AUTOMATION ANYWHERE

Go be great.

BotInsight Briefing AAE V10
March 2018

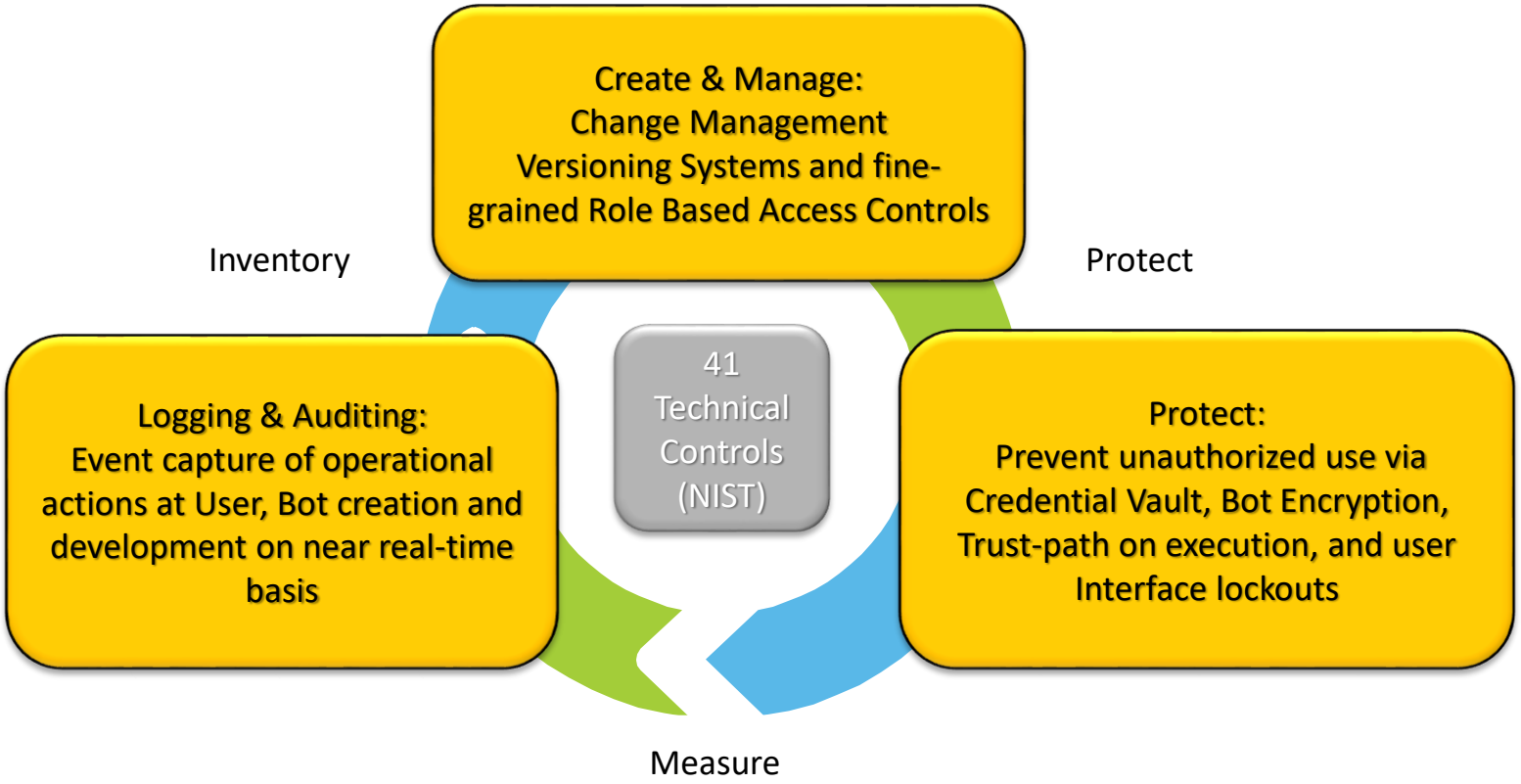
Agenda

- Security Introduction
- Secure Bot Lifecycle
- Summary of seven control areas
- Technical Control Tables

Security Introduction

- Many of the worlds most security institutions rely on our automation software for mission critical operations
- We secure bots thru the entire lifecycle from inception to production and decommissioning with over 41 technical controls
- We help you achieve compliance thru security and auditing across all 41 controls across the six areas: Inventory Control, Access Controls, Configuration Management, Change Management, Vulnerability Management and Incident Response

Industry-leading Bot Lifecycle Security



Automation Anywhere Security Architecture

- **Inventory control of all** elements (Bot, Bot Runners, Users) managed and enforced centrally thru the Control Room (CR) against approved base lines.
- Industry-leading **access controls** across all components.
  - User access is controlled via fine-grained RBAC
  - Bot files access enforced thru bot encryption
  - Bot execution controlled thru token-based Runtime authentication
  - Data secured at-rest via credential vault with support for 3rd party credential stores secured in memory with MS DPAPI
  - Security in-transit via SSL and TLS
  - Tampering at execution prevented via Stealth Mode with complete user interface disabling.
- The CR manages & logs configurations of all components, Bots are controlled via robust versioning system, for roll-back and full event logging.

Automation Anywhere Security Architecture

- **Change Management** managed & enforced via CR:
  - All components require CR authentication and license manager authorization,
  - Bot change control on execution enforced thru encryption and authentication. Tampering at execution is prevented via Stealth Mode with complete user interface disabling,
  - User changes are controlled via RBAC.
- **Vulnerability Management** based on Static, Dynamic source code Veracode analysis with OWAS ZAP and Nessus Vulnerability Assessments.
- **Incident Response** near real-time logging and auditing of Bot operational analytics.
- **Auditing** via event capture, logging and auditing on all three components with user event binding for non-repudiation.


Go be great.