KPMG

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

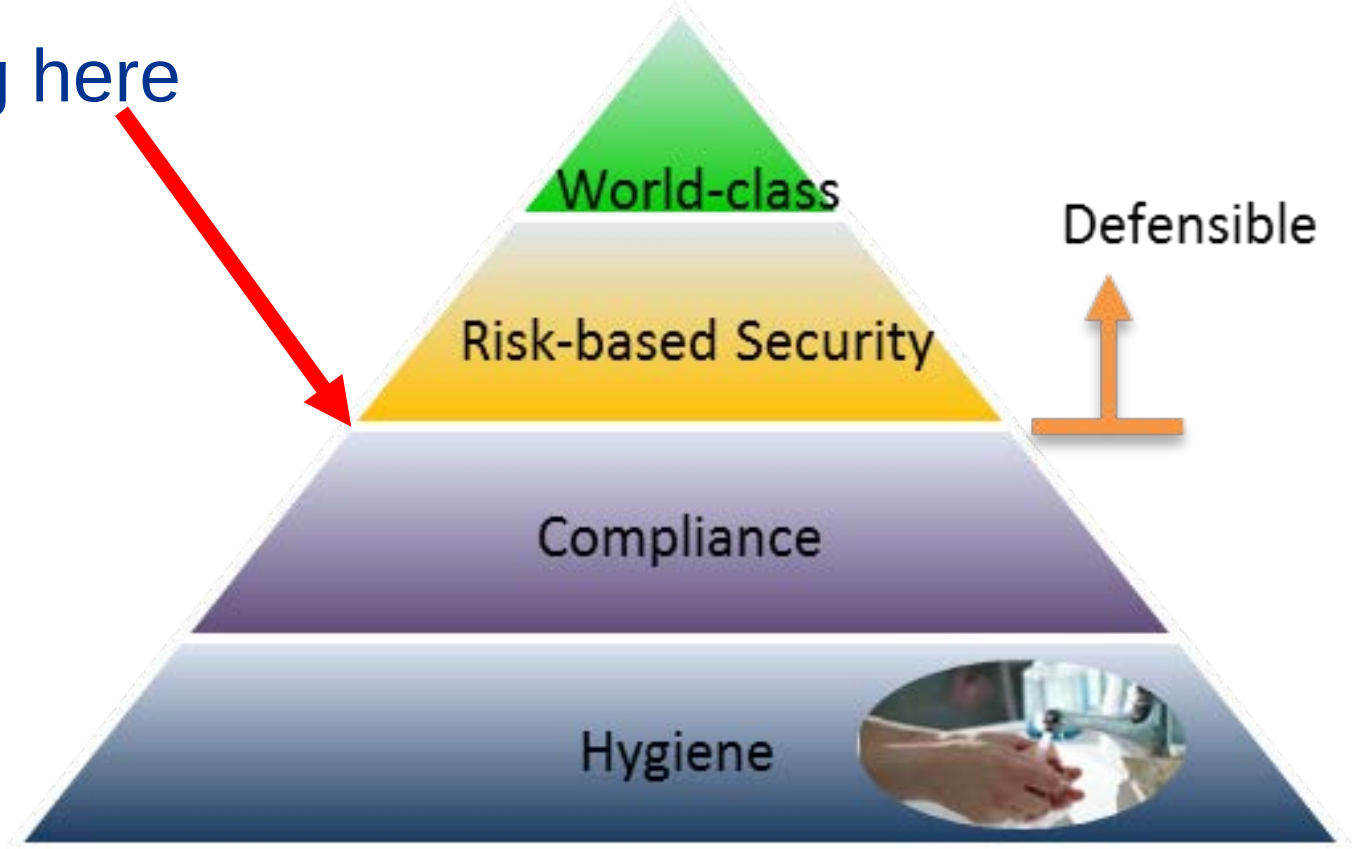
Introductions

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	▪ Identify business specific cyber risks & threats ▪ Identify compliance requirements (legal & regulatory) ▪ Identify "crown jewel" data	Assessment	**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?	▪ Complete a business impact assessment ▪ Complete a gap assessment	GAP analysis & facilitated discussion	**Defined**	▪ Facilitated discussion to consciously accept or remediate risks
3.How do we get there?	▪ Sign off budget ▪ Decide on metrics to track progress (KPIs)	Cyber security strategy & transformation program	**Plan created**	▪ Cyber security strategy & transformation plan
Execute & verify progress (ongoing)			**Achieved**	▪ **Delivery of a risk based security programs & ongoing assessments**

Basic hygiene stuff...

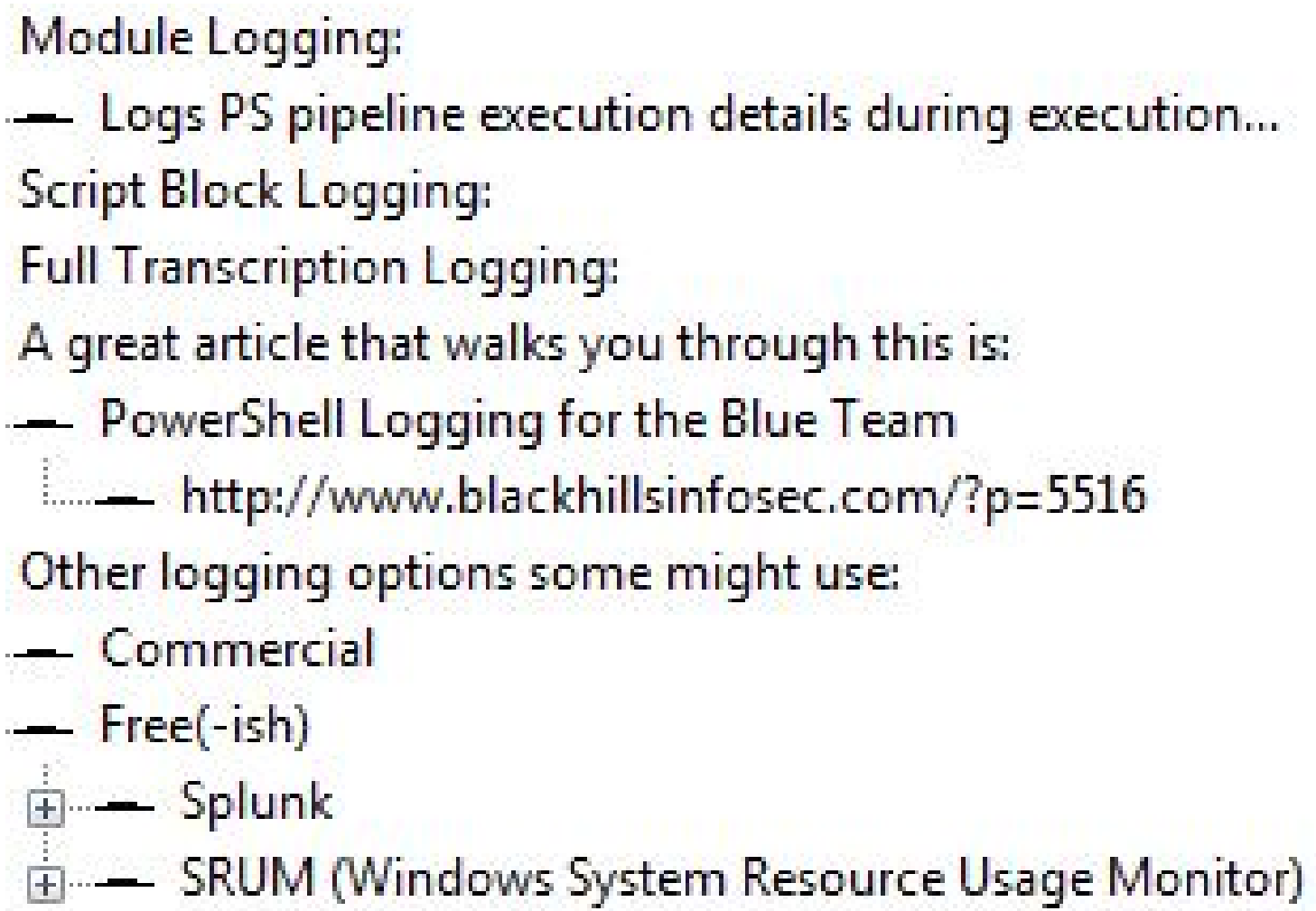
- Cybersecurity is recognized by the executives?
- InfoSec roles are identified and assigned?
- Critical Systems and Data are identified?
- Risks appetite and Risk register is regularly reviewed?
- Security assessments are done on a regular basis for new and existing systems?

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!

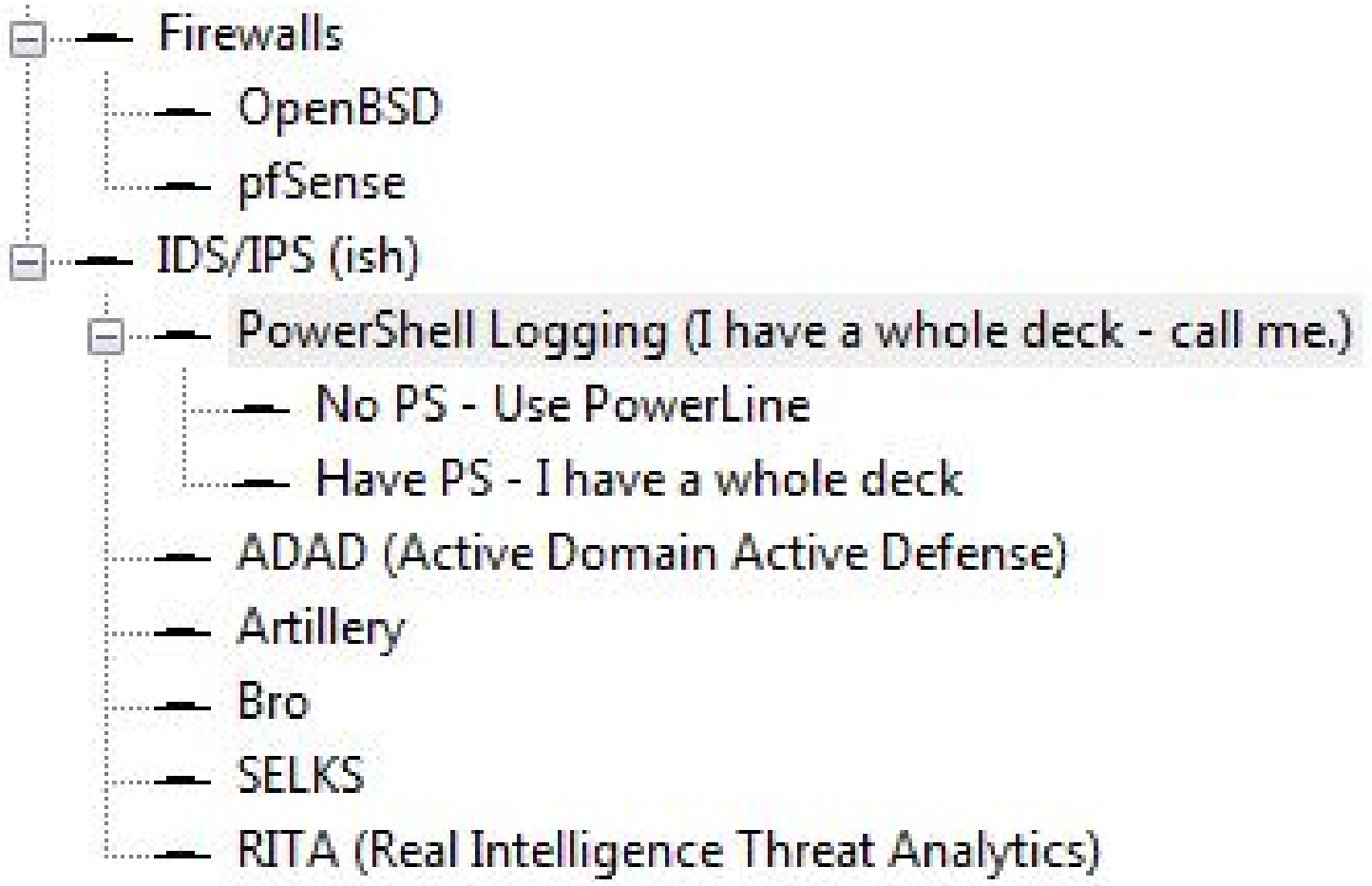
Basic hygiene stuff… (cont'd)

- Windows
  - SCCM
  - PowerShell
  - Python (for Windows 10)
- Linux
  - Bash
  - Python



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

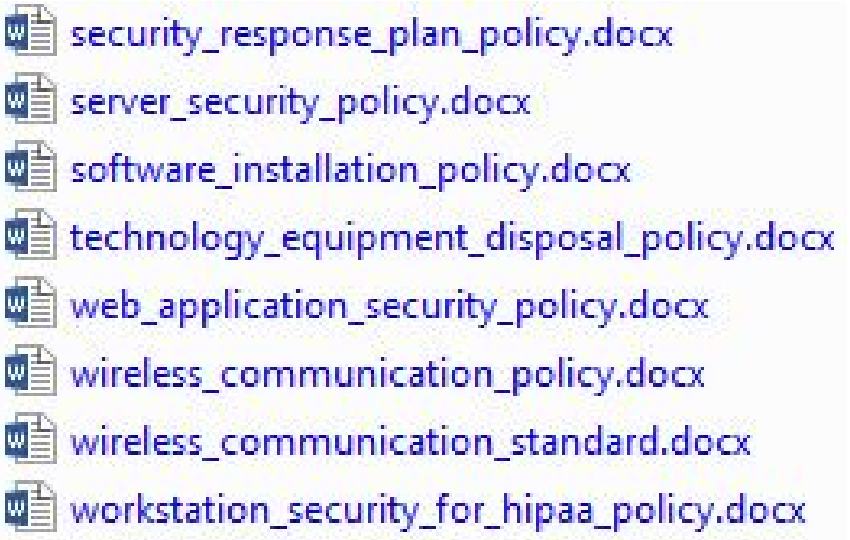
  – CIS(SANS) Top 20

  – ISACA

  – ISO

  – NIST

  – SANS



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


KPMG
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