



MIS|TI™ PRESENTS

InfoSecWorld
Conference & Expo 2018

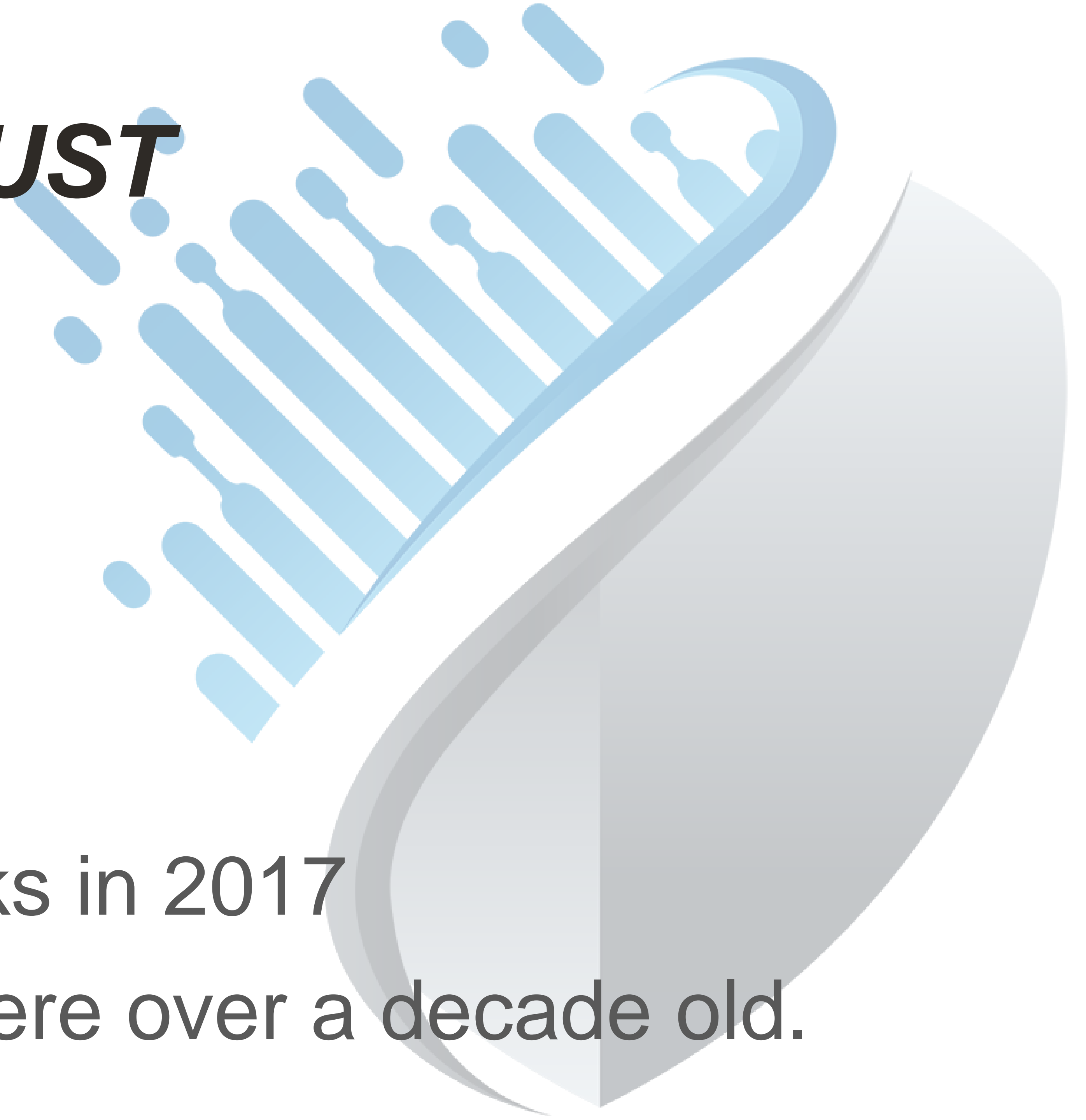
MANAGEMENT MALADIES AND METHODS TO THE MADNESS (MMMM)

Nick Hampson

Regional Director Engineering

***PREVENTION MUST
BE OUR FIRST
PRIORITY***

26% of Cyber Attacks in 2017
used exploits that were over a decade old.



Never-ending Shifts In Your Security Landscape

Scale

More changes more quickly by more unique pieces of the organization driven by

- DevOps
- Continuous Delivery
- Continuous Integration
- Agile Development
- Challenges Team Collaboration - **Security**

More Threats with greater sophistication

- Hackers modify code to **avoid detection**
- Immense growth of **unknown** malware
- Huge Data Breaches, **Ransomware**, APTs
- Most current solutions focused on detection

More Touchpoints

- More devices
 - Consultants
 - Consumers
 - Partner Organizations
- Technology moving further from the core
- Non-corporate assets

Integration of Controls

- Continuous **increase** in attack **entry points** from laptops, tablets, smartphones
- Increasing **de-perimeterisation** challenges
- **Network talking to mobile, endpoint devices and vice-versa** leaves gaping holes in integration

Infrastructure Diversity

- Infrastructure and workloads (**Office 365**) increasingly moving to Cloud
- **Aligning security** with traditional DC, SDDC, IaaS, PaaS, cloud at the same time
- **Different PaaS, IaaS security & controls**
- VM to VM, Inter DC **lateral traffic risks**

Productivity while mitigating risk

Information Security IndustryScape

SECURITY MANAGEMENT AND COMPLIANCE

Managed Security Service Providers



SIEM



Security Training



Governance, Risk and Compliance



INFRASTRUCTURE SECURITY

Data Masking



Enterprise Network Firewalls



Intrusion Prevention Systems



Network Access Control



Unified Threat Management



CYBER SECURITY

Secure Web Gateways



Network Forensics



Threat Intelligence Services



ENDPOINT SECURITY

Secure Email Gateways



Data Loss Prevention



Endpoint Protection & Anti-virus



Endpoint Threat Detection & Response



APPLICATION SECURITY

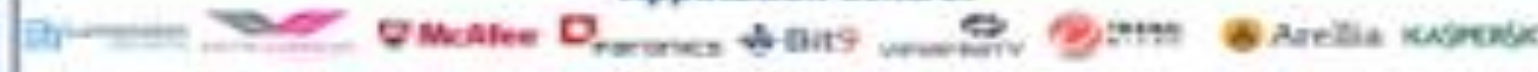
Application Security Testing



Web Application Firewalls



Application Control



CLOUD SECURITY



MOBILE SECURITY



IDENTITY AND ACCESS MANAGEMENT

User Authentication



Identity Governance and Administration



SECURITY PARTNERS

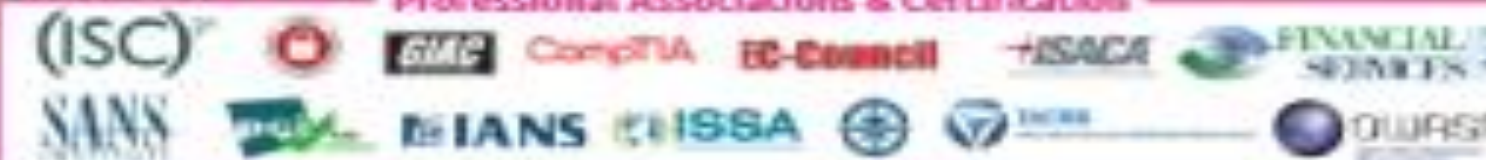


SECURITY ORGANIZATIONS

Education & Academic



Professional Associations & Certification



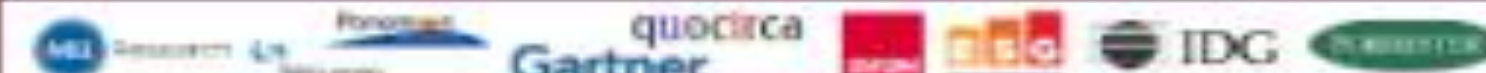
Government











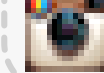


















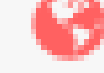



SECURITY CONFERENCES

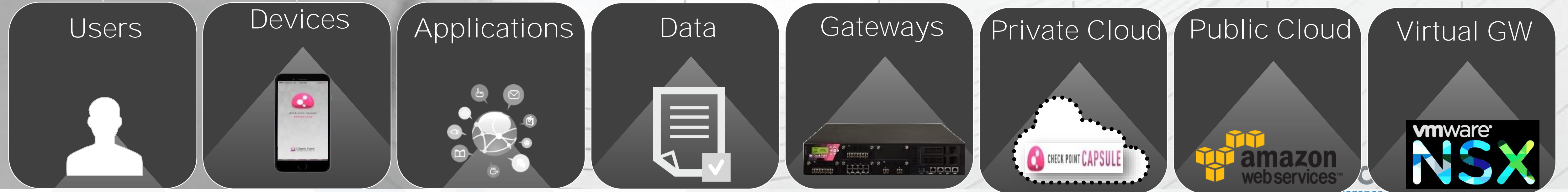


ANALYST HOUSES



OPERATIONS NEED TO BE CONSOLIDATED

Name	Source	Destination	Services & Applications	Data	Action	Install On
Outbound access	 production_net	 Internet	* Any	* Any	 AccessSubLayer	* Policy Targets
Social media for marketing	 marketing_role  John	 Internet	 Twitter  LinkedIn  Instagram	* Any	 Accept	 SG13800
Developers upload	 developer_role	 Internet	 Dropbox  Box	 Any Direction  Source Code - JAVA	 Accept	 SG13800  CapsuleCloud
Access Sensitive Servers	* Any	* Any	* Any	* Any	 SensitiveServers	* Policy Targets
Mobile Access	 Mobile Devices	 MailUS	 MailServer	* Any	 Accept	 Mobile
Access to Web Server	* Any	 WebServer	 https	* Any	 Accept	 AWS  VMWare



Logs

General Overview

Applications and Sites

Threat Prevention

Security Incidents

Security Checkup Summary

Audit Overview

Important Attacks

Application and URL Filtering

Queries

Last 7 Days

Enter search query (Ctrl+F)

Query Syntax

Edit Mode

Add Widget

Redo

Undo

Discard

Done

Low Resolution Mode

Options

Attack Types by Blades

Remove

Add

18 IPS

1 Anti-Bot

14 Anti-Virus

2 Threat Emulation

Activity Timeline

Medium

High

Critical

Logs

Tue 24

Wed 25

Thu 26

Fri 27

Sat 28

Sun 29

Mon 30

Tue 31

Top Attacks

Protection Name	Severity	Blade	Logs
GNU Bash Remote Co...	Critical	IPS	1.3K
MIT Kerberos kadmind...	Critical	IPS	100
Exploited doc document	Critical	Threat Emulati...	74
Exploited pdf document	Critical	Threat Emulati...	24
Backdoor.Win32.Taido...	Critical	Anti-Bot	19
Cisco Unified Commun...	Critical	IPS	12
Microsoft Windows RA...	Critical	IPS	10
Malicious Binary.balmblj	Critical	Anti-Virus	5
MS-SQL Server Sp_repl...	Critical	IPS	4
ShellShock - GNU Bash...	Critical	IPS	4

GEO

- **Understand your risk – look into the traffic (OOB, SPAN, TAP)**

- Evaluate the risk and implement a strategy.
- Patching and patch management tools
- Endpoint controls
- Network controls
- Remote access policy

- **All you work is in the management tool – be nice to it**

- Log what is interesting – what would an audit require?
- SIEM triggers, what's an event?
- Audit your admins. Password complexity, password reuse
- Have a backup – fire drill the backup

- **Have rules when making rules**

- Have a method – understand the grouping



MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THANK YOU

Nick Hampson

nhampson@checkpoint.com