



SEEKINGFIRE

Seeing the Unforseeable

Services Catalogue



Consultancy and advisory services

Security program strategic development

- Virtual and fractional CISO service
- ISO 27001 information security management system (ISMS) implementation
- Support preparing for SOC2 attestation audit
- Risk assessment and risk management support and implementation
- Policy development — actionable, audit-ready policies and governance structures that reflect your organization's culture, size, and compliance obligations
- Supplier/third-party risk management program support and development
- Business continuity planning (BCP) and disaster recovery planning (IT DRP) development
- Business impact assessments (BIA)
- Privacy consulting
- Information security support with your digital transformation
- AI business process introduction and enablement
- SOC 2 and CMMC (and CPCSC next) readiness

You're looking for a CISO to act as a partner and give your organization guidance, but don't feel that the size of your organization warrants a full-time role. We can provide experienced executive-level security leadership, strategic oversight, and guidance sized to your needs to lead the implementation and development of your security management program.

Audit and assessment

- Security gap assessment and compliance readiness assessments (ISO 27001, CIS 20, SOC2, NIST)
- Security program maturity assessment based on the ISO 27001 security framework and using the capability maturity model (CMM) for maturity scoring, including a 3-year practical and risk-prioritized roadmap for improvement
- ISO 27001-based certification readiness assessments
- Security incident response tabletop exercises
- Internal audit support
- External audit support, report review, and regulatory response
- Credit union IT security regulatory audits
- M&A cybersecurity due diligence

Every organization needs a neutral third party to see if their security is up to the standard they think it is. But we only start there - we can help you with a formal audit program to help you achieve your goals, including regulatory compliance.



Once we've illuminated the unknown dark corners, we can also help you build a program to provide ongoing monitoring and track remediation efforts.

Offensive security / testing services

- Vulnerability scanning and risk prioritization

Run regular or one-time scans to identify known vulnerabilities across infrastructure, endpoints, and cloud services. Includes CVSS scoring and remediation guidance.

- Penetration testing (internal, external, Web) including Red team and adversary simulation options

Targeted external, internal, and web application penetration tests simulating real-world attack scenarios including manual techniques. Detailed reporting with prioritized remediation recommendations provided.

- Web application security testing

Assess your business-critical applications for vulnerabilities using the OWASP Top 10. We assess business logic, authentication flows, and access control issues.

- Threat simulation and exploitation

Social engineering, simulated phishing, password spraying, and custom exploit proof-of-concepts tailored to your threat model and risk appetite.

- Wireless security assessments

- Physical security testing

Operational security services

Security incident response and digital forensics

- Incident response planning and playbook creation
- Incident response handling support, including malware analysis and threat attribution
- Forensic imaging & analysis
- Litigation support and expert witness testimony

Virtually all organizations experience breaches. Maybe it is something small like a ransomware issue on a few company laptops. Or something larger like an insider leak and fraud. Preparation reduces the impact, and access to an experienced security incident handler in a time of need can reduce it further.



End-user security and culture

- Role-based security training (including for executives)
- Insider threat program development

Change behaviour, reduce risk.

Cloud

- Cloud security architecture
- Cloud and Microsoft 365 security reviews

Review your cloud configurations, conditional access policies, Secure Score posture, and endpoint management through an experienced lens. Includes actionable recommendations for hardening and governance.

Security operations, tooling, and automation

- Technology security controls: architecture, configuration, and organizational deployment
- Zero trust and network segmentation design
- Secure development lifecycle (SDLC) and DevSecOps integration
- Vulnerability management and patch governance
- Security automation scripting
- MDR integration
- SOAR implementation
- Compromise Assessments & Threat Hunting

Implementing technical security controls is outside the core expertise of many IT teams. We support the planning and solution design for your internal team, letting them focus on what they do best while ensuring that the control will still fit perfectly into your security program.



About Us

Our Mission

To make the digital world a safer, more secure place where people, organizations, and communities thrive.

Non-status indigenous owned, Seekingfire specializes in strategic information security. We use our decades of experience to help clients protect data and critical systems. We can help you:

- reduce the risk of security and privacy threats to an acceptable level,
- offer assurance and peace of mind for your people, your customers, and your partners,
- get the best results from innovative technology, and
- extend your reach to harness opportunities and preserve the trust your customers have in you.

When people feel safe and secure, they are empowered to do their best work.

Our Values

1. Relationships

We value people and the interactions and experiences we have with others. Seekingfire aims to foster an environment of mutual trust and respect.

2. Respect

Seekingfire values its clients and team members and the experience they bring to every project. This mutual respect informs our interactions and communications with one another.

3. Knowledge

Learning is an ongoing process and each day we take in new information that helps us become better. This knowledge is not taken for granted and is key to our success.

4. Care

Seekingfire is a guardian for our clients and their assets. It is our responsibility to protect these assets and provide considered and intentional support and advice.

5. Fun

We love our work and the people we work with. It should be fun.

6. Integrity

We believe in being authentic and honouring our principles. Doing what is right isn't always easy, but we will strive to make the best choices possible whenever possible.