Chaos, order and the way forward
Perspectives on the evolution of cybersecurity

Gary Miller
October 2019
Never before has the creation and preservation of value depended so much on effective cyber security, nor has the means to “getting security right” been so challenging…

...let’s discuss
Our strategic imperative: Protect and enable

We will continue to see digital innovation pushed to new heights— to the benefit of our communities, our societies and our planet.

Strong cyber security is an essential element of Canadian innovation and prosperity. Individuals, governments and businesses will want to have confidence in the cyber systems that underpin their daily lives.”

Source: Public Safety Canada
A convergence of trends has created an asymmetrical, and arguable chaotic, condition.
• Struggling to find clarity amongst excessive market, tools and vendor noise

• Looking to extract greater value from existing security investments

• Urgently needing to modernize security management platforms

87% of organizations are seeking order from chaos
An organizing model

Simplify and solidify the core
• Optimization
• Prioritization
• Management overhead
• Market noise
• New technologies

Improve SIEM platforms
• Visibility
• Alert volume & fidelity
• Costs & licensing
• Use cases
• Data & analytics

Enable advanced detection
• Key vectors
• Behaviors
• Containment
• Intelligence
• Integration

Strengthen cloud defences
• Strategy
• Architecture
• Shadow IT
• 3rd party risk
• Risk analysis

Address convergence
• Cloud, data centre & enterprise
• IT & OT
• Response
• Intelligence
• Supply chain

Create order through strategic programs
An evolutionary process: have a destination and a plan

- Simplify and solidify the core
  - Categorize assets
  - Prioritize risk
  - Simplify tools & processes
  - Modernize program

- Enhance situational awareness
  - Continuous monitoring
  - SIEM optimization
  - Extend visibility
  - Enable convergence
  - Integrate threat intel

- Layer advanced capabilities
  - Managed detection & response
  - Advanced controls
  - Richer data sets
  - Human and automation
  - Actionable threat intelligence

- Evolve advanced analytics, Big Data, AI, SOAR, etc.
  - User & entity behaviour
  - Big data & AI
  - Automation and orchestration
  - Predictive analytics
  - Proactive hunting
  - Enhanced reporting

Tools
- Thresholds
- Humans
- Data
- Reactive
- Spotting

Platforms
- Behaviours/TTPs
- Automation
- Context/insight
- Predictive
- Hunting
The future state

1. You see what you need to see
   - Users
   - Apps
   - Servers
   - Network
   - Security tools
   - Endpoints
   - Cloud
   - IoT

2. The data tells you what you need to know
   - Collect: Behaviour analysis, Automaton & orchestration, Hunting framework, Open data model, Machine Learning & AI
   - Analyze: Log collection, Correlation, Data store, Case management, Reporting & portal
   - Identify & alert

3. You are acting on the things that matter
   - Contextual alerts
   - Incident, IR playbooks & automated responses
   - L1 analyst
   - L2 & L3 analysts, incident handlers & “light” responses

4. You are getting ahead of the threats
   - Alerts, bulletins & reports
   - Pen testing
   - Cyber threat intelligence, data analysts & scientists
   - Actionable intel, IOCs & build use cases

Technology and Security Monitoring
Detection and Response
Hunting / Analytics / Intel
“In the midst of chaos, there is also opportunity.”

Sun Tzu and Samuel B. Griffith.
The Art of War. 1964.
Questions