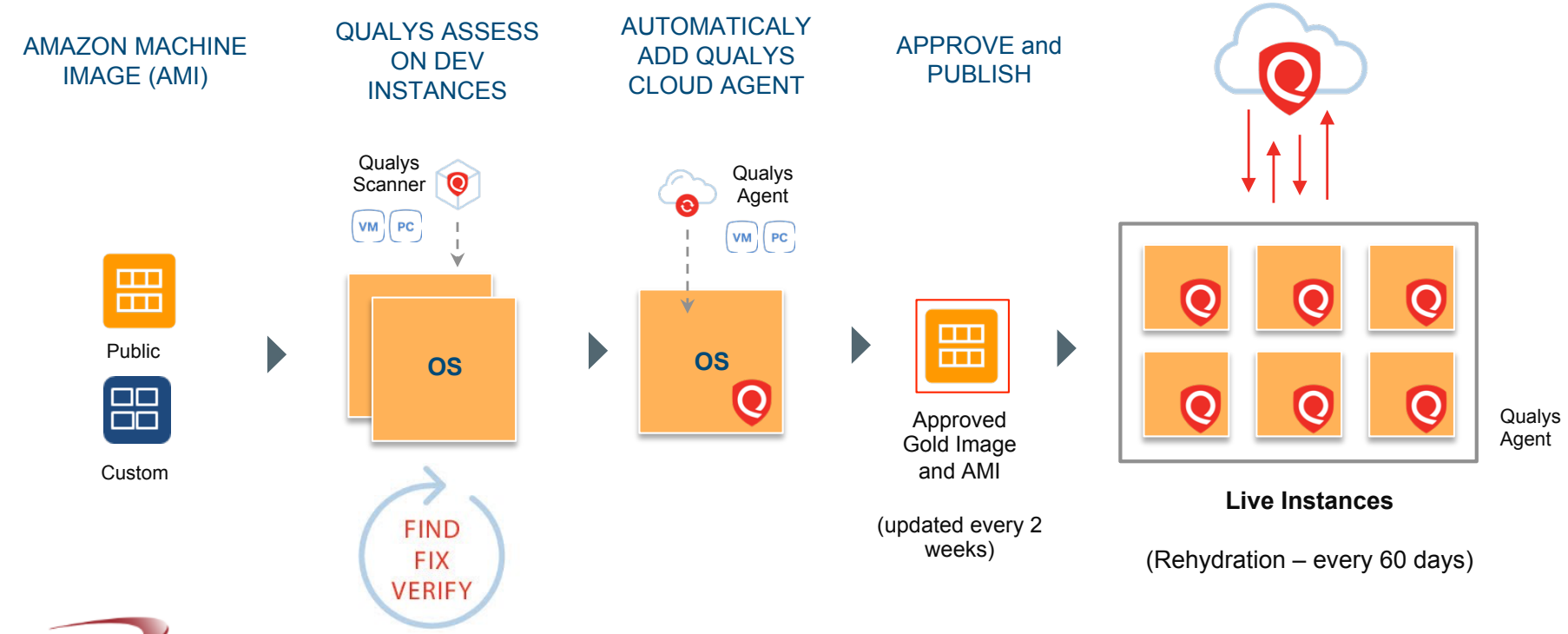
At least two weeks until the AMI is certified for production

Capital One

Qualys.

Introduce Security at the Source

Bake Qualys Security into AMIs



Movement to the Cloud and Containers in AWS

- Cyber goals: enable the business, safeguard the business, undergo data transformation
- With the migration to the cloud, Capital One has encountered unique security challenges
  - Open Source- knowing where to pull the blessed versions of software from
  - Knowing what versions of software are in the real-time instances being spun up
    - Middleware- testing and compatibility with legacy applications
    - The Qualys Agent reports out more instantaneous results on software versions and vulnerabilities in the pre-production software development process

Shifting Left:
You Build It, You Own It, You Secure It

- This movement is part of Capital One's journey towards achieving a true DevOps culture in building and maintaining software
- Developing a more proactive approach to remediation
  - Working to resolve issue in the build pipeline while applications are in development
  - Automating processes so it's as easy and consumable as possible for engineers
- DevOps teams are responsible for ensuring their application remains secure
  - Middleware patches are not included in the gold images from the Machine shop
  - Java patching is driven by the application teams
- Rehydration alone is not enough

Best Practices for Developers at Capital One

- Utilize a single-source of truth for software
  - Navigate to one centralized location to view and pull software
- Keep software current
  - Ensure teams are pulling the latest versions
- Patch using a 60 day rehydration cycle
  - In addition to AMI rehydration, make sure middleware is being patched with the latest version of software available- at a minimum every 60 days
- Leverage enterprise vulnerability scanning tools to scan your images and containers
  - Utilize the Qualys agent and Qualys self service Ad-Hoc Portal

Vulnerability Reporting at Capital One

- Leverage an external vulnerability management tool
  - Ingestion of Qualys data to tool
- Prioritization of vulnerabilities for remediation
  - Asset prioritization: aging, threat posture, regulatory compliance, environment/ attack surface
- Emphasis on education
  - Internal trainings and certification for secure software engineering

A more comprehensive vulnerability and compliance management view, enterprise wide

- Near real-time vulnerability identification
  - Helps with remediation and prioritization based on aged vulnerabilities
  - Dramatic reduction of vulnerabilities within the enterprise
- Near real-time misconfiguration detection of CIS benchmarks
- Qualys cloud agents extend coverage & provide continuous assessment
  - Asset discovery and better ServiceNow data integrity
- Continuous training for software engineers
- Seamless API integration to manage scans and reporting
- Overall cost savings

Capital One

Qualys.

Questions??