Compromised?

Paul Black – Asia Pacific & Japan, Incident Response
Victor Law – Greater China Region, Enterprise Security

Compromise

It will happen

No longer an if - but when

Detection takes too long

229 - Average number of days to discover a breach

Not enough skills

70% of organizations lack staff to counter cyber security threats

Time is money

Big money

Key Themes

Targeted Attacks

Targeted Attacks Shifted from Economic Espionage to Politically Motivated Sabotage and Subversion

Cyber Bank Heists

Attackers Chase the Big Scores, Bigger Ambitions and is Targeting Banks

Internet of Things

Cyber Criminals Harnessed the Processing Power of IoT Devices to Fuel Zombie Army of Devices

Ransomware

Ransomware Squeezing Victims with Escalating Demands

Macros, IT tools & Malware

Attackers Weaponized Commonly Used Software

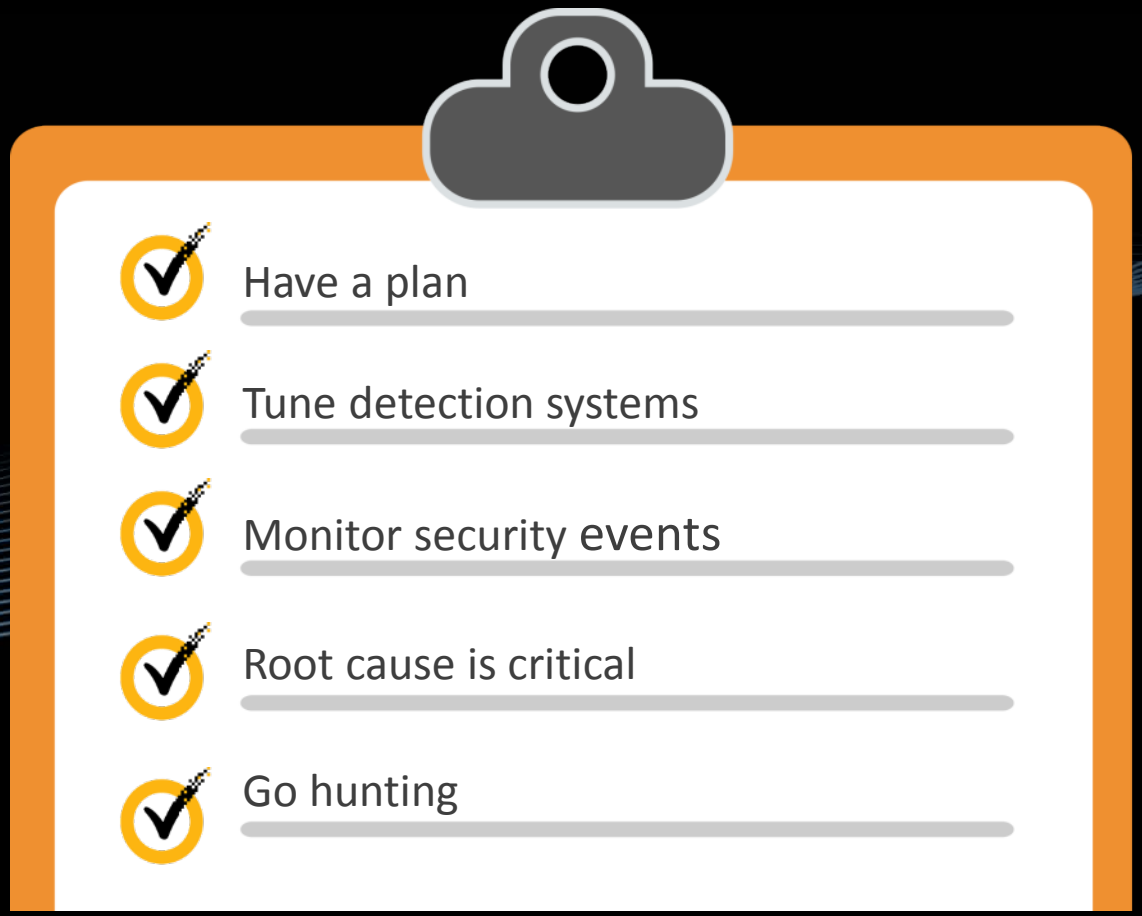
Email

Email Became the Weapon of Choice

Cloud

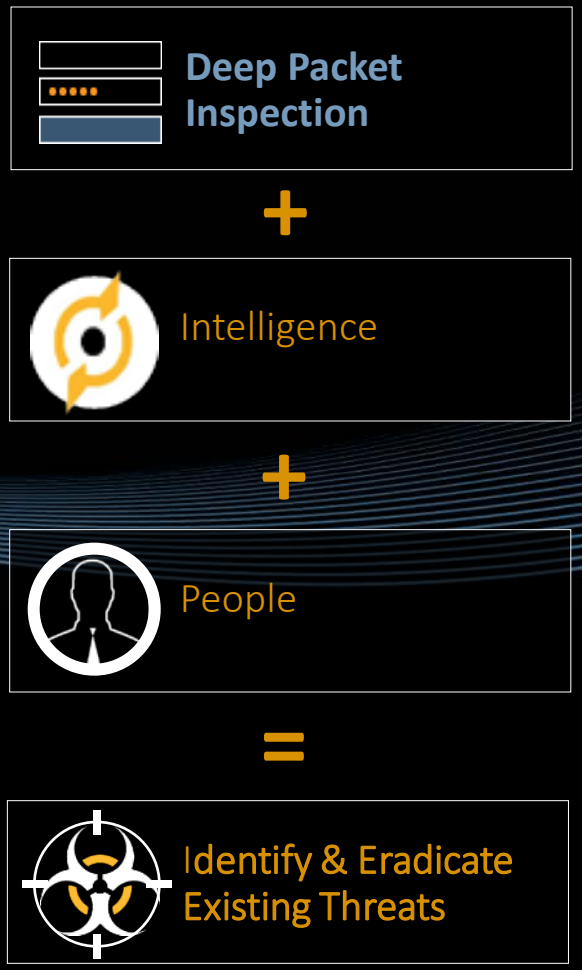
Cracks in the Cloud: The Next Frontier of Cybercrime is Upon Us

Quick Wins


Have a plan
Tune detection systems
Monitor security events
Root cause is critical
Go hunting

Go Hunting

Advanced Threat Hunting



Preventive Incident Response

Regularly hunting for threats helps to establish a consistent, known secure state for your network.

Don’t Wait For an Incident

Identify and **eradicate** existing compromises before they become a major data breach.

Reduce Breach Response Costs

Compromises are common and inexpensive to remediate.

Identify threats early to avoid high incident response costs.

Copyright © 2017 Symantec Corporation

The Importance of Root Cause

Infection vectors don’t change between commodity malware and targeted attacks

Know impact and intent, understand the risk and mitigate appropriately

Strengthen detection and prevention as an outcome of every qualified incident

Build trending and metrics into incident reporting

Use actual incident data to drive security awareness

Quick Wins


Educate users
Enforce complex passwords
Force password rotation
Implement 2 factor authentication
Practice incident response

Thank You!