PALO ALTO CYBERSECURITY ACADEMY
@ CARIBOO HILL SECONDARY

Burnaby School District is pleased to offer the opportunity for grade 8 - 12 students to learn from one of the world's leading cybersecurity companies. The Palo Alto Academy at Cariboo Hill Secondary will provide focussed study on network security skills including firewall installation, antivirus/antispyware software and zero-day vulnerabilities. The Academy will also be integrated with computer programming and computer information systems courses.

Students completing the course work in this Academy will receive globally recognized cyber security technician certification. With business cyber-attacks occurring every 40 seconds and 1.5 million jobs forecast worldwide, students will be well equipped to gain immediate employment in an industry where entry level salaries are higher than average.

COURSE SEQUENCE:

COURSE 1: CYBERSECURITY FOUNDATIONS
Faculty will review the fundamentals of cybersecurity and identify the concepts required to recognize and potentially mitigate attacks against enterprise networks as well as mission critical infrastructure.

Module 1: Cyber - Landscape
Introduction to the modern Cybersecurity Landscape and how vulnerabilities impact enterprise level IT infrastructure systems.

Module 2: Cyber - Threat Actors
Introduction to methods hackers use just to launch advance Threats, Malware, Spamming, Botnets, DDOS, Ransom Ware, APTs, and Phishing.

Module 3: Malware and Spamming
Introduction to malware and spamming techniques used to circumvent and negatively impact business-to-business transactions and networking systems.

Module 4: Wi - Fi and Advanced Threats
Introduction to wireless and advanced threat techniques such as ransomware used to disrupt business operations and impact organizational networks.

Module 5: Network Security Models
Introduction to effective network security models such as perimeter - based, positive control, zero trust, least privilege, and unit - level trust across information systems.

Module 6: Cloud and Data Center Security
Introduction to cloud-based enterprise networks and virtualized data centers.

Module 7: Best Practice and Principles
Introduction to endpoint security, HIPS, Configuration Management, Next Generation Firewalls, IDS/IPS, VPN, DLP, UTM, Threat Intelligence and how these technologies are leveraged to effectively secure perimeter and internal networks.

COURSE 2: CYBERSECURITY GATEWAY

Faculty will review the fundamental tenants of networking and general concepts involved in maintaining a secure network computing environment. During the review, faculty will be able to examine, describe general networking fundamentals and implement basic networking configuration techniques.

Learning Objectives:

- Demonstrate knowledge of interconnected technology in daily communication and lifestyle, and understanding systems that need protection.
- Examine cybersecurity landscape environments, attack threat vectors, exposure, vulnerabilities, and risk factors.
- Demonstrated knowledge of physical, logical, and virtual addressing that accommodates various sized networks through the use of subnet mask schemes.
- Explain the TCP/IP Model and correctly identify the functions of the specific layers including packet encapsulation and lifecycle.
- Accurately explain common use of cloud, virtualization, storage, backup, and recovery procedures.
- Apply the knowledge and skills necessary to plan, design, implement, troubleshoot, and maintain network infrastructure environments.

COURSE 3: CYBERSECURITY ESSENTIALS

Faculty will review the fundamental tenants of cybersecurity and general security concepts involved in maintaining a secure network computing environment. Faculty will review the nature and scope of today's cybersecurity challenges, strategies for network defense, as well as detailed information about next - generation cybersecurity solutions. Faculty will also review how to deploy a variety of security methodologies as well as technologies and concepts used for implementing a secure network environment.

Learning Objectives:

- Formulate an industry-standard design to protect infrastructure against cybersecurity threats
- Apply advanced filtering methodologies such as user, application, and content ID to protect against all known and unknown attack vectors
- Describe the basics of cryptography including synchronous/asynchronous encryption, PKI, and certificates.
- Demonstrate ability to assess and harden endpoints based on security policies
- Describe uses of advanced malware research and analysis to provide enhanced protection for enterprise networks
- Examine mobile and cloud - based connection technologies

COURSE 3: CYBERSECURITY GATEWAY LABS

Module 1

- Configuring DCHP server on Palo Alto Networks Firewall (and set client to DHCP)
- Configuring TCP/IP and a Virtual Router on Palo Alto Networks Firewall
- Creating and using VLANs on the Palo Alto Networks Firewall

Module 2

- Creating Packet Captures (TCP Dump from Firewall/Wireshark)
- Analyzing Packet Captures (Firewall and Client)

Module 3
• Using the Application Command Center to find threats
• Analyzing Firewall Logs – PAN OS
Module 4
• Protecting Sensitive Data
• Preventing threats from the Internet with file blocking
Module 5
• Log Forwarding to Linux (setup syslog to DMZ server)
• Backing up your firewall logs

COURSE 4: CYBERSECURITY ESSENTIAL LABS

Module 1: Cybersecurity Design Principles
• Creating a zero - trust environment – PAN OS
• Configuring Authentication - FW
Module 2: Next Generation Firewalls
• Using two - factor authentication to secure the firewall
Module 3: Cryptography, PKI, and Certificate Protection
Module 4: Advanced Endpoint Protection
Module 5: Threat Prevention and Intelligence
Module 6: Mobile/Cloud Security
• Allowing only trusted applications – APP ID
• Managing Certificates
• Using Online Certificate Status Protocol (OCSP) – Global Protect VPN
• Decrypting Traffic (SSH)
• Securing the endpoint using vulnerability profiles
• Stopping reconnaissance attacks
• Using Mind Meld to update the firewall
• Denying international attackers
• Securing mobile devices using the firewall
• Accessing the network from anywhere
• Configuring Clientless VPN