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](#_Toc157352310)

[Next-Generation EDR Implementation 1](#_Toc157352311)

[Transitioning To Zero Trust Architecture 1](#_Toc157352312)

[Traditional security paradigms, akin to a castle behind a moat, are inadequate for modern threats. The solution is a shift in thinking. Adopting a zero-trust model is imperative for the City of New Westminster, focusing on principles like least privilege, microsegmentation, and multi-factor authentication to continuously verify identity and privilege on the network, both internally and externally. 1](#_Toc157352313)

[Hunting For Threats Before Threat Actors 1](#_Toc157352314)

[Project Details 2](#_Toc157352315)

[Outlining Security Posture & Assessing Threat Categories 2](#_Toc157352316)

[Implementing EDR/MDR Solution 2](#_Toc157352317)

[Offensive Security Measures to Enhance Network Defense 2](#_Toc157352318)

[Defining Next-Generation EDR Technology & Proactive Security 2](#_Toc157352319)

[Project Team Breakdown 3](#_Toc157352320)

[EDR Implementation Project Members 3](#_Toc157352321)

[Penetration Testing & Security Assessment Team (Red Team) 3](#_Toc157352322)

[References: 4](#_Toc157352323)

# 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.

## Transitioning To Zero Trust Architecture

## Traditional security paradigms, akin to a castle behind a moat, are inadequate for modern threats. The solution is a shift in thinking. Adopting a zero-trust model is imperative for the City of New Westminster, focusing on principles like least privilege, microsegmentation, and multi-factor authentication to continuously verify identity and privilege on the network, both internally and externally.

## Hunting For Threats Before Threat Actors

With our proposed defensive MDR solution, proactive threat hunting through vulnerability testing will provide meaningful action items that will further strengthen the security of the City's infrastructure. Functional dashboards allow city officials to witness threats as they are discovered, offering the ability to see the attacker before they see you.

Regular reporting on a weekly schedule real-time alerts that follow BC-IM/IT and other industry standards work to ensure continuous monitoring strategies that leverage the reach and depth of the EDR solution. Incident response strategies, combining AI automation with human oversight, are tailored in collaboration with City security professionals.

# 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.

## Outlining 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

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 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, forwarding reports to those that need to know.

## Project Team Breakdown

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.

## 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+*

# 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/