ENDPOINT PROTECTION PROJECT 2014

Presentation to CTSC
5 February 2015

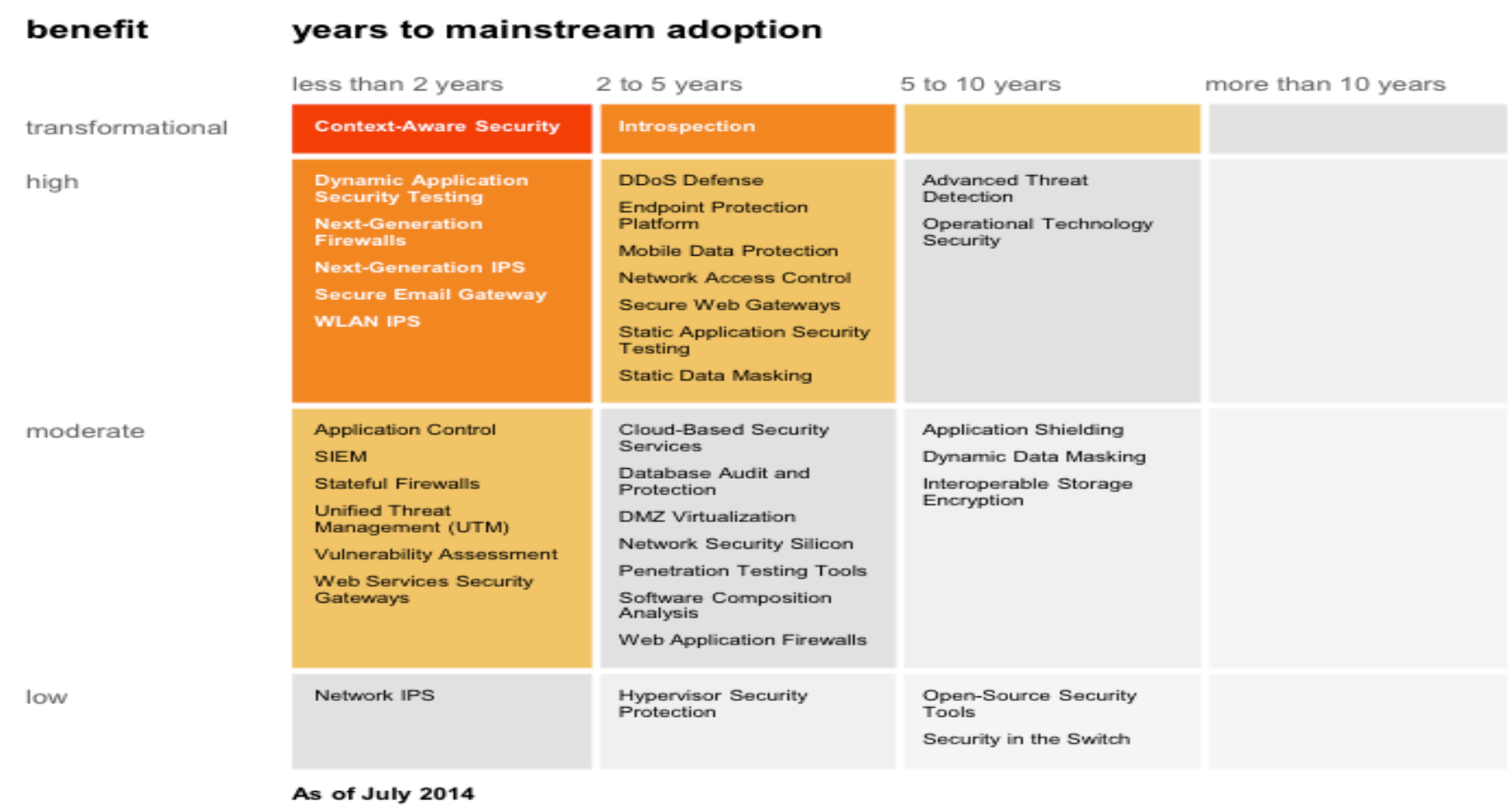
UNIVERSITY OF WATERLOO

WHY ARE WE DOING THIS?

- Antivirus is not top priority industry-wide
  - » CCIRC does not list endpoint or antivirus:https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tp-strtgs-eng.aspx
- Our numbers reflect poor detection & cleanup

GARTNER HYPE CYCLE

Figure 2. Priority Matrix for Infrastructure Protection, 2014



benefit	years to mainstream adoption			
	less than 2 years	2 to 5 years	5 to 10 years	more than 10 years
transformational	Context-Aware Security	Introspection		
high	Dynamic Application Security Testing Next-Generation Firewalls Next-Generation IPS Secure Email Gateway WLAN IPS	DDoS Defense Endpoint Protection Platform Mobile Data Protection Network Access Control Secure Web Gateways Static Application Security Testing Static Data Masking	Advanced Threat Detection Operational Technology Security	
moderate	Application Control SIEM Stateful Firewalls Unified Threat Management (UTM) Vulnerability Assessment Web Services Security Gateways	Cloud-Based Security Services Database Audit and Protection DMZ Virtualization Network Security Silicon Penetration Testing Tools Software Composition Analysis Web Application Firewalls	Application Shielding Dynamic Data Masking Interoperable Storage Encryption	
low	Network IPS	Hypervisor Security Protection	Open-Source Security Tools Security in the Switch	

As of July 2014

Source: Gartner (July 2014)

UNIVERSITY OF WATERLOO

CCIRC ADVICE

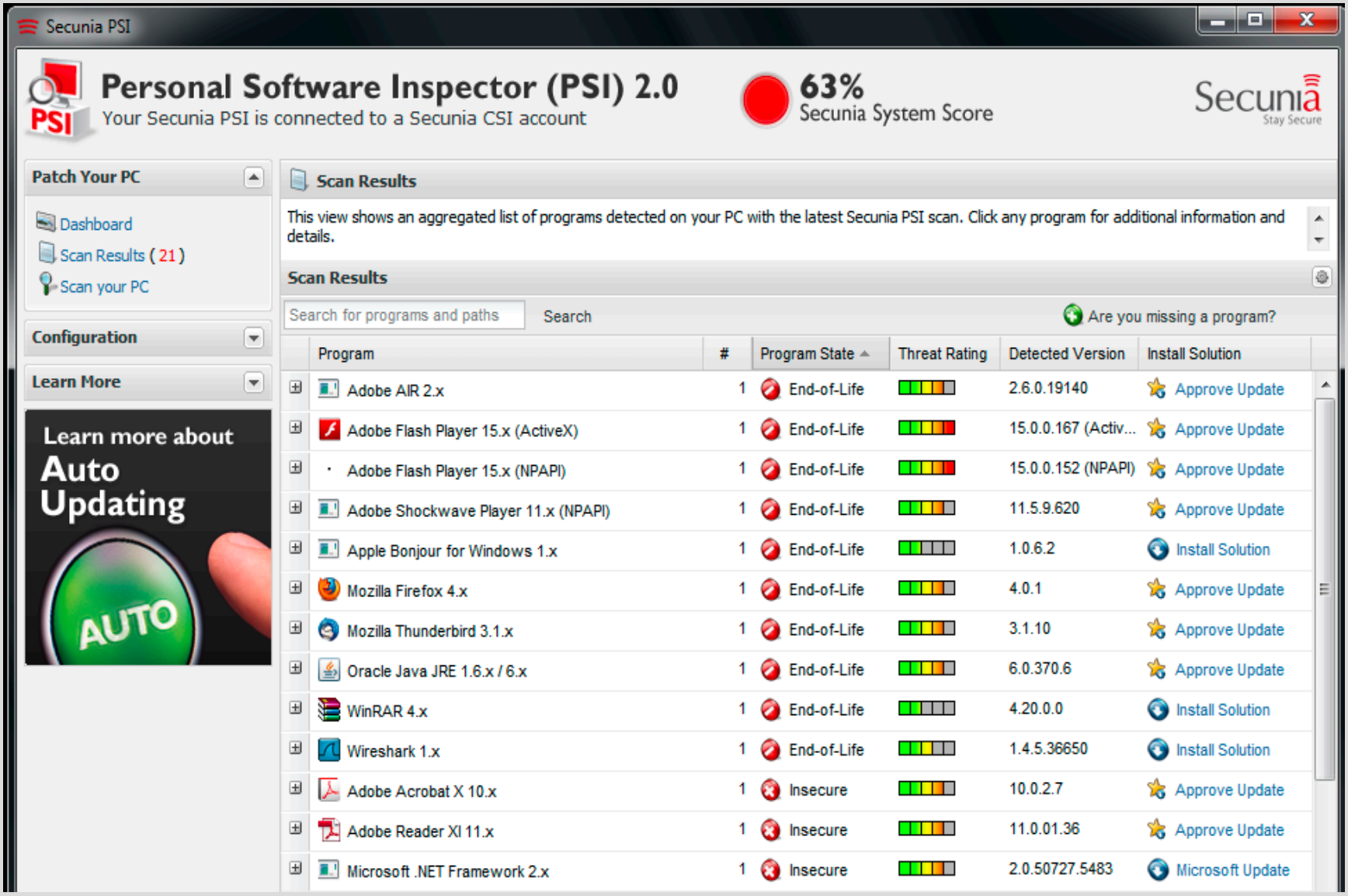
Top 4 Strategies to Mitigate Targeted Cyber Intrusions

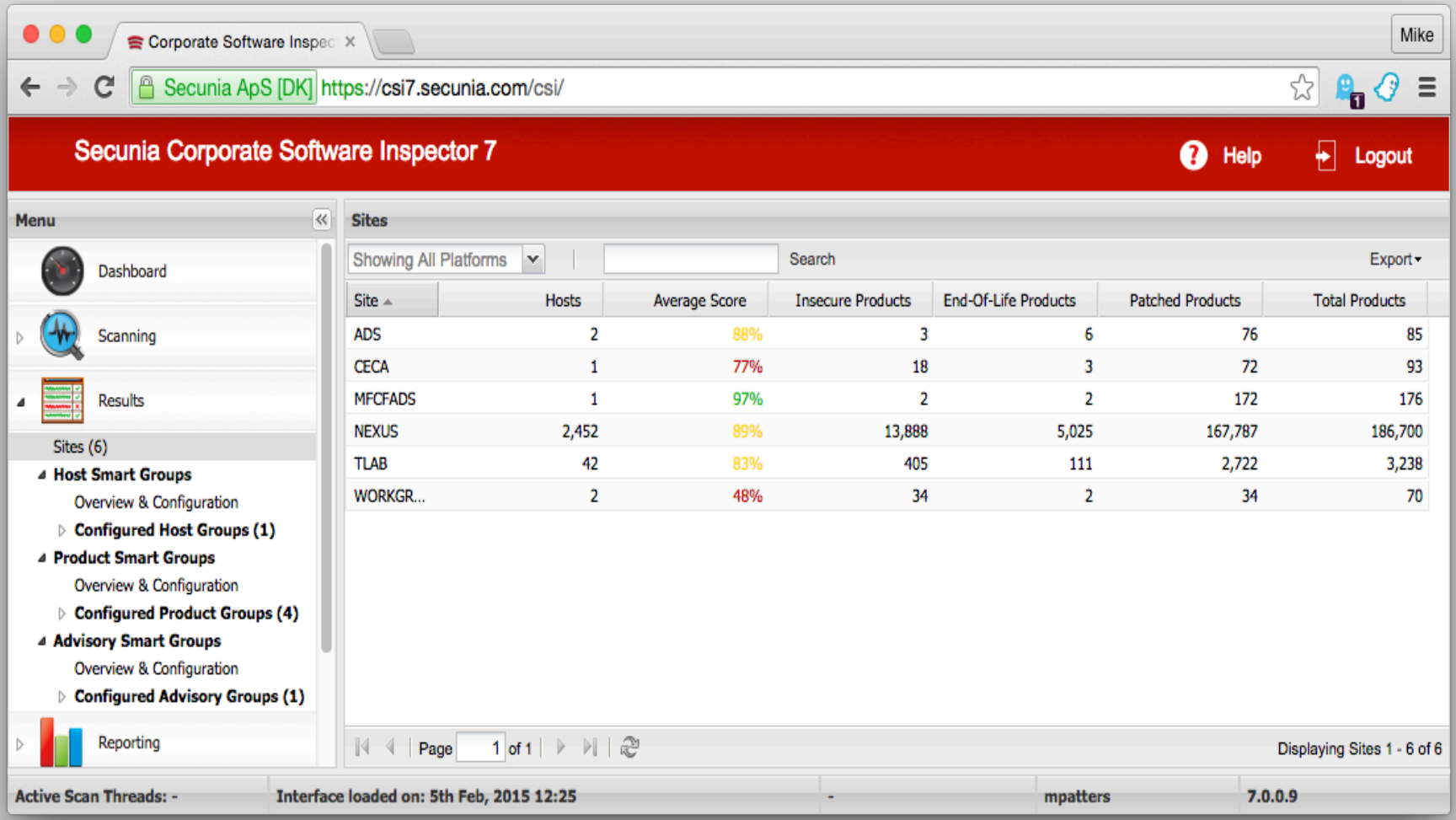
The Canadian Cyber Incident Response Centre (CCIRC) recommends that network administrators implement the following four mitigation strategies, which can prevent as much as 85% of targeted cyber attacks:

Ranking	Mitigation Strategy	Rationale
1	Use **application whitelisting** to help prevent malicious software and unapproved programs from running.	Application whitelisting is one of the best security strategies as it allows only specified programs to run, while blocking all others, including malicious software.
2	**Patch applications** such as Java, PDF viewers, Flash, web browsers and Microsoft Office.	Vulnerable applications and operating systems are the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
3	**Patch operating system** vulnerabilities.	
4	**Restrict administrative privileges** to operating systems and applications based on user duties.	Restricting these privileges may prevent malware from running or limit its capability to spread through the network.

This list of mitigation strategies has broad international consensus and is considered network cyber security fundamentals. These strategies have been endorsed by the Government of Canada, including CCIRC and the Communications Security Establishment Canada. The "Top 4" also underpin CCIRC's Mitigation Guidelines for Advanced Persistent Threats.

UNIVERSITY OF WATERLOO


Secunia PSI
Personal Software Inspector (PSI) 2.0
Your Secunia PSI is connected to a Secunia CSI account
63%
Secunia System Score
Secunia
Stay Secure
Patch Your PC
Dashboard
Scan Results (21)
Scan your PC
Configuration
Learn More
Learn more about
Auto
Updating
AUTO
Scan Results
This view shows an aggregated list of programs detected on your PC with the latest Secunia PSI scan. Click any program for additional information and details.
Scan Results
Search for programs and paths
Search
Are you missing a program?
Program
#
Program State
Threat Rating
Detected Version
Install Solution
Adobe AIR 2.x 1 End-of-Life 2.6.0.19140 Approve Update
Adobe Flash Player 15.x (ActiveX) 1 End-of-Life 15.0.0.167 (Activ... Approve Update
Adobe Flash Player 15.x (NPAPI) 1 End-of-Life 15.0.0.152 (NPAPI) Approve Update
Adobe Shockwave Player 11.x (NPAPI) 1 End-of-Life 11.5.9.620 Approve Update
Apple Bonjour for Windows 1.x 1 End-of-Life 1.0.6.2 Install Solution
Mozilla Firefox 4.x 1 End-of-Life 4.0.1 Approve Update
Mozilla Thunderbird 3.1.x 1 End-of-Life 3.1.10 Approve Update
Oracle Java JRE 1.6.x / 6.x 1 End-of-Life 6.0.370.6 Approve Update
WinRAR 4.x 1 End-of-Life 4.20.0.0 Install Solution
Wireshark 1.x 1 End-of-Life 1.4.5.36650 Install Solution
Adobe Acrobat X 10.x 1 Insecure 10.0.2.7 Approve Update
Adobe Reader XI 11.x 1 Insecure 11.0.01.36 Approve Update
Microsoft .NET Framework 2.x 1 Insecure 2.0.50727.5483 Microsoft Update



UNIVERSITY OF WATERLOO

JAN 2015 MEETING TOPICS COVERED

- Introduction of Brad Krane, Adam Savage
- Deployment update (podium)
- Technology selection criteria
- Are we really getting our money's worth with SEP?
- Contents of report back to CTSC
- https://uwaterloo.ca/information-systems-technology/about/organizational-structure/information-security-services/wnag-ep-subgroup-meetings

FORMAL REPORT BACK TO CTSC: TOPICS

- Concerns related to moving away from SEP for general users
- Advice to FACCUS with respect to a/v for students
- Recommendations/requirements for deployment strategies, regardless of technology

TO RFP OR NOT TO RFP?

- No: 5
- Yes: 3
- Abstain: 3

REMINDER OF: QUESTIONS FOR CTSC

Does campus:

- Rely on off-host protection exclusively
- Combine on-host protection with off-host
- All-in with on-host protection
- All-in on vendor “single pane of glass” type solutions

And does it need to be one size fits all?

Also, work-from-home?