Project Startup Report

Submitted to Large Project Oversight on 3/11/2020

GENERAL INFORMATION

Project Name: Palo Alto Tool Implementation

Agency Name: North Dakota Information Technology

Project Sponsor: Duane Schell

Project Manager: Jacob Chaput

PROJECT DESCRIPTION

Palo Alto Tool Implementation is a technology and core cybersecurity initiative to grow and enhance NDIT's capabilities to secure, defend and respond to cyber-attacks. The project is split across areas –

1. Build A SOC - improve cyber-attack identification, analysis, investigation, and mitigation
2. Cortex XDR - application to enhance capabilities to detect and respond to cyber-attacks by natively integrating network, endpoint and cloud data via cortex data lakes
3. Traps - an enhanced anti-malware solution that reduces endpoint risk to advanced persistent threats, zero-day attacks and blocks attack vectors malware, software vulnerabilities and bugs exploit
4. Prisma/RedLock - provides comprehensive visibility and threat protection across the State's public cloud environment(s)
5. Demisto - an automated incident response platform that will enable effective and efficient security orchestration, incident management, and interactive cyber-attack investigation.

BUSINESS NEEDS AND PROBLEMS

NDIT's current cybersecurity maturity level was rated a 1.2 out of 5.0 in 2018. In alignment with the observations and recommendations noted during that assessment and to successfully deliver on the State's new Cybersecurity Law and strategy. The project is being pursued to specifically address the following gaps:

1. NDIT's capabilities to effectively identify, analyze, investigate and efficiently mitigate cyber-attacks is limited
2. End-point protection to successfully reduce risks to advanced persistent threats, zero-day attacks and our capability to block attack vectors from malware, software vulnerabilities and bugs is not fully deployed
3. Situational awareness and visibility and threat protection across the State's public cloud environment(s) is insufficient and increases insider and external threat risks
4. The current incident response and security orchestration processes to respond to active cyber-attacks is manual, inefficient, and subject to errors
5. Our capability to successfully deliver world class security services in alignment with our "One State, One Security" approach is limited

PROJECT BASELINES

Project Start Date	Baseline Start Date	Baseline End Date	Baseline Budget
7/12/2019	7/12/2019	6/15/2020	$11,314,834.00

Notes:

- Hardware $251,404.00
- Software/Licenses $8,772,014.00
- Consulting $2,000,000.00
- Project Management $16,416

- EPMO Fee $25,000
- Risk Contingency $250,000
- Baseline Project Budget Total $11,314,834.00

OBJECTIVES

Business Objective	Measurement Description
Enhance NDIT's capabilities to effectively identify, analyze, respond, and investigate cyber attacks	Build a Security Operations Center (SOC) including Cyber Operations Center (CyOC), Modular Incident Response (ModIR), and integrations of Palo Alto tools into the SOC.
Improve end-point detection and response (EDR) protection to successfully reduce risks to sophisticated threats	Deployment of Palo Alto's Cortex XDR, Traps, and Demisto tools.
Strengthen and elevate STATE's cyber operations' people and processes	Provide workshops and trainings to build familiarity of SOCs and the Palo Alto tools they will be using. New processes and policies will be created and integrated using workshops and vendor consultants.
Improve incident response capabilities	Creation of incident scenario playbooks and workflow automation using industry best practices and Palo Alto tools.

KEY CONSTRAINTS AND/OR RISKS

Constraints

- The current Security Incident and Event Management (SIEM) is limited in its capabilities to serve as the sole source for all alerts and threat information
- Traps agents have not been fully deployed to all endpoints and will impact the level of situational awareness of threats, visibility of cyber-attacks and end-point protection
- Deployment of Cortex XDR could be limited and dependent upon the Tenants' acceptance and resources (financial and human) to complete implementation (e.g., NDUS, K12)
- Prisma Cloud is constrained to State Public Cloud environments only, no other cloud environments are in scope

Risk	Impact	Response
Resource shortages and constraints.	Lack of resource availability for this project could impact timelines and project costs.	Well-defined resource forecasting; agreement of necessary resources from management.
Impacts to operational tasks and activities.	Operational areas may see disruptions to everyday activities as new tools are implemented.	Utilizing a well-versed vendor in the planning and implementation process to reduce potential negative impacts.