CYBERSECURITY CONSULTING

Threat & Risk Assessments (TRA / hTRA)

A systematic assessment that identifies, rates, and prioritizes the threats and vulnerabilities in a specific system, using the Harmonized Threat and Risk Assessment (HTRA) methodology.

CyberX One's threat and risk assessment examines a specific system or application end to end. Following the HTRA methodology and benchmarking against NIST, ISO 27001, or CIS, we value your assets, map threats and vulnerabilities to concrete risk scenarios, and deliver a prioritized treatment plan that reduces or removes risk.

Objectives

- Recognize potential internal and external threats and vulnerabilities across the system.
- Assess the likelihood and impact of each risk, factoring in compensating controls.
- Prioritize risks by severity and develop actionable remediation plans.
- Strengthen posture through targeted risk-mitigation strategies.
- Ensure the system meets relevant standards, regulations, and legal requirements.

Outcomes & benefits

- **Actionable findings**, a detailed, prioritized list of threats and vulnerabilities.
- **Asset protection**, digital, physical, and human assets safeguarded across the system.
- **Informed decisions**, a foundation for security investment and resource allocation.
- **Stronger governance**, policies and controls updated from concrete findings.
- **Compliance evidence**, a defensible, framework-aligned assessment record.

Scope of service

- Information exchange, review of solution architecture and data-flow diagrams.
- Review of existing cybersecurity documentation, policies, and prior assessments.
- Information-gathering workshops with key personnel to assess control status against NIST, ISO 27001, and CIS.
- Detailed control analysis producing impactful findings tied to real threats and risks.
- An HTRA-methodology report with asset valuations, likelihood/impact ratings, and treatment plans.

Our process

1. **Scope**
   Identify the environments and systems in scope and their criticality.
2. **Map data flows**
   Describe how data moves and the use cases for the system.
3. **Assess**
   Run workshops and analyze controls against the chosen framework.
4. **Report & treat**
   Deliver the HTRA report with prioritized remediation and treatment plans.

What you receive

- HTRA-methodology assessment report
- Asset valuation and threat/vulnerability register
- Likelihood and impact risk ratings
- Prioritized remediation and treatment plan

Engagement at a glance

TYPICAL DURATION	LED BY	SERVICE TYPE
~3-4 weeks per system	Cybersecurity Consultant	Assessment · per system

HTRA · NIST CSF · ISO 27001 · CIS Controls

Ready to start?

Email **shah@cyberxone.ca** · **LinkedIn**

CyberX One Inc. · Markham, Ontario · Serving Canada

Book a discovery call