February 6, 2024

CyberQuack Security Solutions

Vancouver, British Columbia

78 East Broadway – V5T 1V6 CyberQuack Security Solutions

Dear City of New Westminster,

We have attached our proposal for providing a Managed Endpoint Detection & Response (MDR) service, including proactive threat-hunting and reporting facilities, as requested in the request for proposal sought by the City of New West. CyberQuack Security Solutions, excited to demonstrate our decades-long experience securing and maintaining government institutions, follows the RFx Process and General Requirements outlined in the City documentation.

The proposed MDR solution has been divided into 4 phases set to occur over a 6-month period, not including contingencies. The cost of this solution has been projected to be $242,046; a breakdown and analysis of costs can be found in the Budget Section of the proposal.

To implement the proposal effectively, two teams with extensive experience in their respective fields will be required. One team is tasked with developing and maintaining the MDR solution, and another team is dedicated to proactive threat-hunting. Details of team-member qualifications have been included in the attached proposal.

Further information regarding the schedule of the project, budget considerations, contingency plans, and specific implementation strategies can also be found within the attached proposal. If you have any questions about the material in this proposal, please contact our office at (604)-123-4567. Feel free to contact the Project Manager Derek Jeeter directly by email at derek.jeeter@cyberq.com or by phone at (604)-555-4545.

Thank you for your consideration, we look forward to hearing from you.

A black and white image of a person's face

Description automatically generated

CyberQuack Security Solutions

Derek Jeeter, Project Manager

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**

# Executive Summary

The City of New Westminster has been experiencing a transition. A transition towards increased responsibility as its citizens embrace the convenience of reliable City infrastructure.

As the population continues to grow, so does the value of this reliable infrastructure, and with it grows the threat of disruption and destruction. Our cybersecurity firm has conducted analysis showing over 90% of today’s municipal networks can be accessed without consent.

This alarming statistic stems from an idea that Cyberquack has seen countless times in local government applications – today’s problems can be solved with yesterday’s technology.

The fact is that yesterday’s technology has become today’s problem.

Cyberquack’s solution is a comprehensive security apparatus designed to protect the City against the most commonly seen attacks to date. Endpoint device security (EDR) can be hardened using industry-leading software, managed by the decades of combined experience found at Cyberquack.

In conjunction with the EDR solution, our firm will enhance the security posture of the City of New Westminster through vigorous vulnerability analysis and penetration testing. This technique has a proven history of finding the not-so-common attack avenues used by threat actors in modern contexts that traditional services will fail to recognize.

The development of this project will require 4 months solution, with an additional two months designated for testing and optimization of the security apparatus.

The City of New West is invited to continue using the services of Cyberquack on a contingency basis following the completion of the project.

The overall cost of the project is estimated to be $242,046, although much of this cost is dependent on the current security assets in the City’s inventory. If the City already has the required hardware to support the EDR solution, the cost of the project is estimated at $102,046, not including contingency costs.

Table of Contents

[Introduction 1](#_Toc159338039)

[Next-Generation EDR Implementation 1](#_Toc159338040)

[Transitioning To Zero Trust Architecture 1](#_Toc159338041)

[Hunting For Threats Before Threat Actors 1](#_Toc159338042)

[Schedule 2](#_Toc159338043)

[Project Details 3](#_Toc159338044)

[Outlining Security Posture & Assessing Threat Categories 3](#_Toc159338045)

[Implementing EDR/MDR Solution 3](#_Toc159338046)

[Offensive Security Measures to Enhance Network Defense 3](#_Toc159338047)

[Defining Next-Generation EDR Technology & Proactive Security 3](#_Toc159338048)

[Budget 4](#_Toc159338049)

[Phase 1: Security Posture Assessment and Strategy Development 4](#_Toc159338050)

[Phase 2: EDR Initial Setup and Development 4](#_Toc159338051)

[Phase 3: EDR Deployment and Optimization 5](#_Toc159338052)

[Phase 4: Continuous Improvement and Closure 5](#_Toc159338053)

[Budget Breakdown 6](#_Toc159338054)

[Project Team Breakdown 7](#_Toc159338055)

[EDR Implementation Project Members 7](#_Toc159338056)

[Penetration Testing & Security Assessment Team (Red Team) 7](#_Toc159338057)

[Conclusion 8](#_Toc159338058)

[Recommendations 8](#_Toc159338059)

[References: 9](#_Toc159338060)

# 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[1], 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[2].

## 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[3][4]. Incident response strategies, combining AI automation with human oversight, are tailored in collaboration with City security professionals.

|  |  |  |  |
| --- | --- | --- | --- |
| Phase |  | Weeks |  |
|  |  | **1-2** | **Project Kickoff and Initial Assessment**   * Assemble project team * Initial security posture assessment |
| **1** |  | **3-4** | **Planning and Strategy Development**   * Define zero-trust architecture transition plan * Develop threat hunting and incident response protocols |
|  |  | **5-6** | **Tool Selection and Procurement**   * Select and procure Crowdstrike’s EDR technology * Begin vulnerability scanning |
|  |  | **7-10** | **Infrastructure Setup and EDR Implementation**   * Set up servers and network infrastructure * Initial EDR system implementation and configuration |
| **2** |  | **11-14** | **EDR Development and Testing**   * Develop custom EDR components * Begin continuous vulnerability testing with red team |
|  |  | **15-18** | **Deployment and Staff Training**   * Deploy EDR solution across the network * Conduct staff training sessions on the new system |
|  |  | **19-22** | **Optimization and Fine-Tuning**   * Optimize EDR configurations based on red team feedback * Fine-tune threat hunting and incident response procedures |
| **3** |  | **23-26** | **Monitoring and Continuous Improvement**   * Initiate continuous monitoring phase * Regularly review and update the security measures |
|  |  | **27-28** | **Project Review and Closure**   * Conduct final project review * Document lessons learned |

# 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[5] 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[2].

# Budget

## Phase 1: Security Posture Assessment and Strategy Development

During the Security Posture Assessment, an updated inventory of IT assets will be made with the cooperation of City staff. It also involves mapping out the attack surface of a city. With CyberQuack’s in-house scanning and assessment tools, this assessment will only consist of Personnel costs. Our EDR Specialist and Compliance and Security Manager will use information from these assessments to develop a thorough plan for the EDR implementation whilst making sure to follow security standards laid out in the Security Framework.

**Estimated Cost: $240,000+**

Posture Assessment

Lead Ethical Hacker - $6000 for 2 weeks

Security Engineer - $4000 for 2 weeks

Security Engineer - $2000 for 1 week

Technical Analyst - $2000 for 1 week

Strategy Development

EDR Specialist - $6000 for 2 weeks

Compliance Manager - $5000 for 2 weeks

## Phase 2: EDR Initial Setup and Development

CyberQuack’s partnership with Crowdstrike allows us to offer their Latest EDR innovation. During Phase 2, equipment including additional endpoints, servers, and network infrastructure needs to be set up. Most of the cost accumulated during this phase will be dependent on the scope determined in Phase 1.

As a pre-caution for unpredictable consequences, a contingency fund is proposed only for the most damage prone and sensitive equipment. The servers to be installed also require additional software that ensure high availability throughout the system.

**Estimated Cost: $160,000+**

EDR Initial Setup  
Incident Response Manager - $12000 for 5 weeks  
EDR Specialist - $10000 for 3 weeks  
Technical Analyst - $8000 for 4 weeks  
Technical Analyst - $6000 for 3 weeks

Vulnerability Testing  
Compliance & Risk Manager - $5000 for 2 weeks  
Security Engineer - $4000 for 2 weeks

City-wide Network Infrastructure  
Equipment Estimate - $120000+ (Depending on inventory of assets)  
Contingency Fund - $20000

Software Licensing  
Crowdstrike EDR - $924.95 annually  
Server Software - $3799

## Phase 3: EDR Deployment and Optimization

During Phase 3, The EDR Solution will be fully deployed with a central management console for easy monitoring. We will also be conducting training sessions for local City staff. After deployment has been finished, our pentesting team will work together with the deployment team to optimize and fine tune the EDR configuration.

**Estimated Cost: $21,099**

Deployment and Training

Incident Response Manager - $5000 for 2 weeks  
EDR Specialist - $4000 for 2 weeks  
Technical Analyst - $3000 for 2 weeks  
Technical Analyst - $1500 for 1 week

Pentesting and Optimization

Lead Ethical Hacker - $3000 for 1 week

Security Engineer - $2000 for 1 week

Software

Central Management Console (CMC) - $1099

## Phase 4: Continuous Improvement and Closure

During the last phase of the project, continuous monitoring will be provided with regular assessments to improve the system. Costs will consist of maintenance and upkeep for these services.

**Estimated Cost: $2223**

Continuous Maintenance -$1299 annually

Crowdstrike Licensing -$924.95 annually

## Budget Breakdown



# 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+*

# Conclusion

Developing, deploying, and maintaining a next-generation Managed Detection and Endpoint Response service for the City of New West will take 6 months to complete. After 6 months, Cyberquack and the City of New West can negotiate continued support of the security infrastructure. Completion of the EDR portion of the project will involve several months of development, which has been broken down into 3 phases.

Phase one will involve initial security posture assessments and strategy development with the City of New Westminster’s officials. Phase two will involve the initial EDR integration with City infrastructure and development of the EDR into a managed solution that exceeds industry standards. The final phase of EDR development will be the full-scale deployment and further optimization of the system. During this phase Cyberquack’s in-house security team will discover and secure any shortcomings with vigorous penetration testing.

Continuous monitoring and assessment of the MDR solution with Cyberquack’s resources is also offered after the final phase of the project. The period of this phase runs on an annual basis, allowing the City of New West continued confidence in the security of their organization.

Initial costs for the project are estimated to be $29,000 in Phase 1. EDR integration and development in Phase 2 will require extensive testing and analysis by a team of industry experts – the cost is estimated to be $160,000. This figure is based on entirely new equipment costs and meetings with City officials to determine inventory of assets may see this figure grossly overestimated. Final deployment and optimization of the security apparatus is estimated at $13,500.

In total, the cost of the project is estimated at $209,723.

Much of the cost of this project is related to the experience delivered by our team-members. Cyberquack has a golden track record when it comes to the safety and security of critical infrastructure. Attacks against organizations such as hospitals and local governments are on the rise, but the City of New West has a choice. Instead of becoming a statistic, choose Cyberquack.

# Recommendations

Cyberquack recommends that the City of New Westminster consider their unique needs and utilize the talents and resources presented to them in this report. An immediate security assessment by qualified professionals can highlight the gaps in security. These shortcomings must be addressed, and further action must be taken to secure City networks from attacker intrusion. Endpoint security is the highlighted risk in this scenario, and a managed Endpoint Detection and Response by Cyberquack is the solution.

# References:

[1] 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/

[2] S. W. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero trust architecture,” NIST, https://www.nist.gov/publications/zero-trust-architecture (accessed Feb. 20, 2024).

[3] ISO, “ISO/IEC 27001 standard – information security management systems,” *ISO*, Oct. 2022. https://www.iso.org/standard/27001

[4] “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).

[5] D. Benson, “CrowdStrike Falcon® Insight XDR | Products,” *crowdstrike.com*, Dec. 12, 2023. https://www.crowdstrike.com/products/endpoint-security/falcon-insight-xdr/