Managed Endpoint Detection & Response Services

**Paolo Penaflor, Dallas Nuedorf, Logan Johnston**

**City of New Westminster**

**January 26, 2024**

**NWRFP-23-16**

**CyberQuack LLC**

**COMM2130**

**James Phillips**

Table of Contents

[Introduction 1](#_Toc157201091)

[Next-Generation EDR Implementation 1](#_Toc157201092)

[Transitioning To Zero Trust Architecture 1](#_Toc157201093)

[Hunting For Threats Before Threat Actors 2](#_Toc157201094)

[Project Details 2](#_Toc157201095)

[Outline Security Posture & Assessing Threat Categories 2](#_Toc157201096)

[Implementing EDR/MDR Solution 2](#_Toc157201097)

[Offensive Security Measures To Enhance Network Defense 2](#_Toc157201098)

[Defining Next-Generation EDR Technology & Proactive Maintenance 3](#_Toc157201099)

[EDR Implementation Project Members 3](#_Toc157201100)

[Penetration Testing & Security Assessment Team (Red Team) 3](#_Toc157201101)

[Reporting Strategies 4](#_Toc157201102)

[References: 5](#_Toc157201103)

# Introduction

This proposal outlines Cyberquack’s plan to introduce a Managed Detection Response (MDR) solution for the ongoing monitoring, threat hunting, and incident response services required by the City of New Westminster's cyber security program. This plan includes the use of a next-generation Endpoint Detection & Response (EDR) platform, paired with a proactive approach to vulnerability testing, incident response, and regularly available reports.

## Next-Generation EDR Implementation

The City's systems, devices, and cloud solutions are under threat from the continually evolving cyber landscape. With the average time-to-detect (TTD) a threat lasting around 277 days, an effective EDR solution is imperative to mitigating the risk to the City of New Westminster. A major issue that faces any organization implementing an EDR solution is the manpower to design, deploy, test, and maintain the security apparatus. Our firm has extensive experience, particularly in municipal applications, of building mature and thorough threat detection and response models that have proven themselves against modern threat actors. By investing in our managed EDR solution, resources, and staff fatigue traditionally experienced by in-house security teams are reduced and City employees can focus on the exceptional roles they already play in our society. Using the next-generation of the Crowdstrike EDR platform, threats are assessed by a vigorous AI model trained to detect and prevent malicious and zero-day exploits as they happen.

## Transitioning To Zero Trust Architecture

Traditional IT security evolved from the idea of a castle behind a moat. Getting inside the castle can be extremely difficult, but once inside a person is implicitly trusted. From a security point of view, this is a dangerous route for networks such as the City of New Westminster's due to the fact that should a threat-actor compromise a City's endpoint device, they have crossed the moat. Once implicitly trusted, the threat-actor can move through the network and establish themselves as an Advanced Persistent Threat (APT). This issue becomes even greater when cloud networks are considered. The solution is a shift in thinking. By assuming a zero-trust model where threats are considered to already be in the castle, principles such as least privilege, microsegmentation, and multi-factor authentication can be evaluated against current standards to produce a security model that continuously works to verify identity and privilege on the network, both inside and outside the castle.

## Hunting For Threats Before Threat Actors

With our proposed defensive MDR solution, there is another half of the coin. By proactively hunting threats through vulnerability testing, our firm will provide meaningful action items that will further strengthen the security of the City's infrastructure. After briefing with City-assigned security professionals, our firm can provide vulnerability testing and reporting services that follow the British Columbian Information Management / Information Technology (BC-IM/IT) specifications. Regular reporting on a weekly schedule is standard as well as access to functional dashboards that can provide real-time alerts and notifications to City IT professionals. Incident response strategies that leverage the reach and depth of the EDR solution will be developed alongside City security professionals, combining the split-second decision making of AI automation with human-powered review of critical alerts.

# Project Details

The first order of business is to meet with City officials and debrief on the current security posture of the organization. This will clearly define the scope of our EDR solution. During this we will gather any existing documentation available and create topology maps to fully understand the overall network structure. We will also collaborate with key personnel to define which assets and components will need to be included.

## Outline Security Posture & Assessing Threat Categories

Once City officials have outlined their posture, the system will be assessed via vulnerability scanning to establish what vulnerabilities can be mitigated with the EDR solution and what vulnerabilities need to be addressed outside the EDR solution.

Once these vulnerabilities have been categorized, the EDR solution will be implemented alongside an employee training program that educates end-device users on the role they play securing the networks that they use. Vulnerabilities not resolved with the EDR solution will be addressed to City officials to clarify responsibilities and scope in order to further strengthen the security posture of the City.

## Implementing EDR/MDR Solution

After implementation, the EDR solution will develop its managed service by first developing the baseline of normal network behavior for end-devices, systems, and cloud applications. Telemetry from this data will be bundled into a dashboard that will leverage security platforms already in place in City infrastructure, creating a real-time analytics dashboard that can be accessed by City security officials and planners.

## Offensive Security Measures To Enhance Network Defense

Once all known vulnerabilities in the system architecture have been addressed and resolved via EDR or City security officials, our firm will begin focusing on developing a periodic penetration testing framework. Cyberquack’s in-house Red Team specializes in offensive security testing enterprise-level networks and have a multitude of purpose-built tools that will continue to test the attack surface of the City of New Westminster’s IT networks. With regular meetings and reporting, this value-added service has the potential to stop threat actors and inform decision makers of priority concerns.

## Defining Next-Generation EDR Technology & Proactive Security

Using Crowdstrike’s latest EDR innovation, the City of New Westminster can rest assured their networks have a guardian angel always watching over them. Crowdstrike’s Cyber Threat Intelligence Integration powers the EDR with real-time updates on modern tactics, techniques, and procedures (TTPs), and can identify the stealthiest of attackers. This next-generation EDR creates something like a TV’s DVR on every network endpoint. Using the Falcon platform, this recorded intelligence can be accessed from and calculated in the cloud, allowing ultimate visibility from anywhere in the world.

To complement the EDR solution, a management team of highly skilled network engineers, security analysts, and system administrators take security to the next level. Through our highly skilled management team, the EDR solution becomes an MDR solution that not only detects, but proactively hunts, investigates, and responds to emerging or advanced threats. Our in-house security team will work closely with our Red Team pentesters to develop a threat database based on behavior, EDR artificial intelligence (AI) insights, and cutting-edge industry insider knowledge.

## EDR Implementation Project Members

Developing this project will require two teams of highly qualified security specialists. The first team will deal with EDR implementation and development:

**Michael Rodriguez (Incident Response Manager – Lead)** *– 10+ years managing defensive and offensive security teams. GCIH, CISM, CCSP*

**Samantha Lee (EDR Specialist)** *– 7+ years’ experience in EDR development for municipal governments. CISSP, CompTIA Security+, Certified Endpoint Security Specialist*

**Rachel Green (Technical Analyst)** *– 4 years’ experience assessing vulnerabilities in a Tier 2 position for enterprise. 2 years’ experience Tier 3 SOC analyst. Certified Vulnerability Assessor (CVA), CompTIA Sec+, Net+, CCNA*

**Daniel Kim (Technical Analyst)** *– 3 years’ experience as Tier 1 security operations center (SOC) analyst. CompTIA Sec+, Net+, Pentest+*

## Penetration Testing & Security Assessment Team (Red Team)

For the continued vulnerability and penetration testing service, our Red Team includes:

**Isabella Martinez (Certified Ethical Hacker – Lead)** – *5 years’ experience as a network security manager for Fortune 500s, 12 years’ experience in offensive penetration testing with a focus on government and non-profit organizations. CCNP, CCSP, CISSP, CEH*

**Olivia Wilde (Compliance and Risk Manager)** *– 10 years’ experience mitigating risks and ensuring compliance with ISO27001:2002 in the context of government infrastructure. Certified Risk and Information Systems Control (CRISC), Certified Compliance & Ethics Professional (CCEP)*

**Lucas Brown (Security Engineer)** *– 5 years’ experience as a network security engineer. CCNA, CCNP, CompTIA Sec+, Net+, Pentest+*

**David Smith (Security Engineer)** – *6 years’ experience in offensive penetration testing with a focus on banking and Fortune 500 contexts. Offensive Security Certified Professional (OSCP), CCNA, CCNP, CompTIA Sec+, Net+, & Pentest+*

## Reporting Strategies

We will provide regular status reports and updates on the progress of the MDR solution that will include key milestones achieved and tasks that have been completed. We will also define and track key performance indicators from the Crowdstrike EDR platform, Falcon Cloud Integration, and existing City infrastructure.

These reports will be bundled into a weekly status update which outlines the tasks, threats, and solutions discovered. The data from these reports can also be accessed in real-time via a custom online dashboard developed by Cyberquack.

The main Key Performance Indicators (KPI) assessed in these reports include, but are not limited to:

* + Number of security incidents detected and resolved
  + Average Time to detect and respond to any incidents
  + System uptime and availability
  + Unidentified end-devices visible on the network
  + IoT devices visible on the network
  + Risk Assessment as per our in-house Compliance and Risk Management

Our Red Team will provide additional documentation after completing regular vulnerability scans and penetration tests on City network infrastructure. This documentation will be used to supplement the MDR solution to better suit the unique requirements of municipal IT networks.

# References:

* S. W. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” *www.nist.gov*, Aug. 2020, Available: https://www.nist.gov/publications/zero-trust-architecture
* CrowdStrike, “What is Managed Detection and Response (MDR)? | CrowdStrike,” *crowdstrike.com*, Feb. 15, 2022. https://www.crowdstrike.com/cybersecurity-101/managed-detection-and-response-mdr/
* ISO, “ISO/IEC 27001 standard – information security management systems,” *ISO*, Oct. 2022. https://www.iso.org/standard/27001
* “British Columbia Data Administration Standards,” *gov.bc*, Feb. 12, 1998. https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/data\_administration\_standards.pdf (accessed Jan. 26, 2024).
* D. Benson, “CrowdStrike Falcon® Insight XDR | Products,” *crowdstrike.com*, Dec. 12, 2023. https://www.crowdstrike.com/products/endpoint-security/falcon-insight-xdr/