Election Cybersecurity in the Cloud
Security Automation and Orchestration for the elections process
Introduction

The US elections infrastructure faces an array of sophisticated threats designed to undermine system integrity and public trust throughout the electoral process. The increasing sophistication of cybersecurity attacks, coupled with social media misinformation campaigns and security talent shortages, makes these multi-factorial threats complex and pervasive. It is therefore crucial that all stakeholders, from executive leaders and IT directors to volunteer poll workers, work collaboratively to implement best practices that strengthen election security programmatically from every aspect. Election officials work diligently to secure systems, but like so many other areas of infrastructure, the looming threat stretches beyond any individual county or state as the effects can be rippling. Through the use of security automation and a continuous risk treatment, users can achieve strong, consistent, and resilient defenses for voting systems and ancillary supports. Amazon Web Services (AWS) offers scalable Election-as-a-Service solutions within three core pillars: Security & Compliance, Voter Engagement, and Elections Management. This white paper will explore Security Automation and Orchestration within the first pillar.

Differences Between Traditional and Cloud Computing Environments
Cloud computing differs from a traditional, on-premises environment in many ways, including flexible and scalable capacity, managed services, built-in security, options for cost optimization, and various operating models. In a traditional computing environment, you provision capacity based on an estimate of a theoretical maximum peak. This can result in periods where expensive resources are sitting idle, or occasions of insufficient capacity and poor user experience. With cloud computing, you can access as much or as little capacity as you need and dynamically scale to meet actual demand, while only paying for what you use. On AWS, servers, databases, storage, and higher-level application components can be instantiated within seconds. You can treat these as temporary resources, free from the inflexibility and constraints of a fixed and finite IT infrastructure. This resets the way you approach change management, testing, reliability, and capacity planning. This change in approach encourages experimentation by introducing the ability in processes to “fail fast” and iterate quickly.

Built-in Security
In traditional IT environments, infrastructure security auditing can be a periodic and manual process. In contrast, the AWS cloud provides governance capabilities that enable continuous monitoring of configuration changes to your IT resources. Security at AWS is the highest priority, which means that you benefit from data centers and network architecture that are built to meet the requirements of the most security-sensitive organizations. You can formalize and embed your security policy within the design of your infrastructure. With the ability to spin up temporary environments, security testing can now become part of your continuous delivery pipeline. Finally, you can leverage a variety of native AWS security and encryption features that can help you achieve higher levels of data protection and compliance.

AWS and its comprehensive partner ecosystem developed an automated security approach for securing elections in the cloud. Collaborations with partners such as Center for Internet Security (CIS), Anitian, Trend Micro, Yubico, Barracuda, Saint along with DevOPS partners GitHub and Puppet have developed a secure election environment that aligns with the principles defined by the Center for Internet Security (CIS) in the Handbook for Elections Infrastructure Security using the CIS Controls and CIS Benchmarks.
The goal is simple
Replace manual security configuration and management with automated, auditable practices to make election systems secure by default and by design.

Microservices approach to secure elections systems
There are many flavors of elections infrastructure, both from a technology and a process perspective. And this is not limited only to various types of vote capture and tabulation devices. To ensure fundamental security components are implemented in all elections systems, AWS has developed a microservices architecture security approach. This architecture is able to support multiple core election functions. AWS and our partners use secure general support systems (GSS), which follow leading security practices through the use of a microservices approach.

*Microservices architecture* is a design approach where applications use a coordinated set of small, purpose-built services. Each service runs in its own, secured environment and communicates with other services through a well-defined programmatic interface, typically a lightweight REST API. Microservices are built securely around a single business capability such that each supportive service is narrowly scoped and tightly controlled.

AWS Security Automation and Orchestration for Elections
The Security Automation and Orchestration (SAO) for Elections program uses a microservices architecture to enable a repeatable elections security architecture. This architecture constrains, tracks, and publishes continuous risk treatments (CRT) which maintains security consistently. Moreover, the environment uses DevOps practices, specifically continuous integration (CI) and continuous delivery (CD), to provide repeatable, scalable environments that adapt quickly to a diverse set of use cases and threat profiles.

AWS SAO automates simple as well as complex tasks, such as hardening systems, enforcing configuration standards, patching, and validating security policies to documented requirements. This creates a real-time risk management and assessment capability, or Continuous Risk Treatment (CRT), that seamlessly integrates with DevOps practices and tools.

How Automation works in AWS
AWS CloudFormation provisions your resources in a safe, repeatable manner. This allows you to build and rebuild your infrastructure and applications, at a moment’s notice, without having to reperform manual actions or write custom scripts that adhere to predefined security standards.
How DevOps Works
Under a DevOps model, development and operations teams unite into a common workflow. Engineers, developers, and security specialists work together through the entire application lifecycle, from development, to test, to deployment, and then production. Furthermore, the individuals on each team develop a broad, overlapping set of skills not limited to a single function.

In DevOps, quality assurance and security teams are also more tightly integrated with the application development lifecycle. When security fuses into the entire process, DevOps can become DevSecOps. Security is no longer an afterthought, applied after the application is developed or in production. Rather, security is integrated into every dimension of the environment from the start.

AWS SAO microservices architecture for securing elections
Using automation as a security force-multiplier for election systems creates a leaner, more responsive platform that is easily adaptable, without sacrificing compliance. Below is a sample of the partners and components that provide the critical foundation of the election microservices architecture across platforms.

**CIS Benchmark on AWS - AWS Foundations Benchmark**
This Quick Start implements the CIS AWS Foundations Benchmark, which is a set of security configuration best practices for hardening AWS accounts, and provides continuous monitoring capabilities for these security configurations. Reference: [AWS CIS Foundation Benchmark Quick Start](https://aws.amazon.com/quickstart/cis-foundation-benchmark/)

**Amazon Virtual Private Cloud - Modular and Scalable VPC Architecture**
This Quick Start provides a networking foundation based on AWS best practices for your Cloud infrastructure, building a virtual private network (VPC) environment with public and private subnets. Reference: [AWS VPC Quick Start](https://aws.amazon.com/quickstart/aws-vpc/)

**CIS Hardened Amazon Machine Images (AMIs)**
Hardened according to a Level 1 CIS Benchmark developed in a consensus-based process that is broadly accepted by government, business, industry, and academia. Reference: [CIS AWS Marketplace](https://aws.amazon.com/marketplace/cis-amazon-machine-images/)

**Linux Bastion Hosts Quick Start**
This Quick Start creates a new architecture with bastion host instances, or deploys the bastion hosts into an existing infrastructure. The bastion hosts provide secure access to Linux instances located in private and public subnets. Reference: [Linux Bastion Host Quick Start](https://aws.amazon.com/quickstart/aws-linux-bastion-hosts/)

**Jump box Remote Desktop Quick Start**
This Quick Start reference deployment guide includes architectural considerations and configuration steps for deploying Remote Desktop Gateway (RD Gateway) on the Amazon Web Services (AWS) Cloud. Reference: [RD Gateway Quick Start](https://aws.amazon.com/quickstart/aws-rd-gateway/)
Active Directory Domain Services on AWS – Quick Start
This Quick Start deploys Microsoft Active Directory Domain Services (AD DS) on the AWS Cloud. AD DS and Domain Name Server (DNS) are core Windows services that provide the foundation for many Microsoft-based solutions. Reference: AD DS on the AWS Quick Start

GitHub Enterprise on AWS – Quick Start
This Quick Start deploys a GitHub Enterprise on a development and collaboration platform enabling developers to build and share software easily and effectively. It provides an integrated platform for continuous integration and development, a non-linear workflow for collaboration, and in-depth monitoring and auditing for administrators. Reference: GitHub Quick Start

Puppet on AWS – Quick Start
This Quick Start automatically deploys a Puppet master and Puppet agents in the AWS cloud. Puppet is a declarative, model-based configuration management solution that helps define the state of your IT infrastructure, and automatically enforces that desired state. Reference: Puppet Quick Start

Yubico YubiKey - USB-A, Two-Factor Authentication
A multi-protocol security key providing strong two-factor, multi-factor and password-less authentication, and seamless touch-to-sign. Supports FIDO2, FIDO U2F, one-time-password (OTP), and smart card; choice of form factors for desktop or laptop. Reference: Yubico on Amazon

Deep Security on AWS – Quick Start
This Quick Start automatically deploys Trend Micro Deep Security on AWS, using its services and best practices. As a host-based security product, it provides Intrusion Detection and Prevention, Anti-Malware, Host Firewall, File and System Integrity Monitoring, and Content Filtering modules in a single agent running in the guest OS. Reference: Trend Micro – Quick Start

Anitian Sherlock Compliance Automation (SCA)
As the backbone of the automation process, SCA performs the deployment, hardening, and security of component systems and platforms. In a short time, SCA can have an entire security management and monitoring architecture running, fully aligned with a strict set of compliance standards and requirements. This platform can also be customized and scaled to meet any performance or size requirements. Reference: Sherlock.io

Anitian Sherlock Managed Detection and Response
Sherlock MDR provides 24x7 threat hunting and security monitoring from a USA-based Security Operation Center. Sherlock fuses the latest threat intelligence for elections systems with automated and manual threat hunting to spot, track, and block attacks. The high-performance Security Event and Information Management (SIEM) platform scales to any size environment, and adapts to a vast array of threats. Reference: Sherlock.io

SAINT (pre-authorized) in AWS
SAINT provides integrated vulnerability scanning, penetration testing, and vulnerability management from an easy-to-use web interface. Powerful dashboards, analytics, reporting, and asset tagging make it easy to manage your results. Reference: Saint in AWS Marketplace

The Barracuda CloudGen WAF
Barracuda WAF detects all inbound web traffic and blocks SQL injections, cross-site scripting, malware uploads, volumetric & application DDoS, or any attacks against your web applications. Reference: Barracuda CloudGen WAF for AWS
Conclusion
The Security Automation and Orchestron program creates a “Trust Boundary” that defends election systems in real-time. Moreover, officials are enabled to focus on running elections in a secure, scalable, and cost-effective way, rather than building the underlying infrastructure to support their efforts.

About AWS
With over 2,300 government agencies using AWS, we understand the requirements US government agencies have to balance: economy and agility with security, compliance and reliability. In every instance, we have been among the first to solve compliance challenges facing cloud computing and have consistently helped our customers navigate procurement and policy issues related to adoption of cloud computing.

AWS is the only cloud provider offering four U.S. cloud models to ensure that government compliance can be met using its standard, GovCloud, Secret or Top Secret regions across the full range of data classifications (unclassified, sensitive, secret and top secret). Options include regions that are highly isolated, managed by U.S. citizens on US soil, and those with FedRAMP Moderate or FedRAMP High authorization to store and process critical elections data.

AWS is a member of the U.S. Department of Homeland Security (DHS) and Election Assistance Commission’s (EAC) Election Infrastructure Subsector Coordinating Council (EI-SCC) to contribute in helping make the U.S. election systems as secure as possible.

For more information on Elections-as-a-Service, including use cases, customer testimonials, or to schedule a free onsite workshop, visit https://aws.amazon.com/stateandlocal/election-as-a-service/ or contact us at Elections2020@Amazon.com.