



Security Hygiene

Be in a defensible position.

Be cyber resilient.

November 8th, 2017



Agenda

Getting defensive

How will we do it?

Basic hygiene stuff

Getting started

Questions



Introductions



Guy Rosario
Manager, KPMG
Office: (250) 480-3608
grosario@kpmg.ca

- Over 20 years Cybersecurity experience
- Vice-President, ISACA Victoria Chapter
- Manager, IT Advisory and Cyber Security
- Local cyber security SME (TV, Radio, public courses, etc.)

Getting defensive

- We're going to talk about getting here
- Why are we going to do it?
 - Often the basics aren't done
- Here's some examples:
 - Network
 - Social Engineering, etc.



How will we do it?

Finding and maintaining a Cyber defensible position

Link the three most frequently asked questions on Cyber security to an organization's maturity for preventing, detecting & reacting to Cyber security incidents

Questions	Impact	Phase	Defensible position status	Typical action
1. Where are we regarding cyber security	<ul style="list-style-type: none"> Identify business specific cyber risks & threats Identify compliance requirements (legal & regulatory) Identify "crown jewel" data 	Assessment	None	<ul style="list-style-type: none"> Basic hygiene and compliance Cyber maturity assessment / cyber security review Red teaming+ Proactive breach compromise assessment
2. Where do we want to be regarding cyber security?	<ul style="list-style-type: none"> Complete a business impact assessment Complete a gap assessment 	GAP analysis & facilitated discussion	Defined	<ul style="list-style-type: none"> Facilitated discussion to consciously accept or remediate risks
3. How do we get there?	<ul style="list-style-type: none"> Sign off budget Decide on metrics to track progress (KPIs) 	Cyber security strategy & transformation program	Plan created	<ul style="list-style-type: none"> Cyber security strategy & transformation plan
Execute & verify progress (ongoing)			Achieved	<ul style="list-style-type: none"> Delivery of a risk based security programs & ongoing assessments

Basic hygiene stuff...

- Cybersecurity is recognized by the executives?
- InfoSec roles are identified and assigned?
- Critical Systems and Data are identified?
- Risks appetite and Risk register is regularly reviewed?
- Security assessments are done on a regular basis for new and existing systems?

Basic hygiene stuff... (cont'd)

- What if I told you, the first part is done.
 - You just need to get it in writing from the Executives?
 - Don't have the docs?.. No worries
 - Don't know how to actually do it?.. We have it covered.
 - Don't have the time for it?..
 - It can be initially built in a day
 - Automated in a week!

Basic hygiene stuff... (cont'd)

– Windows

- SCCM

- PowerShell

- Python (for Windows 10)

– Linux

- Bash

- Python

Module Logging:

- Logs PS pipeline execution details during execution...

Script Block Logging:

Full Transcription Logging:

A great article that walks you through this is:

- PowerShell Logging for the Blue Team

-— <http://www.blackhillsinfosec.com/?p=5516>

Other logging options some might use:

- Commercial

- Free(-ish)

- ⊕.....— Splunk

- ⊕.....— SRUM (Windows System Resource Usage Monitor)

Basic hygiene stuff... (cont'd)

– Windows

- SCCM

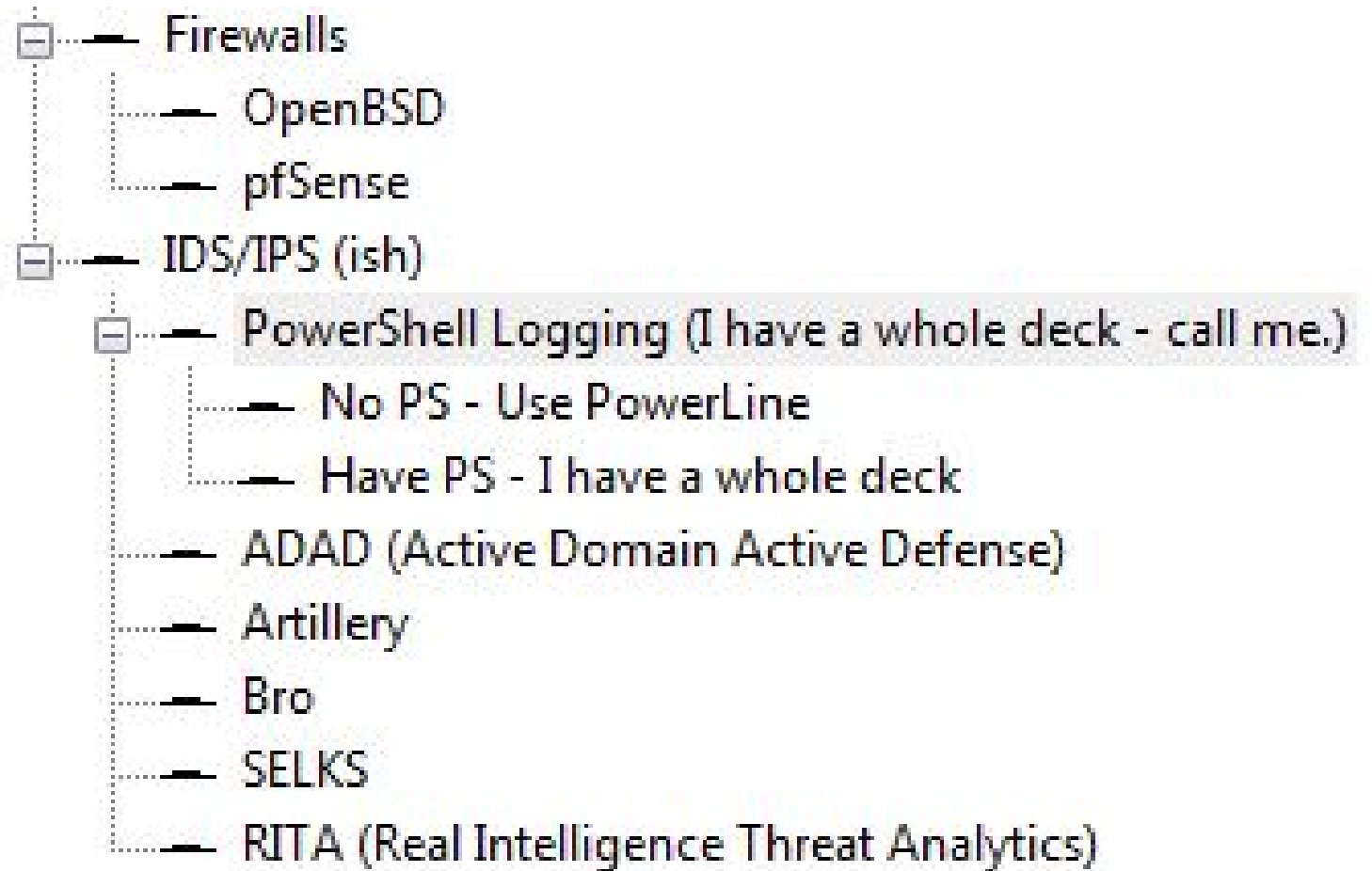
- PowerShell

- Python (for Windows 10)

– Linux

- Bash

- Python



Getting started...

– There are best practices and policies from:

– The Canadian Government

– CERT

– CIS(SANS) Top 20

– ISACA

– ISO

– NIST

– SANS

 Acceptable Use Policy.docx

 acceptable_encryption_policy.docx

 acquisition_assessment_policy.docx

 bluetooth_baseline_requirements_policy.docx

 clean_desk_policy.docx

 data_breach_response.docx

 database_credentials_policy.docx

 digital_signature_acceptance_policy.docx

 disaster_recovery_plan_policy.docx

 email_policy.docx

 end_user_encryption_key_protection_policy.docx

 security_response_plan_policy.docx

 server_security_policy.docx

 software_installation_policy.docx

 technology_equipment_disposal_policy.docx

 web_application_security_policy.docx

 wireless_communication_policy.docx

 wireless_communication_standard.docx

 workstation_security_for_hipaa_policy.docx

Getting started... (cont'd)

- Readily configured:

- IDS/IPS

- ADHD and BRO

- Asset and Inventory

- Management

- PowerShell, CMD.EXE, Python, BASH, etc.

- Vulnerability Scanners

- OpenVAS and NMAP

- Logging and Monitoring Systems

- Backup and Recovery Systems

- Readily downloadable:

- Policy templates

- Best Practices and Standards



Questions?





Thank you

KPMG's Cyber Team works with organizations to prevent, detect and respond to cyber threats.

We can help your organization be cyber resilient in the face of challenging conditions.

Contact us



Guy Rosario
Manager, Cyber Security
T: 250 589 2538
E: grosario@kpmg.ca



kpmg.ca/cyber



© 2017 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.