IBM SECURITY STRATEGY

DRIVING INNOVATION WHILE HELPING TO SECURE 17,500+ CUSTOMERS

David Millar  
Security Services Executive  
IBM Canada

Steve Rainville  
Associate Partner Security Services  
IBM Canada

November 2017
Cybersecurity is a universal challenge

By 2020, there will be…

20.8 billion
“things” to secure

5 billion
personal data records stolen

$8 trillion
lost to cybercrime
What our customers are facing

**COMPLIANCE MANDATES**
GDPR fines can cost **billions** for large global companies

**SKILLS SHORTAGE**
By 2022, there will be **1.8 million** unfulfilled cybersecurity positions

**TWO MANY TOOLS**
Organizations are using **too many** tools from too many vendors
Start a Committee

Your Cyber Security Committee!

CEO & Board Member(s)

Finance

HR

Comms

Marketing & Sales

Operations
To ramp up your SOC to detect and respond to advanced threats you need…

People

Process

Technology
Technology
Does this look familiar?

Security analytics

Data access control

Fraud protection

Vulnerability management

Application security management

Criminal detection

Threat and anomaly detection

Privileged user management

Incident response

Identity governance and administration

Network forensics and threat management

Firewalls

Sandboxing

Content security

Access management

Data protection

Network visibility and segmentation

IDaaS

Device management

Virtual patching

Threat sharing

Endpoint patching and management

Malware protection

Transaction protection

Endpoint detection and response

Indicators of compromise

Malware analysis

Mainframe security

Application scanning

Threat hunting and investigation

Network forensics and threat management

Virtual patching

Sandboxing

Content security

Threat sharing

Endpoint detection and response

Indicators of compromise

Malware analysis

Mainframe security

Application scanning

Threat hunting and investigation

Network forensics and threat management

Virtual patching

Sandboxing

Content security

Threat sharing

Endpoint detection and response

Indicators of compromise

Malware analysis

Mainframe security

Application scanning

Threat hunting and investigation

Network forensics and threat management

Virtual patching

Sandboxing

Content security

Threat sharing

Endpoint detection and response

Indicators of compromise

Malware analysis

Mainframe security

Application scanning

Threat hunting and investigation

Network forensics and threat management

Virtual patching

Sandboxing

Content security

Threat sharing

Endpoint detection and response

Indicators of compromise

Malware analysis

Mainframe security

Application scanning

Threat hunting and investigation

Network forensics and threat management

Virtual patching

Sandboxing

Content security

Threat sharing

Endpoint detection and response

Indicators of compromise

Malware analysis

Mainframe security

Application scanning

Threat hunting and investigation

Network forensics and threat management

Virtual patching

Sandboxing

Content security

Threat sharing

Endpoint detection and response

Indicators of compromise

Malware analysis

Mainframe security

Application scanning

Threat hunting and investigation

Network forensics and threat management

Virtual patching

Sandboxing

Content security

Threat sharing

Endpoint detection and response

Indicators of compromise

Malware analysis

Mainframe security

Application scanning

Threat hunting and investigation

Network forensics and threat management

Virtual patching

Sandboxing

Content security

Threat sharing

Endpoint detection and response

Indicators of compromise

Malware analysis

Mainframe security

Application scanning

Threat hunting and investigation

Network forensics and threat management

Virtual patching

Sandboxing

Content security

Threat sharing

Endpoint detection and response

Indicators of compromise

Malware analysis

Mainframe security

Application scanning

Threat hunting and investigation

Network forensics and threat management

Virtual patching

Sandboxing

Content security

Threat sharing

Endpoint detection and response

Indicators of compromise

Malware analysis

Mainframe security

Application scanning

Threat hunting and investigation

Network forensics and threat management

Virtual patching

Sandboxing

Content security

Threat sharing

Endpoint detection and response

Indicators of compromise

Malware analysis

Mainframe security

Application scanning

Threat hunting and investigation
An integrated and intelligent security immune system

**SECURITY ECOSYSTEM**
- Network forensics and threat management
- Firewalls
- Sandboxing
- Virtual patching
- Network visibility and segmentation

**ENDPOINT**
- Endpoint detection and response
- Endpoint patching and management
- Malware protection

**NETWORK**
- Security analytics
- Vulnerability management
- Threat and anomaly detection

**MOBILE**
- Transaction protection
- Device management
- Content security

**APPS**
- Application scanning
- Application security management
- Malware protection

**DATA**
- Indicators of compromise
- Malware analysis
- Threat sharing

**IDENTITY & ACCESS**
- User behavior analytics
- Incident response
- Threat hunting and investigation

**ADVANCED FRAUD**
- Fraud protection
- Criminal detection

**SECURITY ORCHESTRATION & ANALYTICS**
- Privileged user management
- Identity governance and administration
- Access management
- IDaaS
- Mainframe security

**THREAT INTEL**
- Security analytics
- Vulnerability management
- Threat and anomaly detection
Asking for the Cash!

Do we already have a product deployed with similar or the same functionality?
Asking for the Cash!

Does one of our current vendors have a product that integrates better into our existing environment than the one you are recommending?
Asking for the Cash!

Does this new technology have open API’s that will integrate into our existing technology portfolio?

Does it leverage AI to enhance the skills on our team?
Asking for the Cash!

Is all of our current security technology currently up to the latest version, patched, integrated and fully optimized? Is there any opportunity for automation in our current portfolio?
Process
NIST Cybersecurity Framework

Identify  Protect  Detect  Respond  Recover
Houston, we have a problem…

1. Get an outside firm on retainer NOW

2. Use an IR platform to help you build out, automate and integrate your tools and orchestrate your response

3. Practice, practice, practice
People
There are an estimated 3,000+ open security positions in Canada today.

How are you going to compete for security resources?
You are going to need to be part of the solution in helping to buildout the next generation of Canada’s cyber security skills.

• One Professional Hire
• Current Staff
• Local Colleges and Universities
• Women in Security - Why?
• New Collar Workers
• Selectively Out-Task SecOps, L1/L2, Threat Hunting, Emergency Response, etc. to an MSSP
Please remember, people are human…not machines.
Ramp up your SOC to detect and respond to advanced threats with...

AUGMENTED People

ORCHESTRATED Processes

INTEGRATED Technology
THANK YOU

FOLLOW US ON:

ibm.com/security
securityintelligence.com
xforce.ibmcloud.com
@ibmsecurity
youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2017. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.