Australian Information Security Association

LESSONS LEARNT FROM DOING INCIDENT RESPONSE IN THE CLOUD AND RED TEAM EXERCISES AGAINST MSSPS

BENJAMIN MOSSE

Thursday, July 28th, 2016

MOSSÉ SECURITY
THREAT MATTERS

About Me

- CEO of Mossé Security
- Founder of Mossé Cyber Security Institute - Melbourne
- +30,000 machines compromised during penetration testing
- +300 penetration tests delivered
- +100 incidents responded
- +150 security advisories published

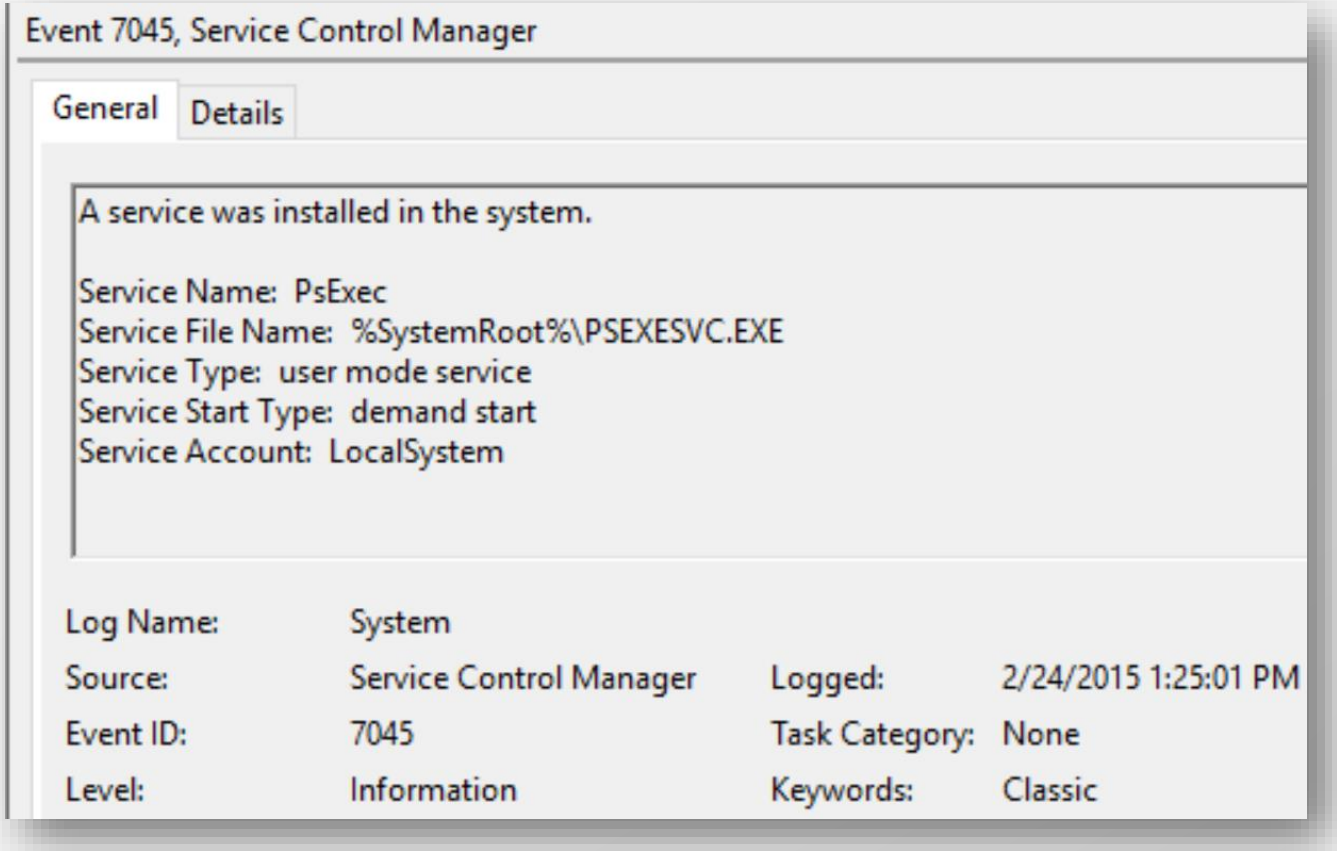
The Mossé Security team has compromised +100,000 machines during engagements.

Key Points

Conclusions and Observations:

1. No evidence that moving to the cloud (IaaS) improved our clients' defences.
2. Cloud providers face the same security challenges as other organisations and showed no better at solving them.
3. Our analysis concludes that the major security challenges faced in the cloud, and elsewhere, are related to the current maturity of our industry rather than an allocation of resources.

Case Study 1: PSEXEC as a Service



As a result of this incident the client moved to another cloud provider.

Context:

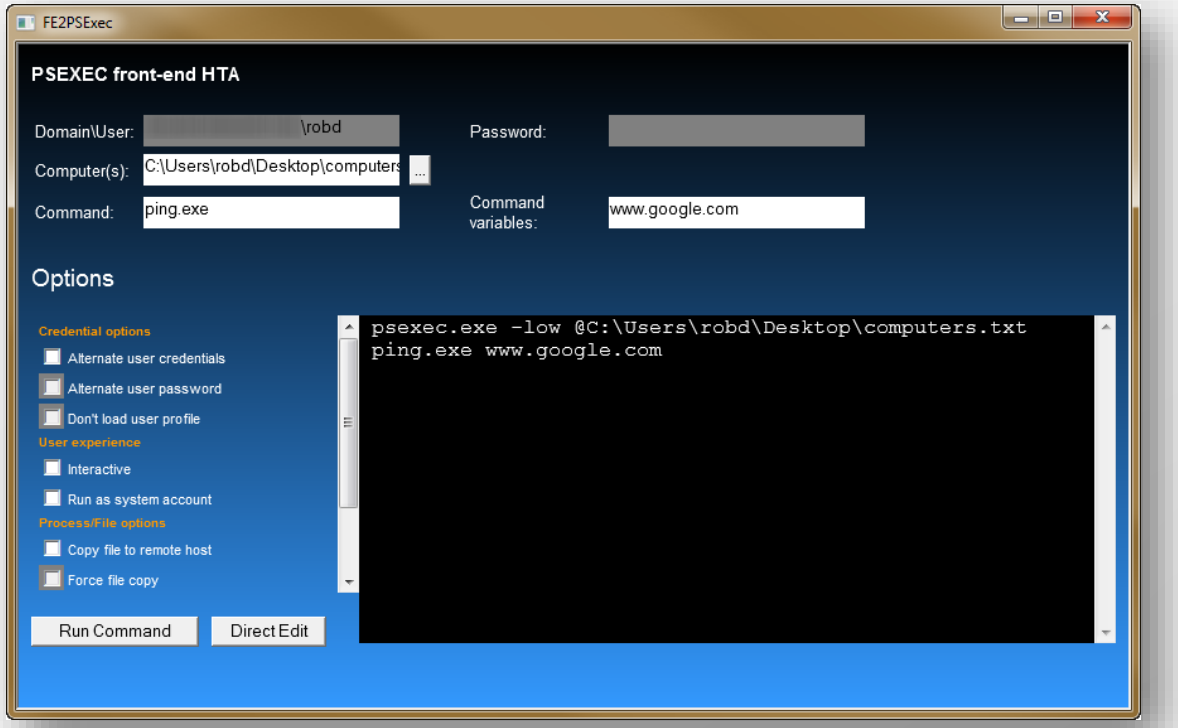
- Mosse Security responded to an security attack for a major Australian brand in 2015.
- The client, had outsourced their web infrastructure to a major IaaS company.

Discoveries:

The cloud provider,

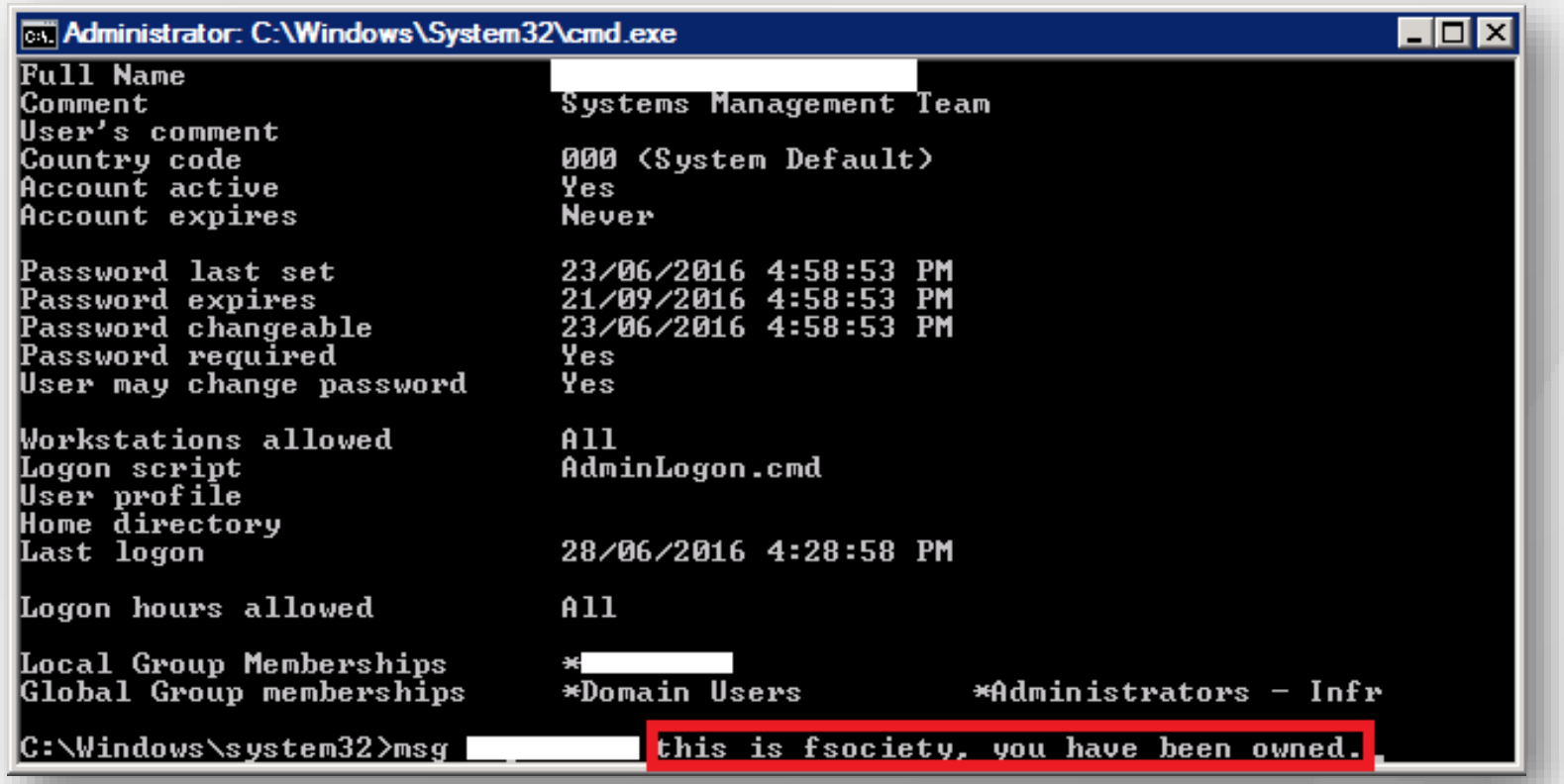
- Only kept security event logs for 24 hours
- Could not confirm whether it was them or the attackers that used PSEXEC
- Took over 12 hours to respond to incident response queries
- Could not provide VMDKs for digital forensics analysis

Case Study 1: PSEXEC as a Service (cont.)



- PSEXEC is a tool to execute commands and binaries to remote machines.
- It is provided and maintained by Microsoft. Although, *the official method to remotely administer machines is using WMI and WinRM*.
- PSEXEC is also:
  - Used by Metasploit
  - Available in all the pentesting toolkits
  - Used by all the script kiddies
  - Used by Chinese APT threat actors
  - Flagged by most anti-virus as dangerous
- Any organisation serious about security will ensure that PSEXEC is not used across the environment.

Case Study 2: FSOCIETY Is On Your Network



We get engaged to test cloud provider's incident response capabilities.

In many cases, they didn't have any.

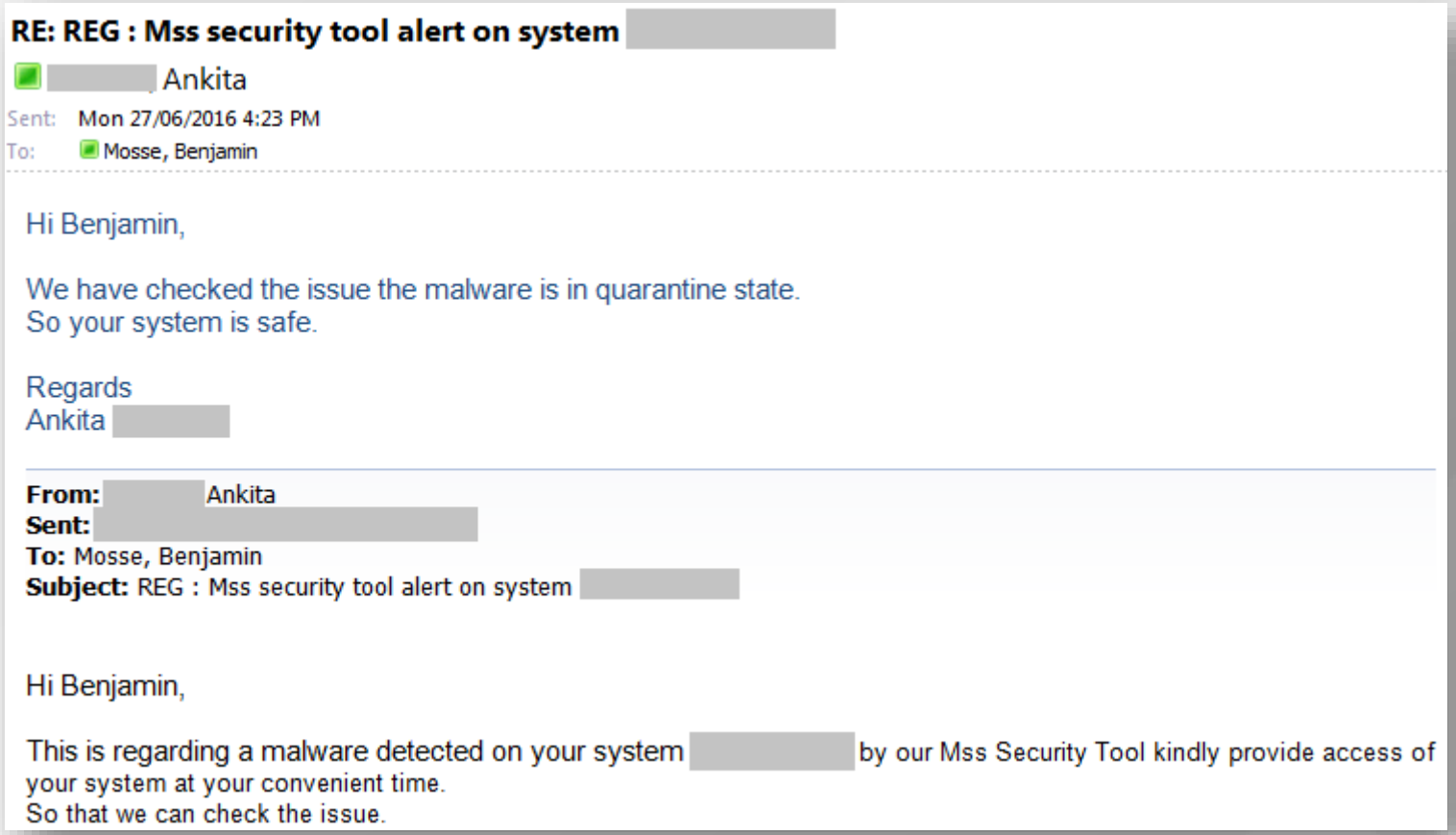
Case Study 3: MSSPs Not Detecting Mimikatz

```
Using 'tacticalkatz.log' for logfile : OK

tacticalkatz # lsadump::lsa /patch
Domain : XXXXXXXXXX / S-1-5-21-1220945662-823518204-XXXXXXXXX

RID  : 000001f4 (500)
User : XXXXXXXX
LM   :
NTLM : 5ed08e20674366270db30e92fbXXXXXX

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 0d51722cbe3e701894168f3f20XXXXXX

RID  : 0000046b (1131)
User : XXXXXXXX
LM   :
NTLM : c5dc4b276bfac3f1e01e693c04XXXXXX
```

We disabled the anti-virus and ran a password dumper 5 times in 12 months on a client's domain controller.

And their managed security service provider did not catch on once.

Case Study 4: MSSPs Do Not Understand Attackers



RE: REG : Mss security tool alert on system [redacted]

[redacted] Ankita

Sent: Mon 27/06/2016 4:23 PM

To: Mosse, Benjamin

Hi Benjamin,

We have checked the issue the malware is in quarantine state.
So your system is safe.

Regards
Ankita [redacted]

From: [redacted] Ankita
Sent: [redacted]
To: Mosse, Benjamin
Subject: REG : Mss security tool alert on system [redacted]

Hi Benjamin,

This is regarding a malware detected on your system [redacted] by our Mss Security Tool kindly provide access of your system at your convenient time.
So that we can check the issue.

We downloaded known APT binaries onto a client's workstation.

The MSSP's anti-virus detected and quarantined the malware. However, the person reviewing the incident failed to understand that this malware represented important threat actors.

Case Study 5: Weak Passwords

Happy administrator credentials!

- Administrator:Administrator
- Username:Username
- Default Passwords
- The word “password”
- Welcome1
- password1

Observation

After conducting a combination of over 100 incident response and attack simulation engagements against cloud providers and MSSPs:

We cannot conclude that outsourcing the I.T security function to a third party improved our clients' security posture.

Third Party Providers Face The Same Challenges As Everyone Else

Not enough people

Not enough security training

Outdated security strategies

Security is solely tactical not strategical

Not enough assurance is provided

Our Professional Opinion

We don’t think those results reflect negatively on the cloud providers.

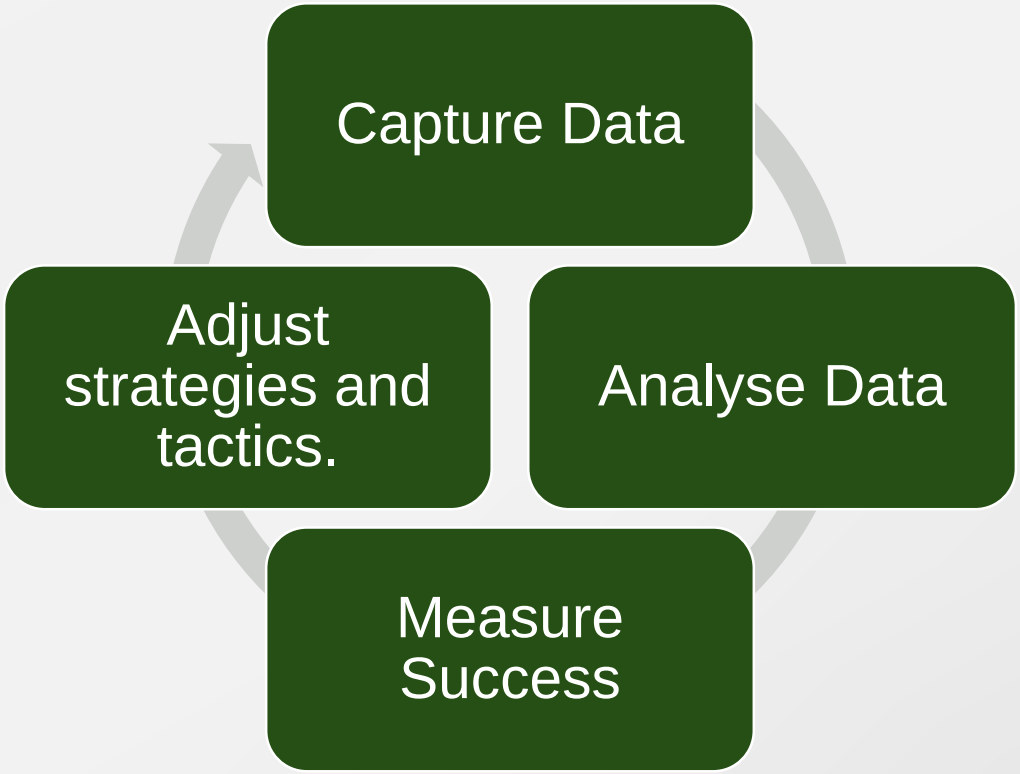
Instead, we believe that they reflect the challenges that our industry is facing today.

Let’s Engage in the Real Talk.

The progressive conversation to have is:

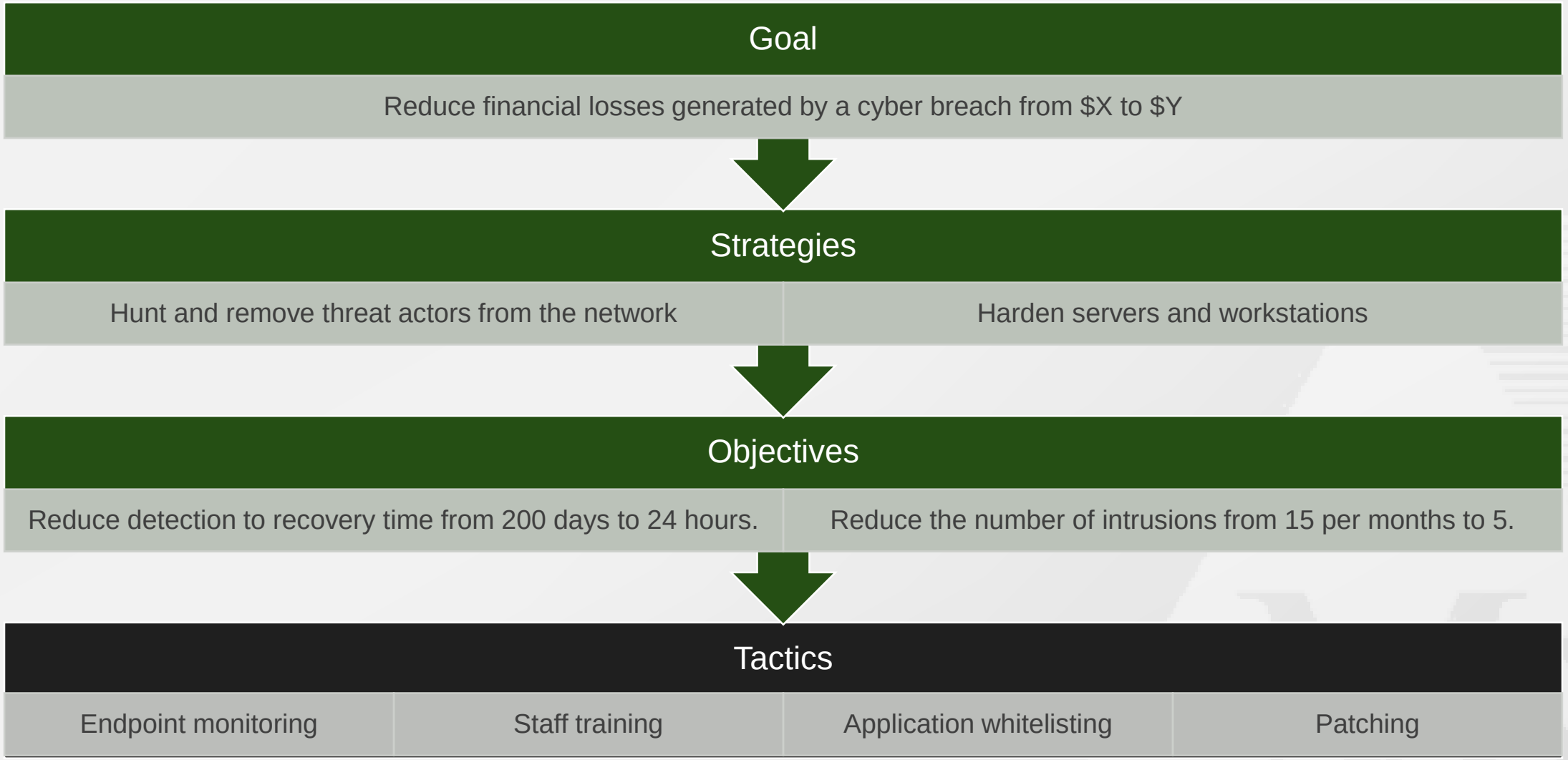
What changes are we proposing to help our industry address all the challenges mentioned in this presentation?

Proposition 1: Data Driven Security.



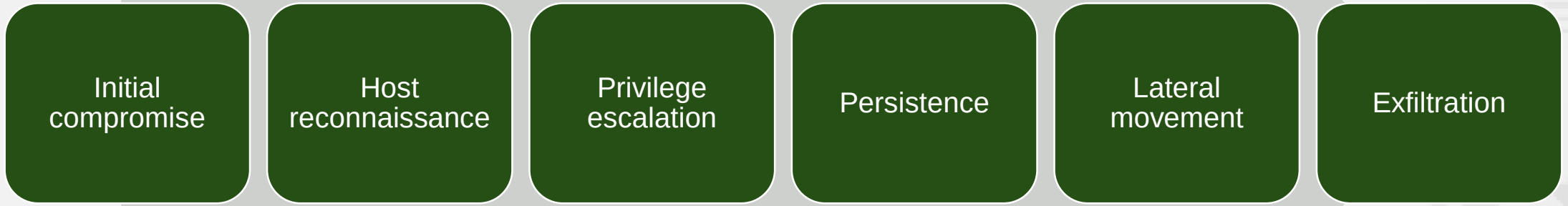
Examples of Measurable Objectives
Reduce financial losses generated from cyber breaches from $X to $Y
Reduce the number of intrusions into our network from X to Y over period Z
Reduce average time from detection to recovery from X days to Y hours

Proposition 2: Be More Strategical Than Tactical



Proposition 3: Scenario Driven Testing

1. Simulate full kill chain attacks against your networks across a wide range of threat actors:
   - Organised criminals
   - Nation states
   - Ransomwares
   - Basic malware and script kiddies
2. Measure success of stopping attackers before the last step of the kill chain.
3. Test 24 hours by 7 and all year round.



Proposition 4: Invest in People

Skill shortage is our industry's greatest challenge.

Help us solve it!

Proposition 5: Bring More Honesty Into Our Industry

Infosec is a sham: The reality of IT security

Op-ed. Infosec numbers don't add up: we need better training, standards, accountability.

by Rupert Goodwins - Jun 9, 2016 7:16pm AEST

http://arstechnica.co.uk/security/2016/06/infosec-is-broken-how-to-fix-it/

CONTACT US

Benjamin Mossé, CEO

Mossé Security

Mossé Cyber Security Institute

1300 730 035

contact@mosse-security.com

MOSSÉ SECURITY
THREAT MATTERS