2022 Grant Proposal For Managed Security Information And Event Management System

for the

FY 2022 State and Local Cybersecurity Grant Program (SLCGP)

Government Entity: City of North Port
Primary Contact Name: Rosalie Sanders
Title: Security Administrator
Mailing Address: 4970 City Hall Boulevard
North Port, FL 34286
Phone Number: 941-429-7239
Email: rsanders@northportfl.gov

Secondary Contact Name: Vicki Edwards
Title: Senior Business Administrator
Phone Number: 941-429-7141
Email: vedwards@northportfl.gov

RAPID7 MANAGED DETECTION AND RESPONSE SIEM TOOL

1. Project Title

Rapid7 Managed Detection and Response Security Information Event Management (SIEM) Tool

The City of North Port Information Technology Division desires to purchase a SIEM Tool to be deployed within the City's network environment to improve cyber security and increase resilience against cyber risks. The total cost to purchase Rapid7's Managed Detection and Response (MDR) SIEM service is $90,000 for the first year. The City of North Port is respectfully requesting $81,000 from the FY 2022 State and Local Cybersecurity Grant Program (SLCGP) and will provide a 10% match of $9,000.

2. Project Summary

The City of North Port's Information Technology Division has researched SIEM Tool Solutions to strengthen cybersecurity practices and resilience. The IT Division wishes to purchase Rapid7's Managed Detection and Response Services, which includes a SIEM platform and 24/7/365 monitoring services. After implementing the SIEM platform within the City's network environment, it would become a yearly subscription for the managed services.

The SIEM platform from Rapid7 provides several key benefits as part of a mature cybersecurity strategy for the enterprise. InsightIDR managed service monitors network activity in the enterprise and creates a baseline on what is considered normal user behavior and attributes activity back to user accounts. The creation of network activity baselines and user attribution is processed by a cloud-hosted AI (artificial intelligence) engine that can cut through the noise of millions of event logs, providing discreet and actionable alert notifications to the City of North Port's IT security team. These notifications allow the IT security team to take a proactive approach in cybersecurity incident response and mitigation.

The deployment of the Rapid7 InsightIDR managed SIEM platform will significantly improve the City of North Port Government's cybersecurity posture while empowering its IT security team to play a proactive role in monitoring network activity.

a. SIEM

Security Information and Event Manager (SIEM) technology is used to collect, analyze, and report security related data used to find, understand, and react to security related threats. SIEM can be used as a software only product, hardware appliance, or cloud service. Additionally, the SIEM will serve as a system of record (SOR) that will provide forensic log data that can be used for root cause analysis (RCA) in the case of a cyber event. A SIEM is critical for the mature cybersecurity practice as it will speed along investigations and remediation processes in the case of an incident.

b. Managed Detection & Response

Rapid7's Managed Detection and Response (MDR) service will extend the City’s security operations team to achieve 24x7 threat detection and response without hiring additional headcount. Rapid7’s world-class experts manage the burden of threat monitoring, detection, and how to respond so that the City can improve its cyber resilience and focus on what matters most. This collaborative partnership — backed by the industry Incident Response experts and leading technology, InsightIDR — enhances our cyber security decision making to continuously improve our resilience and stop malicious activity across your expanding modern environment: endpoints, network, users, and cloud.

PROJECT STATEMENT AND ANALYSIS

1. Project Statement and Analysis

With the increase of cyber security related incidents, the City of North Port wants to become proactive in mitigating such risks of an incident occurring. With the purchase and implementation of a managed SIEM service, the City of North Port will gain extra hands-on cyber security surveillance by partnering with Rapid7.

With the purchase of Rapid7’s MDR SIEM, City of North Port’s Information Technology Division will install monitoring agents on the City’s endpoints (workstations and servers) via a graphic user interface (GUI) dashboard and collect event sources from the City’s network (including Firewalls, Syslog Servers, LDAP, Active Directory, and Microsoft 365). The event sources will populate the GUI dashboard with traffic logs, user behavior analytics to establish normal patterns for user authentications, user activities, and use advanced behavior rules to identify malicious activity across all event sources.

Key benefits include:

- **Threat Intelligence** – Identifying and investigating known threats in our environment that may lead to a breach.
- **User Behavior Analytics** – Establishing normal patterns for user authentications in our environment and alerting on deviations.
- **Attacker Behavior Analytics** – Using advanced behavior rules to identify attacker activity across event sources.
- **Data Analytics** – Collecting and analyzing security data via InsightIDR to devise new methods of identifying breaches.
- **Improve resilience** - Go on the offense with threat intelligence. Offload full incident detection, validation, and response to our team of experts; save time by partnering with a vendor that provides actionable insights and reporting based on 20+ years of experience. Achieve full coverage across the modern

environment leveraging advanced behavioral analytics (UBA, ABA) and XDR capabilities to identify malicious activity.

- **Scale SecOps with Experts** - Get 24x7 coverage with follow-the-sun operations and investigate incidents at scale and access experts when we need them. Rapid7's team will provide prescriptive guidance and accelerate our MTTR with a collaborative approach to ensure we're able to strategically strengthen our security posture.

2. Project Description

a. **Target Population:** City of North Port employees
b. **Parties responsible for implementing the project:** City of North Port's Information Technology Division
c. Partners involved: Rapid7

The project will take place in North Port FL, and will be implemented by the Information Technology Division, managed by the IT Security Administrator.

The City of North Port's Information Technology Division has chosen this project to include additional security measures, and to become proactive in the case of an incident. Rapid7's managed SIEM tool will increase security response time for the City in the event of an incident or attack. It will allow the City's network environment to be monitored 24/7/365 and have a hands-on team of security analysts to manage and mitigate cyber risks.

3. Challenges

There are no expected challenges during the integration of the SIEM tool, as the City's IT will be using all existing IT infrastructures and equipment to complete the project.

4. Project Milestones

- Submit Grant Proposal Application: **Nov. 1, 2022**
- Projected Period of Performance Start Date: Purchase Rapid7's SIEM tool: **Beginning of 2023 (January-March)/After grant is awarded.**
- Up to 8 hours of implementation guidance with Rapid7 engineers' team: **After initial purchase of the tool.**
- City of North Port's Security Administrator does a 2-Day training: **After the implementation guidance is complete.**
- Rapid7's MDR SIEM will continuously scan the City of North Port's network environment to learn users' authentication and activities (normal behavior): **The first 30 days following the endpoints' agent's installation.**
- Projected Period of Performance End Date: **First Year ends Beginning of 2024 (January-March).**

GOALS, OBJECTIVES AND OUTCOMES

1. **Goal:** The implementation of a managed SIEM tool within the City of North Port's network environment will provide increased security protections commensurate with risks by enhancing a cybersecurity plan and responding to cyber security incidents while ensuring continuity of operations.

2. **Overall Project Categories**

   a. **Planning:** Purchase of Rapid7's SIEM, installation on endpoints, staff training, full integration of SIEM tool in environment.

   b. **Organization:** Enhanced 24/7/365 cyber security for the City of North Port.

   c. **Training:** Rapid7 provides a 2-Day training for the Information Technology Security Administrator with the purchase of their managed SIEM tool.

   d. **Equipment:** Full platform management of the cloud based SIEM solution includes:

   • Integration of all applicable data sources for Windows/syslog-based data sources.

   • Ensure ingestion of appropriate Security Events

   • Integration of applicable API integrations where applicable.

   • Installation, building, setup, tuning, and operation RFP for Palo Alto Border Firewalls 3

   • Security architecture workshop – Initial and periodic.

   ▪ SIEM Tuning & Baselining

   • Setup basic, pre-packaged SIEM alerts for the environment.

   • Setup custom alerts applicable to the environment.

   • Adjust rules and thresholds as applicable to the environment.

3. **Objectives:**
   Objective 1: Within 90-120 days of being awarded the funds, the purchase of Rapid7's SIEM tool will be 100% complete.
   Objective 2: Within 30 days post purchase, user training and additional cross-training for Rapid7's SIEM tool will be 100% complete.
   Objective 3: Within 30 days post user training, the installation of the SIEM tool on endpoints will be 100% complete.
   Objective 4: Within 30 days post installation on endpoints, Rapid7's SIEM tool normal user behavior learning will be 100% complete.

Objective 5: Within 60 days post learning normal user behavior, the SIEM tool will be 100% integrated within the network environment.

4. **Outcome:** With a managed SIEM tool in place within the City of North Port's network environment, cyber resilience will increase to mitigate all future security risks. The managed SIEM will provide the City with a team of professional experts to assist in monitoring the City's network activities 24/7/365.

PROJECT SCOPE

1. Capabilities Building:
   a. Building a 24/7/365 cyber security environment for the City of North Port.

BUDGET

The total cost of the project, with 10% contingency is $90,000. The City of North Port is requesting $81,000 from the FY 2022 State and Local Cybersecurity Grant Program (SLCGP). The City will provide a match of 10% ($9,000).

The implementation of the SIEM tool services will be completed in one phase. Below are the individual components of the Rapid7 product that will need to be purchased:

Product	Quantity	Cost	Total Cost
InsightIDR Certified Specialist Training 2-Day Training Class (one-time cost)	1	$2,451	$2,451
InsightIDR Quick Start Up to 8 Hours of Implementation Services (one-time cost)	1	$3,087	$3,087
Managed Detection and Response Services (12 months service)	600	$140.77	$84,462
Total Project Cost			**$90,000**
City of North Port 10% match			-$9,000
Total Fund Request			**$81,000**