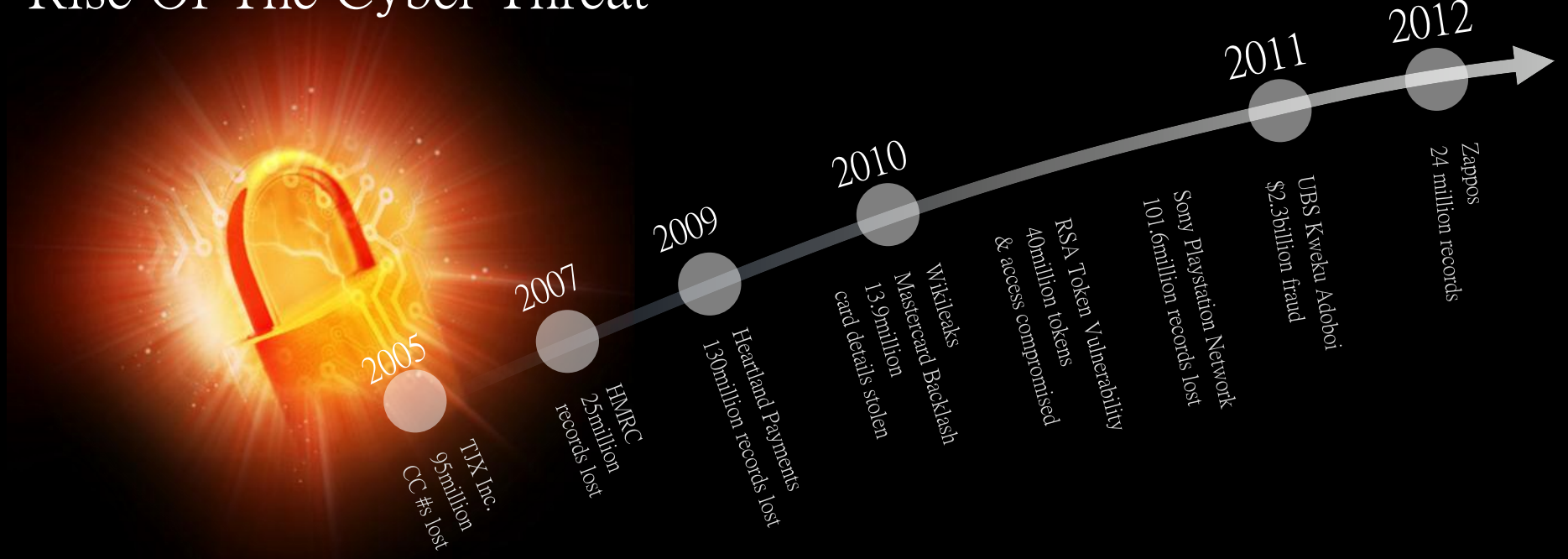
應用SIEM偵測與預防APT緩攻擊

HP Enterprise Security

林傳凱 (C. K. Lin)
Senior Channel PreSales, North Asia
HP ArcSight, Enterprise Security

ENTERPRISE SECURITY

Rise Of The Cyber Threat



Enterprises and Governments are experiencing the most AGGRESSIVE THREAT ENVIRONMENT in the history of information.

Security Awareness at Board Level

Organizational and security leadership is under immense pressure

EXTENDED SUPPLY CHAIN — **44%** OF ALL DATA BREACH INVOLVED 3RD PARTY MISTAKES

CYBER THREAT — **56%** ORGANIZATIONS HAVE BEEN THE TARGET OF A NATION-STATE CYBER ATTACK

INCREASING COST PRESSURES — **11%** OF TOTAL IT BUDGET SPENT ON SECURITY

Source: HP internal data and Forrester Research

Chief Information Security Officer sits at heart of the enterprise security response

Disruptive Technology Trends

COLLABORATIVE
OPEN & EXTENDED

DATA,
INFRASTRUCTURE
& DEVICES

FORTRESS
Reactive Perimeter Security

BIG DATA
Content, Context, Unstructured

CLOUD
Public, Private, Adoption

CONSUMERIZATION
Mobility, Device & Social Media

FUTURE OF SECURITY:

PROACTIVE RISK
MANAGEMENT

Enterprise Security Priorities

- Manage INFORMATION RISK in the era of mobile, cloud, social media
- Protect against increasingly sophisticated CYBER THREATS
- Improve REACTION TIME to security incidents
- Reduce costs and SPEND WISELY
- Achieve COMPLIANCE in a predictable and cost-effective way

The Enterprise Security Problem

BREACHES CONTINUE…
even though they have hundreds of security solutions available

SILO’D SECURITY PRODUCTS…
don’t learn or share information

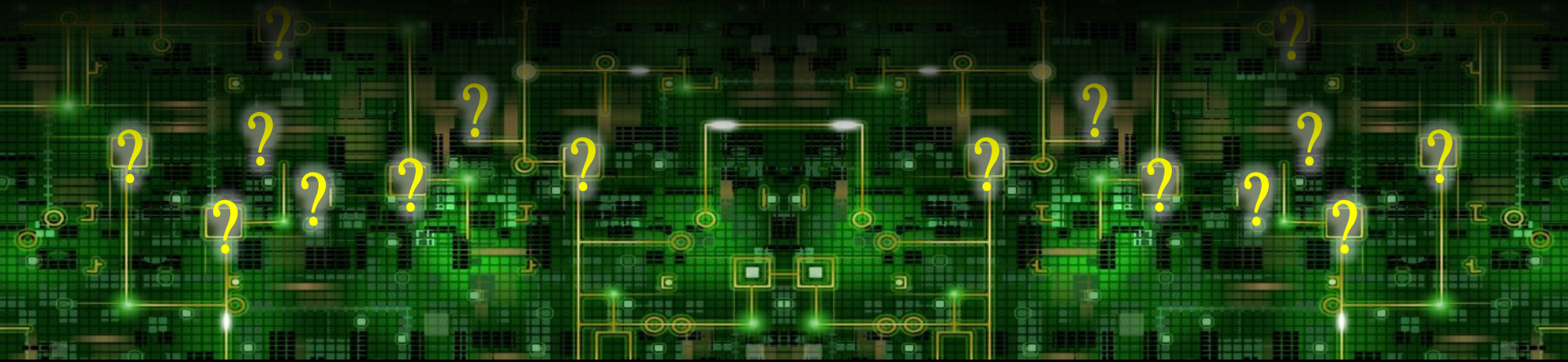
LIMITED CONTEXT…
a gap between IT operations and security constrains potential actions

NO EFFECTIVE WAY…
to understand and prioritize risk

The Result: Increased Risk and Wasted Resources

*Gartner estimates more than $1B in IT spending is misallocated each year because of a lack of business line of sight impact.**

That level of investment is unsustainable.



*Gartner, Business Intelligence for IT: Integrating Operational and Security Intelligence 10/2011

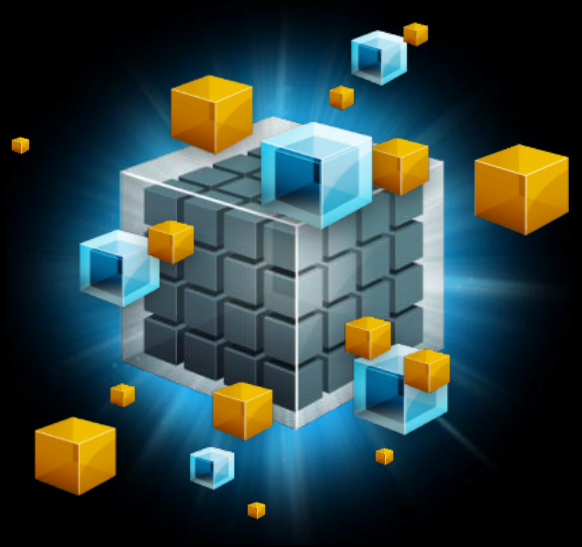
What is APT?

ENTERPRISE SECURITY

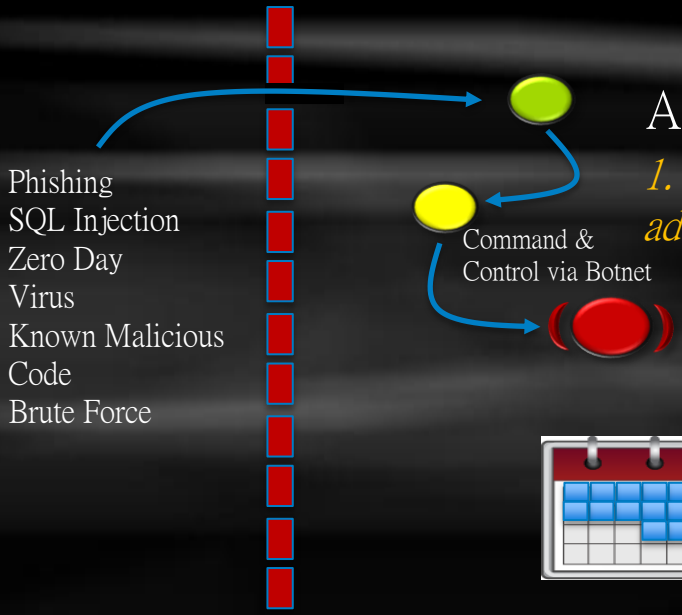
APT Threat Landscape

What is APT?

- Advanced
  - Using exploits for unknown vulnerabilities (Zero Day Attack)
  - Using customized malwares that aren’ t detected by any antivirus or signature based IDS/IPS products
  - Using hybrid attack
- Persistent
  - Attacks lasting for months or years and multi-phases
  - Attackers are dedicated to the targets
- Threat
  - Targeted at specific individuals and groups within an organization, aimed at compromising confidential information
  - Not random attacks



Anatomy of Advanced Persistent Threat (APT)



Acquire target, sneak in, hop around

*1. Penetrate the **perimeter** with relatively advanced techniques*

Get privileged access to critical assets

*2. Expand internal footprint by mimicking **privileged users** & **authorized users***

Conduct the crime for an extended time

*3. Achieve **Persistence***

Intelligent ESP Solutions

ESP Security Intelligence and Operations Solutions

Breach Recovery Solution

HP ArcSight ESM Provides Instant Visibility to….

- Assess the extent of the breach
- Limit & contain the breach to minimize adverse impacts
- Prioritize & expedite remediation activities

HP ArcSight and Operations Management

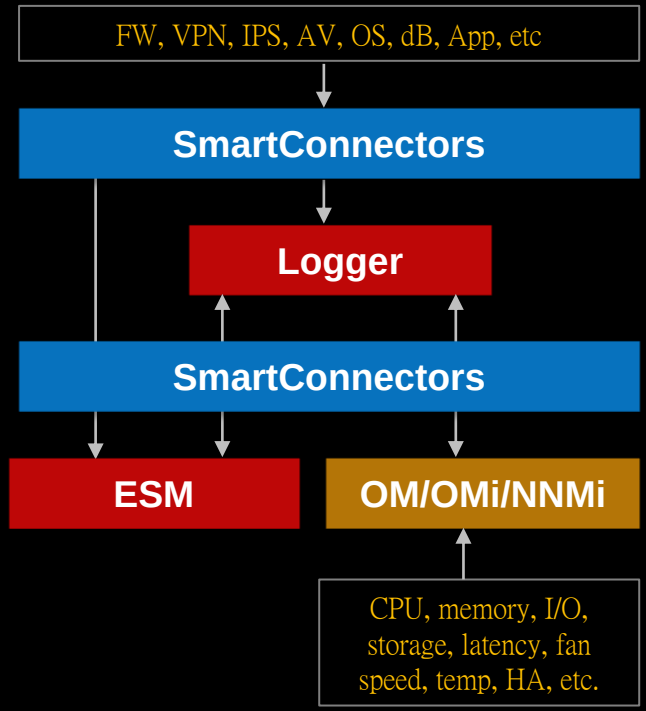
360º view of security and IT events

WHAT IT IS

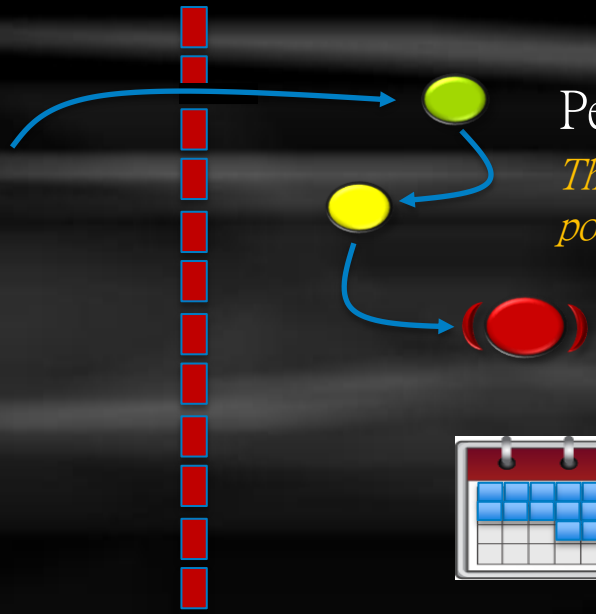
- Bi-directional integration between OM/NNM/NNMi and HP ArcSight ESM/Logger

BENEFITS

- Complete visibility into anomalies and threats
- Single pane of glass view of security, compliance and IT ops
- Reduced gap between NOC and SOC
- Security and compliance related KPIs to IT operations service health dashboards
- Automate business process and workflows to enable effective business risk management



Protecting Against Advanced Persistent Threats



Perimeter Security Intelligence

The Perimeter will be breached at some points

Insider Threat Security Intelligence

*Understand the behaviors of **privileged users** & **authorized users** to identify anomalies*

An Effctive Operational Capability

People, Processes and Procedures


Thank you
ENTERPRISE SECURITY