Toronto AI School

Master Program in AI Cybersecurity & Ethical Hacking

Week 1 – Cybersecurity Foundations

Session	Topics Covered
Day 1 – Modern Cyber Threat Landscape	- Overview of global cyber threats - Types of cyber attacks (ransomware, phishing, malware) - Security architecture fundamentals - Zero Trust architecture concept - Security operations center (SOC) overview - Case Study: Colonial Pipeline cyber attack - Case Study: SolarWinds supply chain breach
Day 2 – Security Frameworks	- NIST cybersecurity framework - ISO 27001 security standards - Threat modeling methodologies - Security risk assessment process - Enterprise security architecture layers - Case Study: Equifax data breach - Case Study: Target retail data breach
Day 3 – AI in Cybersecurity	- AI-driven threat detection systems - Machine learning for fraud detection - Behavioral analytics in cybersecurity - Automated threat response systems - Security analytics pipelines - Case Study: TD Bank fraud detection systems - Case Study: Mastercard fraud detection AI

Week 2 – Ethical Hacking Fundamentals

Session	Topics Covered
Day 1 – Penetration Testing Process	- Penetration testing lifecycle - Reconnaissance techniques - Open-source intelligence gathering - Network scanning using tools - Vulnerability identification - Case Study: Uber security breach - Case Study: Yahoo data breach
Day 2 – Exploitation Techniques	- Password cracking methodologies - Privilege escalation attacks - Buffer overflow vulnerabilities - Social engineering attacks - Credential theft techniques - Case Study: LinkedIn credential breach - Case Study: Facebook security vulnerabilities

Day 3 – Hacking Lab Activities	- Hands-on vulnerability scanning - Simulated phishing campaign exercise - Password cracking lab - Network penetration testing exercise - Web vulnerability testing - Case Study: ransomware attack simulation - Case Study: enterprise breach investigation

Week 3 – Network Security

Session	Topics Covered
Day 1 – Network Architecture Security	- Network protocols vulnerabilities - Firewalls and security gateways - Intrusion detection systems - Network traffic analysis - Packet inspection techniques - Case Study: Verizon telecom network security - Case Study: AT&T; enterprise network defense
Day 2 – Threat Detection	- Security Information Event Management (SIEM) - Log monitoring systems - Threat intelligence platforms - Real-time network monitoring - Incident detection frameworks - Case Study: Cisco threat detection architecture - Case Study: CrowdStrike endpoint security
Day 3 – Security Defense Strategies	- Network segmentation - Advanced firewall rules - Intrusion prevention systems - Security monitoring dashboards - Threat hunting methodology - Case Study: government cyber defense systems - Case Study: enterprise SOC operations

Week 4 – Web Application Security

Session	Topics Covered
Day 1 – OWASP Security Risks	- OWASP Top 10 vulnerabilities - SQL injection attacks - Cross-site scripting attacks - Cross-site request forgery - Authentication vulnerabilities - Case Study: Shopify application security - Case Study: Amazon web platform security
Day 2 – Secure Coding Practices	- Secure software development lifecycle - DevSecOps pipelines - Secure API design - Input validation techniques - Authentication best practices - Case Study: Google secure development process - Case Study: Microsoft secure code practices

Day 3 – Application Penetration Testing	- Web application vulnerability scanning - Manual security testing - Authentication bypass testing - API security testing - Application firewall protection - Case Study: PayPal security architecture - Case Study: Stripe payment security

Week 5 – Cloud Security

Session	Topics Covered
Day 1 – Cloud Security Architecture	- AWS security fundamentals - Azure security architecture - Google Cloud security model - Identity and access management - Cloud data protection - Case Study: Netflix cloud security - Case Study: Capital One cloud breach
Day 2 – Cloud Threat Monitoring	- Cloud logging systems - Security monitoring pipelines - Threat detection in cloud environments - Cloud access audits - Security automation tools - Case Study: AWS security architecture - Case Study: Google Cloud enterprise security
Day 3 – Cloud Incident Response	- Cloud security incident response - Security event investigation - Threat containment strategies - Disaster recovery planning - Cloud backup systems - Case Study: enterprise ransomware response - Case Study: banking cloud security incident

Week 6 – AI Security & Adversarial AI

Session	Topics Covered
Day 1 – AI Security Threats	- Adversarial machine learning - Model poisoning attacks - Data manipulation threats - Prompt injection attacks - AI model exploitation risks - Case Study: chatbot manipulation attacks - Case Study: AI system vulnerabilities
Day 2 – Protecting AI Systems	- AI security architecture - Model monitoring frameworks - Secure training pipelines - AI data protection - AI system access control - Case Study: enterprise AI governance - Case Study: secure LLM deployments

Day 3 – AI Threat Detection	- AI-powered SOC assistants - Security analytics using ML - Threat prediction models - Security anomaly detection - AI security automation - Case Study: financial fraud AI detection - Case Study: telecom anomaly detection

Week 7 – Digital Forensics

Session	Topics Covered
Day 1 – Cyber Incident Investigation	- Digital evidence collection - Forensic investigation process - Chain of custody procedures - System log analysis - Incident reconstruction - Case Study: ransomware investigation - Case Study: corporate cyber espionage
Day 2 – Malware Analysis	- Malware behavior analysis - Reverse engineering basics - Threat intelligence collection - Malware detection strategies - Malicious code analysis - Case Study: WannaCry ransomware - Case Study: Stuxnet cyber weapon
Day 3 – Forensic Tools	- Digital forensic software tools - Memory analysis techniques - Disk analysis procedures - Network forensic analysis - Evidence documentation - Case Study: law enforcement cyber investigation - Case Study: enterprise forensic response

Week 8 – Security Automation

Session	Topics Covered
Day 1 – Security Automation Systems	- Security orchestration platforms - Automated incident response - Security automation workflows - Threat intelligence integration - Security alert automation - Case Study: enterprise SOC automation - Case Study: banking fraud automation
Day 2 – AI Security Agents	- Autonomous cyber defense agents - AI threat hunting agents - Security monitoring automation - AI-based security alerts - Security analytics automation - Case Study: AI SOC assistants - Case Study: enterprise AI defense systems

Day 3 – Security Infrastructure Automation	- DevSecOps automation pipelines - Security CI/CD integration - Automated vulnerability scanning - Continuous security monitoring - Automated patch management - Case Study: cloud security automation - Case Study: fintech security automation

Week 9 – Governance, Risk & Compliance

Session	Topics Covered
Day 1 – Cyber Governance	- Corporate cybersecurity governance - Risk management frameworks - Cyber insurance strategies - Executive cyber risk management - Board-level security oversight - Case Study: enterprise cyber governance - Case Study: banking cybersecurity strategy
Day 2 – Compliance Frameworks	- GDPR compliance overview - HIPAA healthcare security - Canadian privacy regulations - Data protection compliance - Compliance audit procedures - Case Study: healthcare security compliance - Case Study: financial regulatory compliance
Day 3 – Security Policy Design	- Enterprise security policies - Security risk assessments - Policy enforcement frameworks - Security awareness programs - Compliance monitoring - Case Study: government cyber policy - Case Study: enterprise risk management

Week 10 – Capstone Security Projects

Session	Topics Covered
Day 1 – Security Architecture Design	- Design enterprise security architecture - Create zero trust framework - Develop cloud security plan - Implement security monitoring - Build threat detection pipeline - Project: enterprise cyber defense system - Project: AI threat detection engine
Day 2 – Ethical Hacking Project	- Penetration testing project - Web vulnerability assessment - Network security audit - Exploit demonstration - Security report preparation - Project: enterprise penetration test - Project: application security audit

Day 3 – AI Security Systems	- Develop AI-based SOC assistant - Build anomaly detection model - Deploy automated security pipeline - Design threat monitoring dashboard - Integrate security automation - Project: financial fraud detection AI - Project: telecom anomaly detection AI