# Presentation to ITAC

## Agency Vision

**Our vision is to be the information technology leader for Arizona government, providing innovative and transformative services. This won't happen overnight. And it won't happen in a vacuum. Working together toward this shared goal, we will succeed.**

## Agency Mission

**Inspired by that vision, our mission is to deliver forward-thinking and secure IT solutions to state agencies. We will achieve this by:**

- **Putting the customer first**
- **Offering world-class services**
- **Focusing on value, not cost**

## Advanced Endpoint Protection - CrowdStrike

State of Arizona – Arizona Department of Administration

September 16, 2020

# Project Introduction

On March 31, 2020, ADOA ASET approved the original project investment justification (PIJ) to procure an Advanced EndPoint Protection solution.

This solution:

- Protects systems by using machine-learning and behavioral analysis
- Keeps users endpoints (devices) safe from malicious content
- Provides visibility and blocking of malicious use of scripting tools such as Powershell, batch, bash;
- Identifies and blocks misuse of system utilities and other post-exploitation tools
- Provides near real-time alert generation

Prior to purchase, the solution was tested by more than 10 State Agencies to validate the product and functionality.  The multi-agency committee made their recommendation which was approved by the Enterprise Security Program Advisory Council (ESPAC).

The original PIJ spanned five months and had development costs of $188,946.50.

# Project Change Request for ITAC

ESPAC is working to consolidate vendors and tools where practical.  During the course of the project, the opportunity was identified to consolidate vendors and expand functionality for the Enterprise solution by including:

- End Point Detection Response,
- Managed Detection Response, and
- Threat Hunting

The additional functionality will increase the development cost from $188,946.50 to $1,328,419.54 requiring ITAC approval.

# Proposed Solution

**Procurement**

- ESPAC established Multi-Agency Committee to evaluate Advanced EndPoint Solution
- AEP Committee - Drafted Technical Requirements
- SPO
  - Sent Requirements to Vendors on State Contracts - SVAR, Networking (Security), and Cloud
  - Requested Vendors chose Manufacturers to bring in for Demos
- AEP Committee Selected 2 Manufacturers to further test in free POC
- ESPAC Approved Recommendation and Budget 8/11/20
- Received Quotes from Vendors Approved to Sell Manufacturer's Product

**Technology**

- Cloud hosted in vendor's FedRamp AWS instance
- SaaS platform
- Single agent installed on endpoints
- No infrastructure required

# Project Benefits

## Project Benefits

- Enterprise Solution - Multi-Agency, Multi-Tenant
- Increase visibility of malicious processes and indicators of compromise (IOCs) across the Enterprise
- FedRamp, vendor hosted SaaS solution
- Exponentially reduce cyber attacks
- Address the increased attacks - due to increased remote work locations
- Ability to remotely remediate threats
- Potential cost avoidance as the State will experience less data breaches
- 24/7 external monitoring to expand security operations capabilities of ADOA
- Vendor team to perform correlations and patterns of activities that could indicate malicious or insider threat behavior

# Project Responsibilities

## Agency

1. ADOA - Initial Console Config
2. Agencies (including ADOA) - Deployment to endpoints
3. Agencies (including ADOA) - Develop agency level policies based on recommendations provided by vendor and knowledge of environment
4. Agencies (including ADOA) - designate technical resources to respond to information and alerts generated

## Shared

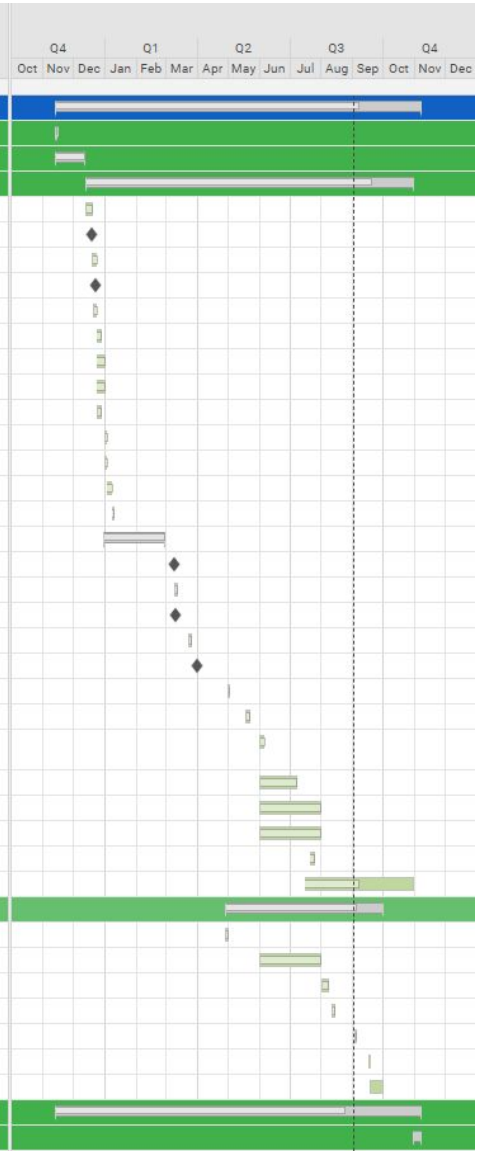
1. Training - Vendor supplied resources, Agencies must participate
2. Documentation - Vendor supplied, Agencies must read and engage
3. Updates - Vendor provided, Agencies must determine how to push to the agent

## Vendor/Contractor

1. Supports platform
2. Supports Infrastructure
3. Provide Technical resource - TAM
4. Provide Support Portal

# Project Timeline

| Task Name | Duration | Start | Finish | % Complete | Status |
|---|---|---|---|---|---|
| SCHEDULE ROLLUP LINE | 250d | 11/12/19 | 11/06/20 | 83% | In Progress |
| INITIATION | 1d | 11/12/19 | 11/12/19 | 100% | Complete |
| PLANNING | 21d | 11/12/19 | 12/11/19 | 100% | Complete |
| EXECUTION | 224d | 12/12/19 | 10/30/20 | 87% | In Progress |
| Deliverable: Preliminary Price Quotes | 6d | 12/12/19 | 12/19/19 | 100% | Complete |
| *Milestone: Select Vendors for POC* | 0 | 12/19/19 | 12/19/19 | 100% | Complete |
| *Deliverable: Procurement Vehicle for POC* | 3d | 12/19/19 | 12/23/19 | 100% | Complete |
| *Milestone: Award Vendor(s) POC* | 0 | 12/23/19 | 12/23/19 | 100% | Complete |
| *Deliverable: Draft Use Cases* | 2d | 12/20/19 | 12/23/19 | 100% | Complete |
| Gather Admin Info and Licenses | 4d | 12/23/19 | 12/27/19 | 100% | Complete |
| Gather Requirements - CrowdStrike | 6d | 12/23/19 | 12/31/19 | 100% | Complete |
| Gather Requirements - Fortinet | 6d | 12/23/19 | 12/31/19 | 100% | Complete |
| *Deliverable: SOW* | 3d | 12/24/19 | 12/27/19 | 100% | Complete |
| *Milestone: SOW Approval* | 1d | 12/31/19 | 12/31/19 | 100% | Complete |
| Enter ticket(s) for necessary changes | 1d | 12/31/19 | 12/31/19 | 100% | Complete |
| Server Config/Firewall Rules | 4d | 01/02/20 | 01/07/20 | 100% | Complete |
| Issue PO - Zero Dollar POC | 1d | 01/07/20 | 01/07/20 | 100% | Complete |
| POC | 42d | 12/30/19 | 02/28/20 | 100% | Complete |
| *Milestone: Select Product* | 0 | 03/09/20 | 03/09/20 | 100% | Complete |
| *Deliverable: Recommendation to ESPAC* | 1d | 03/09/20 | 03/09/20 | 100% | Complete |
| *Milestone: ESPAC Approved* | 0 | 03/10/20 | 03/10/20 | 100% | Complete |
| *Deliverable: Project Investment Justification* | 3d | 03/23/20 | 03/25/20 | 100% | Complete |
| *Milestone: PIJ Approved* | 0 | 04/01/20 | 04/01/20 | 100% | Complete |
| Issue PO | 1d | 04/30/20 | 04/30/20 | 100% | Complete |
| *Deliverable: Migration Communications Plan* | 5d | 05/18/20 | 05/22/20 | 100% | Complete |
| *Deliverable: Create training plan* | 5d | 06/01/20 | 06/05/20 | 100% | Complete |
| ADOA Migration | 26d | 06/01/20 | 07/07/20 | 100% | Complete |
| ADOA Managed Agencies Migration | 44d | 06/01/20 | 07/31/20 | 100% | Complete |
| Deploy to Early Adopters | 44d | 06/01/20 | 07/31/20 | 100% | Complete |
| *Milestone: CrowdStrike University Training* | 5d | 07/20/20 | 07/24/20 | 100% | Complete |
| *Milestone: Deploy to 80% of Agencies* | 76d | 07/15/20 | 10/30/20 | 50% | In Progress |
| Phase II | 109d | 04/28/20 | 09/30/20 | 83% | In Progress |
| Define Technical Requirements for EDR/MDR | 3d | 04/28/20 | 04/30/20 | 100% | Complete |
| Test Functionality of EDR/MDR | 44d | 06/01/20 | 07/31/20 | 100% | Complete |
| *Deliverable: Recommendation to ESPAC* | 6d | 08/01/20 | 08/07/20 | 100% | Complete |
| *Milestone: ESPAC Approval* | 1d | 08/11/20 | 08/11/20 | 100% | Complete |
| *Deliverable: PIJ Change Request* | 1d | 09/02/20 | 09/02/20 | 100% | Complete |
| *Milestone: ITAC Approval* | 1d | 09/16/20 | 09/16/20 | 0% | Not Started |
| Issue PO/Invoicing | 10d | 09/17/20 | 09/30/20 | 0% | Not Started |
| MONITOR & CONTROL | 250d | 11/12/19 | 11/06/20 | 79% | In Progress |
| CLOSE | 6d | 10/30/20 | 11/06/20 | 0% | Not Started |




- **Initiation:** 11/12/19 - 11/30/19
  - 100% Complete
- **Planning:** 11/12/19 - 12/11/19
  - 100% Complete
- **Execution:** 12/12/19 - 10/30/20
  - 87% In Progress
- **Phase II:** 4/28/20 - 9/30/20
  - 83% In Progress
- **Monitor and Control:** - 11/12/19 - 11/6/20
  - 80% In Progress
- **Closure:** - 10/30/20 - 11/06/20
  - 0% Not Started

# Original Project Costs

| Project Costs by Category | FY20 | FY21 | FY22 | Total |
|---|---|---|---|---|
| Professional & Outside Services (contractors) | $21,225 | $21,225 | $21,225 | $63,675 |
| Hardware | | | | |
| Software | | | | |
| Communications | | | | |
| Facilities | | | | |
| License & Maintenance Fees | $170,702.91 | $170,702.91 | $170,702.91 | $512,108.73 |
| Other Operational Expenditures | | | | |
| Total Operational | $191,927.91 | $191,927.91 | $191,927.91 | |

# Amended Project Costs

| Project Costs by Category | FY20 | FY21 | FY22 | FY23 | FY24 | Total |
|---|---|---|---|---|---|---|
| Professional & Outside Services (Contractors) | $21,225 | $115,300 | $115,300 | $115,300 | TBD | $367,125 |
| Hardware | | | | | | |
| Software | | | | | | |
| Communications | | | | | | |
| Facilities | | | | | | |
| License & Maintenance Fees | $170,702.91 | $1,021,191.63 | $1,105,667.46 | $1,105,667.46 | TBD | $3,403,229.46 |
| Other Operational Expenditures | | | | | | |
| Total Development | $191,927.91 | $1,136,491.63 | | | | $1,328,419.54 |
| Total Operational | | | $1,220,967.46 | $1,220,967.46 | | $2,441,934.92 |

# Financial Impact

| | |
|---|---|
| Actual Spend from May through June 2020 | $ 191,928 |
| Projected Spend for FY21 | $ 1,136,492 |
| Forecast (FY22) | $ 1,220,967 |
| Forecast (FY23) | $ 1,220,967 |
| Total Spend | $ 3,770,354 |

- FY20 - Purchased Initial Anti-Virus Licenses and Associated Professional Support
- FY21 - Discontinued Other Products/Contracts and Consolidating Vendor/Tools
- FY21 - Received Credit of $111,888.65 for existing Licenses and co-term all software
- FY21 - Purchase Expanded Functionality Through Software Licenses
- FY22 and FY23 - Renewal of Software Licenses

# What Success Looks Like

## Change Management

- Project Milestones
  - Communications Plan - 5/22/20 - on target
  - Training Plan - 6/5/20 - on target
  - Complete Deployment - 10/31/20*
    To coincide with contract expiration of previous tool

## Measures of Success

- 80% deployment by October 31, 2020
- 100% increase in visibility of malicious processes
- 100% increase in ability to remotely remediate malicious activities

# Requesting Approval For

Agency is requesting approval for EDR/MDR licensing purchase of the CrowdStrike Tool

- Initial licensing for next generation anti-virus was completed in FY20
- Platform is already built and configured
- Deployment in progress, to be completed by the end of October 2020
- Additional functionality is automatic with licensing purchase - no additional development actions required

# Q & A Session