GetCyber™ | Dan Duran, MSc Cybersecurity, MBA, CISSP, CCSP

# Security Assessments & Advisory for Regulated, Data-Sensitive, and Critical Operations.

## Hacker Insight. Executive Judgment.

Security work is only valuable if it leads to clear decisions. GetCyber connects technical exploitation to strategic risk decisions to ensure your defenses are built for reality, not a checklist.

Built for organizations operating in regulated, procurement-sensitive, and mission-critical environments shaped by privacy, governance, security, and resilience expectations.

### Identity Attack Surface

Assess how identity, access, and privileges could be used to move through your environment or escalate access.

### AI Security & Governance

Assess how AI tools and third-party models access your data and the risk of unintended or unauthorized data access.

### Sensitive Data Exposure

Assess sharing, permissions, misconfigurations, and uncontrolled visibility across Microsoft 365 & Google Workspace.

### Security Governance & Operational Risk

Assess governance, control maturity, vendor dependencies, and operational risk from control gaps and ownership ambiguity.

### Ongoing Advisory & Specialized Support

Continuous strategic security advisory aligned to evolving risk, architecture, and regulatory requirements.

getcyber.me

### Industries & Sectors

- ☑ Defence Contractors
- ☑ Government & public sector
- ☑ Essential Services & Critical Infrastructure
- ☑ Healthcare
- ☑ Financial Operations
- ☑ Law, Accounting & Tax
- ☑ Universities, Colleges & School Boards

### Compliance / Standards

- ☑ ITSG-33 & GC (CSP, CCSC)
- ☑ NIST (CSF, SP 800-53, SP 800-171)
- ☑ CMMC 2.0 & CIS Controls
- ☑ ISO 27001, SOC 2, PCI DSS
- ☑ PIPEDA & Canadian Privacy
- ☑ Healthcare Privacy (HIPAA)



14 Main St W, Grand Bend
ON, N0M 1T0, Canada

Phone: 1-519-721-8345
Email: dan@getcyber.me

# About Dan Duran

Hacker Insight. Executive Judgment.

**Dan Duran is a cybersecurity researcher, CTO, and senior risk advisor with over 20 years of experience across security, software engineering, and cloud platforms.**

He specializes in identifying real-world attack paths in identity and data-driven environments, translating technical exposure into focused, defensible actions for leadership.

Dan holds a Master's in Cybersecurity, an MBA, and CISSP and CCSP certifications. He is the principal behind GetCyber™, a cybersecurity advisory practice established in 2021, where he leads focused security assessments for regulated and high-risk environments, delivering clear insight into actual attack surface and actionable next steps.


LinkedIn

The Hacker's Lens

## Attacker Perspective

I assess your environment by identifying realistic attack paths—focusing on identity compromise, over-permissioned access, and data exposure.

- **Identity-First:** Hunting for initial exploitation, privilege escalation and lateral movement paths.
- **Data Exposure:** Locating overshared M365/SaaS data before an attacker does.
- **Realism Over Theory:** Prioritizing vulnerabilities that are actually exploitable.
- **Validation:** Ensuring findings are grounded in technical proof, not generic scanner noise.

The Advisor's Lens

## Advisory Judgment

Findings are translated into a prioritized roadmap. I help leadership understand what matters, why it matters, and where to act first.

- **Risk-First Approach:** Aligning security needs with business impact, not just compliance.
- **Actionable Remediation:** Providing implementation-ready steps to close exposure gaps quickly.
- **Decision Support:** Reducing uncertainty for confident and optimized resource decisions.
- **Governance Alignment:** Contextual mapping to compliance and standards.

**Available for engagements across Canada, the US, and select international markets.**

# Request a Security

The first 60 minutes is on us!

Includes a focused discovery session, scoped assessment, and prioritized findings within weeks—not months.

(519) 721-8345 | dan@getcyber.me



14 Main St W, Grand Bend
ON, N0M 1T0, Canada

Phone: 1-519-721-8345
Email: dan@getcyber.me

# GetCyber™ Identity Attack Surface Assessments

## This assessment provides a researcher-led review of how your identity, access, and privilege structures could be used to move through your environment, escalate access, or weaken control boundaries.

Includes roles, administrative permissions, service accounts, authentication controls, and access relationships across key systems.

**A Different Approach to Risk:** We replace long consulting cycles and "checkbox security" with fast, high-impact assessments that lead to measurable reduction in exposure.

### Identity is the New Perimeter

Most modern breaches do not originate from traditional perimeter failure; they stem from identity compromise, over-permissioned access, and lateral movement. For organizations managing sensitive data or critical infrastructure, a single weak identity relationship can lead to full environment compromise.

The Hacker's Lens

### Technical Validation

- **Realistic Attack Paths:** Identifying how an attacker moves from initial entry to your most sensitive data.
- **Privilege Escalation:** Hunting for hidden paths that allow standard users to gain administrative control.
- **Credential & Auth Review:** Analyzing weak authentication controls and service account vulnerabilities.
- **Lateral Movement:** Mapping over-permissioned accounts allowing attackers to jump between isolated systems.

The Advisor's Lens

### Business Impact

- **Prioritized Risk:** Findings are ranked by consequence and likelihood, not just technical severity.
- **Decision Support:** Translating complex exploitation paths into concise, decision-ready business context.
- **Strategic Remediation:** Practical next steps to reduce uncertainty and improve security decisions.
- **Ownership Clarity:** Identifying where ambiguity in access ownership creates operational risk.

## High-Signal Intelligence Prioritized findings report designed for both technical and executive teams.

- ☑ **Key Risks:** What is actually at stake.
- ☑ **Exploitation Path:** A clear map of how the compromise would occur in practice.
- ☑ **Business Impact:** Why this matters to your operations and regulatory standing.
- ☑ **Remediation Roadmap:** Immediate, risk-aligned actions to close the exposure.
- ☑ **Deliverables:** Executive summary of risk, technical findings, remediation guidance, a strategic action plan, compliance mapping and an executive presentation.

## Request a Security

The first 60 minutes is on us!

Includes a focused discovery session, scoped assessment, and prioritized findings within weeks—not months.

(519) 721-8345 | dan@getcyber.me



14 Main St W, Grand Bend
ON, N0M 1T0, Canada

Phone: 1-519-721-8345
Email: dan@getcyber.me

GetCyber™

# AI Readiness Assessments

## This assessment identifies how AI tools, models, and third-party integrations interact with your data and permissions before and during enterprise adoption.

Includes data access by AI tools, permission scopes, model integrations, vendor dependencies, governance controls, and risks of unintended data exposure across connected systems.

**A Different Approach to AI Risk:** We replace reactive policies and unchecked AI adoption with focused assessments that identify real data exposure and governance gaps before they scale.

### AI Adoption = Exposure

The rapid integration of AI tools and Copilots often outpaces existing security controls. For organizations with sensitive data, AI creates a high-velocity discovery path for internal information, where misconfigured permissions or "Shadow AI" usage can lead to massive, unintended data ingestion and leakage.

The Hacker's Lens

### Technical Validation

- **Unintended Data Discovery:** Identifying where AI tools surface sensitive data due to over-permissioned access.
- **Permission Leakage:** Mapping how AI-integrated platforms can bypass traditional data boundaries.
- **Vendor Exposure:** Analyzing technical risks associated with third-party model data ingestion and privacy.
- **Control Boundary Analysis:** Testing the effectiveness of existing guardrails against AI-driven data access.

The Advisor's Lens

### Business Impact

- **Governance Gaps:** Identifying maturity deficiencies affecting safe and compliant AI deployment.
- **Vendor Dependency Risk:** Translating model risks into operational and contractual business impacts.
- **Compliance Alignment:** Reviewing AI usage against regulatory frameworks and standards.
- **Strategic Decisions:** Providing insights to help leadership decide where to permit or restrict AI usage.

## High-Signal Intelligence You will receive a prioritized report designed to enable safe AI adoption.

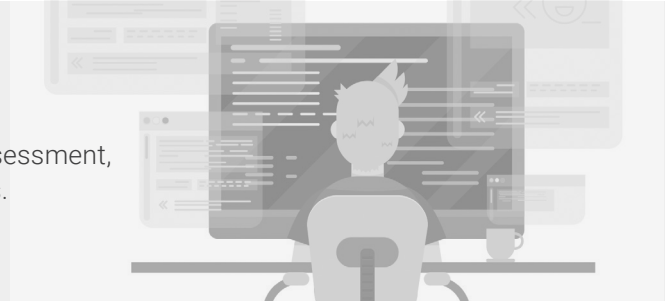
- ☑ **Key AI Risks:** Exposure points within your AI environment.
- ☑ **Ingestion & Leakage Paths:** Clear mapping of how data could be unintentionally accessed or leaked.
- ☑ **Business Impact:** Analysis of how AI exposure affects regulatory standing and data privacy.
- ☑ **Remediation Roadmap:** Clear, prioritized actions to secure AI-driven workflows.
- ☑ **Deliverables:** Executive summary of risk, technical findings, remediation guidance, a strategic action plan, compliance mapping and an executive presentation.

## Request a Security

The first 60 minutes is on us!

Includes a focused discovery session, scoped assessment, and prioritized findings within weeks—not months.

(519) 721-8345 | dan@getcyber.me





14 Main St W, Grand Bend
ON, N0M 1T0, Canada

Phone: 1-519-721-8345
Email: dan@getcyber.me

# GetCyber™ Sensitive Data Exposure Assessments

## This assessment reviews how sensitive data is exposed across platforms such as Microsoft 365, Google Workspace, SAP, and Salesforce, as well as other integrated

Includes file sharing, permissions, inherited access, public links, external collaboration, and configurations that create unintended data exposure across cloud platforms.

**A Different Approach to Data Exposure:** We replace broad data reviews and compliance checks with focused assessments that identify real exposure paths, oversharing, and misconfigurations before they lead to data loss.

### Data Exposure Breaches

Modern breaches rarely result from traditional perimeter failures; they stem from oversharing, misconfigured access, and inherited permissions within cloud environments. For cloud-heavy organizations using Microsoft 365 and SaaS platforms, sensitive data is often just one misconfigured link away from public exposure.

The Hacker's Lens

### Technical Validation

- **Shadow Exposure:** Identification of overshared, publicly accessible, or misconfigured data links.
- **Permission Inheritance:** Reviewing how complex permission structures lead to uncontrolled data visibility.
- **Access Paths:** Mapping how an attacker moves from an initial entry point to sensitive data repositories.
- **SaaS Sprawl:** Assessing exposure across integrated third-party SaaS applications and cloud storage.

The Advisor's Lens

### Business Impact

- **Material Risk Prioritization:** Findings are ranked by their business impact and likelihood of exploitation.
- **Regulatory Compliance:** Aligning data exposure findings with regulatory frameworks and standards.
- **Decision Clarity:** Translating technical data risks into clear choices for leadership and operational teams.
- **Actionable Outcomes:** Providing remediation steps to close exposure gaps without disrupting workflows.

## High-Signal Intelligence Focused report designed to identify and close data exposure gaps.

- ☑ **Key Data Risks:** What information is materially exposed.
- ☑ **Exploitation Potential:** Why the exposure matters and how it could be abused.
- ☑ **Business Impact:** The consequence of exposure to your operations and reputation.
- ☑ **Remediation Steps:** Clear, prioritized actions to harden data access controls.
- ☑ **Deliverables:** Executive summary of risk, technical findings, remediation guidance, a strategic action plan, compliance mapping and an executive presentation.

## Request a Security

The first 60 minutes is on us!

Includes a focused discovery session, scoped assessment, and prioritized findings within weeks—not months.

(519) 721-8345 | dan@getcyber.me



14 Main St W, Grand Bend
ON, N0M 1T0, Canada

Phone: 1-519-721-8345
Email: dan@getcyber.me

GetCyber™

# Governance & Risk Assessments

## This assessment reviews security governance to identify where ownership ambiguity or control gaps create regulatory, contractual, or business

Includes control maturity, policy and standards alignment, ownership and accountability, vendor dependencies, and governance gaps that introduce operational and regulatory risk.

**A Different Approach to Governance Risk:** We replace static audits and policy reviews with focused assessments that identify control gaps, ownership ambiguity, and decision risk before they impact operations or compliance.

### The Reality

Compliance is not security. Many organizations fall into "compliance theater," where checkboxes are marked but meaningful exposure remains. In high-stakes environments with operational dependencies and regulatory pressure, weak governance and ownership ambiguity create material business risk.

The Hacker's Lens

### Technical Validation

- **Control Maturity Analysis:** Identifying gaps in security controls that leave technical systems vulnerable.
- **Vendor & Platform Risk:** Evaluating technical dependencies and risks from third-party vendors.
- **Dependency Mapping:** Reviewing how platform-related risks affect the technical resilience of the environment.
- **Ownership Identification:** Pinpointing where technical ownership ambiguity leads to unmanaged security debt.

The Advisor's Lens

### Business Impact

- **Strategic Risk Alignment:** Bridging the gap between technical risk findings and business impact.
- **Decision-Making Support:** Reducing uncertainty to enable clearer, faster security decisions.
- **Actionable Oversight:** Practical recommendations to strengthen governance without overengineering.
- **Prioritized Remediation:** Focusing efforts on risks that have the most measurable impact on risk reduction.

## High-Signal Intelligence Reports that connects governance gaps to real-world operational impact.

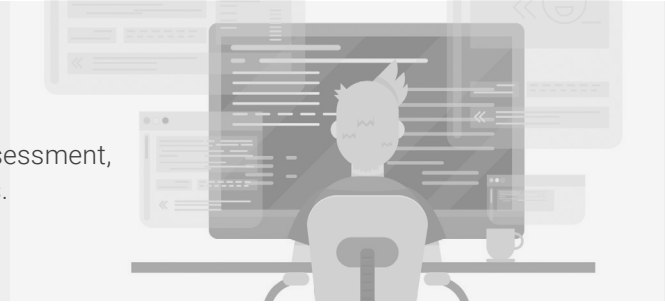
- ☑ **Key Risks:** Prioritized maturity gaps and ownership risks.
- ☑ **Impact Analysis:** Why the risk matters to your business operations and leadership.
- ☑ **Exploitation Likelihood:** Realistic assessment of how these gaps could be abused.
- ☑ **Remediation Actions:** Clear, practical steps to improve oversight and reduce exposure.
- ☑ **Deliverables:** Executive summary of risk, technical findings, remediation guidance, a strategic action plan, compliance mapping and an executive presentation.

## Request a Security

The first 60 minutes is on us!

Includes a focused discovery session, scoped assessment, and prioritized findings within weeks—not months.

(519) 721-8345 | dan@getcyber.me





14 Main St W, Grand Bend
ON, N0M 1T0, Canada

Phone: 1-519-721-8345
Email: dan@getcyber.me

# GetCyber Ongoing Advisory & Specialized Support

## This service provides continuous access to expert-led security guidance for organizations that need support with risk decisions and evolving priorities.

Includes ongoing security guidance, architecture and design input, risk and control validation, vendor and technology decisions, and support for initiatives requiring expert oversight.

**A Different Approach to Security Advisory:** We replace ad hoc consulting and fragmented guidance with consistent, expert-led advisory that aligns decisions to real risk, architecture, and evolving operational requirements.

### A Continuous Process

Emerging threats, shifting architectures, and rapid technology adoption mean that exposure is never static. For organizations without a full-time security lead, the gap between technical risk and business decision-making often widens, leading to expensive "checkbox" solutions that don't address realistic attack paths.

The Hacker's Lens

### Technical Validation

- **Attack Path Validation:** Testing how changes in architecture introduce new paths to sensitive data.
- **Abuse Case Analysis:** Identifying how features, integrations, or workflows could be misused by attackers.
- **Control Evasion Testing:** Assessing whether new controls can be bypassed under realistic attack conditions.
- **Exposure Drift Detection:** Identifying how incremental changes create unintended access or data exposure.

The Advisor's Lens

### Business Impact

- **Fractional Strategic Support:** Access to high-level advisory without the cost of a full-time hire.
- **Prioritized Decision-Making:** Focus on risks that lead to measurable, real-world risk reduction.
- **Bridge Technical & Executive:** Translating complex technical exposure into clear roadmaps.
- **Vendor & Tool Triage:** Objective, tool-agnostic advice on security investments.

## High-Signal Intelligence Outputs are structured to drive immediate, informed action.

- ☑ **Direct Access:** Priority availability for urgent questions or architecture reviews.
- ☑ **Validated Insights:** Manual review of security concerns—no generic scanner noise.
- ☑ **Clear Next Steps:** Actionable remediation or decision support for every finding.
- ☑ **Strategic Alignment:** Ensuring security priorities always mirror business objectives.
- ☑ **Outcome:** Focused, expert-led support that transforms security from a roadblock into a business enabler.

## Request a Security

The first 60 minutes is on us!

Includes a focused discovery session, scoped assessment, and prioritized findings within weeks—not months.

(519) 721-8345 | dan@getcyber.me



14 Main St W, Grand Bend
ON, N0M 1T0, Canada

Phone: 1-519-721-8345
Email: dan@getcyber.me