



■ Cyber Preparedness

> A Proactive Response to Infiltration

Colin McKinty

Vice President, Cyber Strategy for the Americas

colin.mckinty@baesystems.com

April 2016

■ Cyber Preparedness



How To Get Started



Take A Proactive Stance



Be Ready to Respond

■ Cyber Preparedness



How To Get Started



Take A Proactive Stance



Be Ready to Respond

Where Does Cyber Preparedness Begin?

Technology?

Security team?

Processes?





It starts with **The Board.**

It is driven by a culture where
cyber risk is addressed as part
of operational risk



Why Should They Care?

The Obvious





Reducing Risk.

Enables Growth.

■ Cyber Preparedness



How To Get Started



Take A Proactive Stance



Be Ready to Respond



- ❑ Fire started in a NJ home last year
- ❑ A driver saw the fire and banged on the front door until someone answered
- ❑ The alarms went off -- afterward
- ❑ The family inside escaped
- ❑ Fireman eventually got control
- ❑ Happy ending ... but what if the driver did not stop?
- ❑ Also, almost one year later, re-construction is just starting

Effective Smoke Detection



- Consider where you replace them
- Ensure the batteries work
- Monitor and maintain



Have a Plan for When the Alarm Goes Off

- ❑ Think of this as Incident Response
- ❑ The value of knowing someone is looking after you ... ready to bang on your door when fire starts



- ❑ What if there's a "fire" in your network?
- ❑ What if the alarms don't go off right away or if you don't have the right alarms in place?
- ❑ What kind of damage could that do if your business took a year to get back to normal?
- ❑ Also, consider the scenario where your entire operation "burns to the ground"

■ Hierarchy of Security Needs

To be fully prepared and avoid disasters:

- Detect new, hidden threats
- Effectively and efficiently respond
- Reduce the time & resources required in the detection to resolution phase

■ Prevention: Still Important

TRAINING

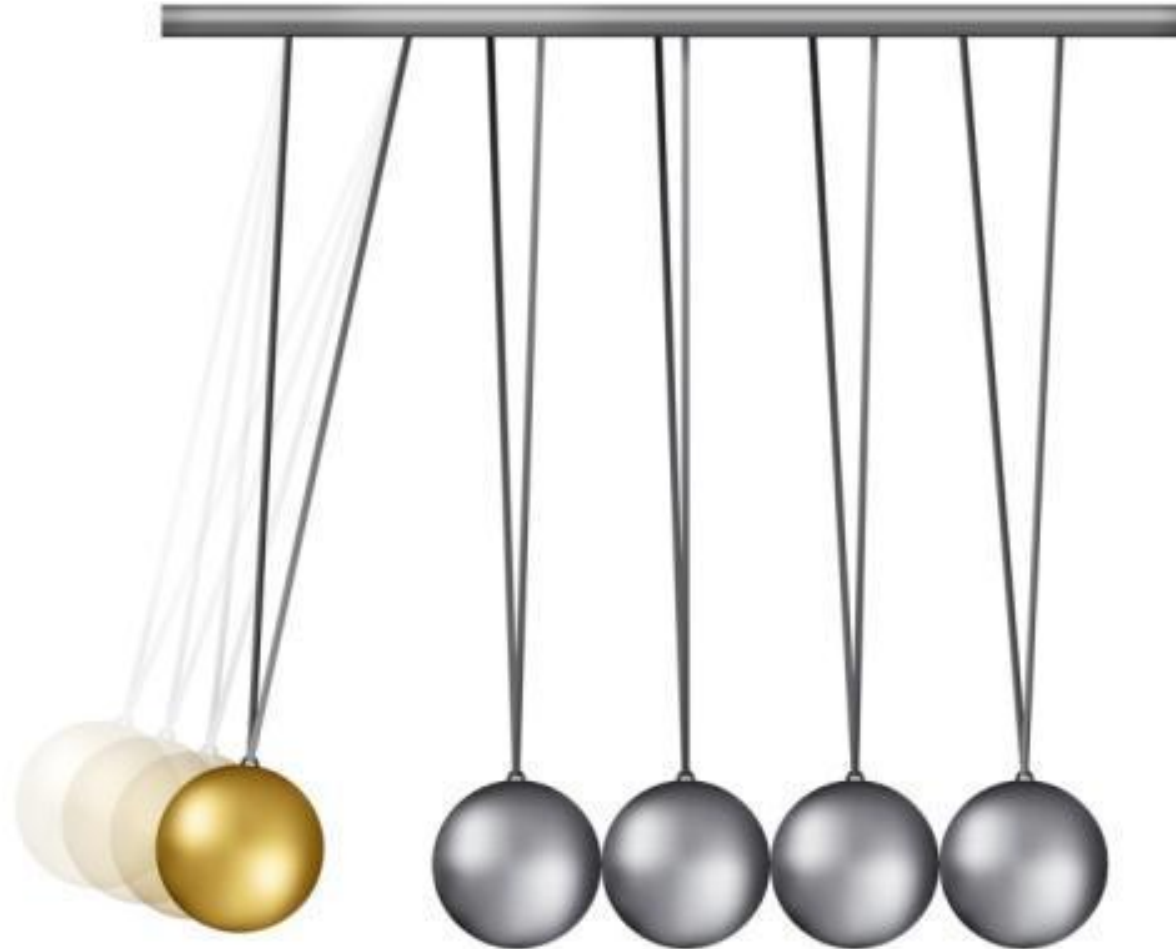


■ Balancing Spend Allocations

Prevention

Detection

Response



The ability to respond to an incident is only as good as an organization's ability to ...

detect the incident.





Detection

> Why It's Challenging

- Too many bad guys/attacks
- Bad guys don't want to be found
- Attacks take new forms every day
- Sophisticated APT and targeted attacks routinely circumvent existing security defenses
- The longer they stay undetected, the greater the financial damage and sensitive data loss

Analytics Techniques

Detection Techniques

- Anomaly Detection Analytics
- Unsupervised machine learning

- Anomaly Detection Analytics
- Behavioural Analytics
- Unsupervised machine learning

- Anomaly Detection Analytics
- Behavioural Analytics
- Supervised machine learning

- Signatures
- Rules

Attacks

New, unknown, attacker techniques
Nation state, targeted attacks

Known attacker techniques.
Beaconing, watering hole etc.

Known attacker methods.
Exploit kits, evolving malware strains. e.g. key loggers, browser clashes

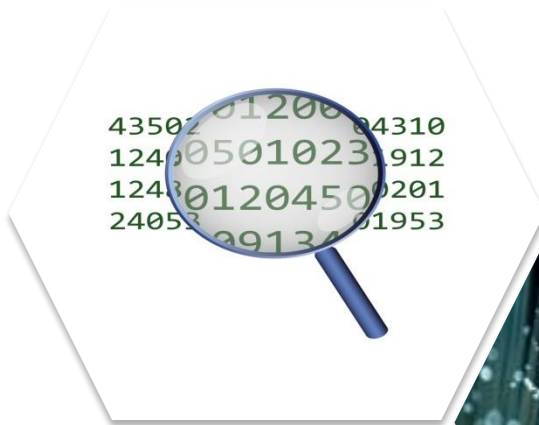
Previously seen threat.
Exact malware match, known bad end points

Increasing Risk

**Threat
Landscape**

Characteristics of Behavioral Analytics

Potentially bad vs
known bad



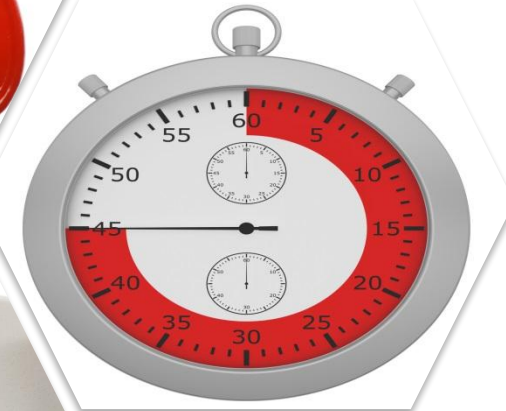
Risk based
vs binary



Enduring
vs brittle



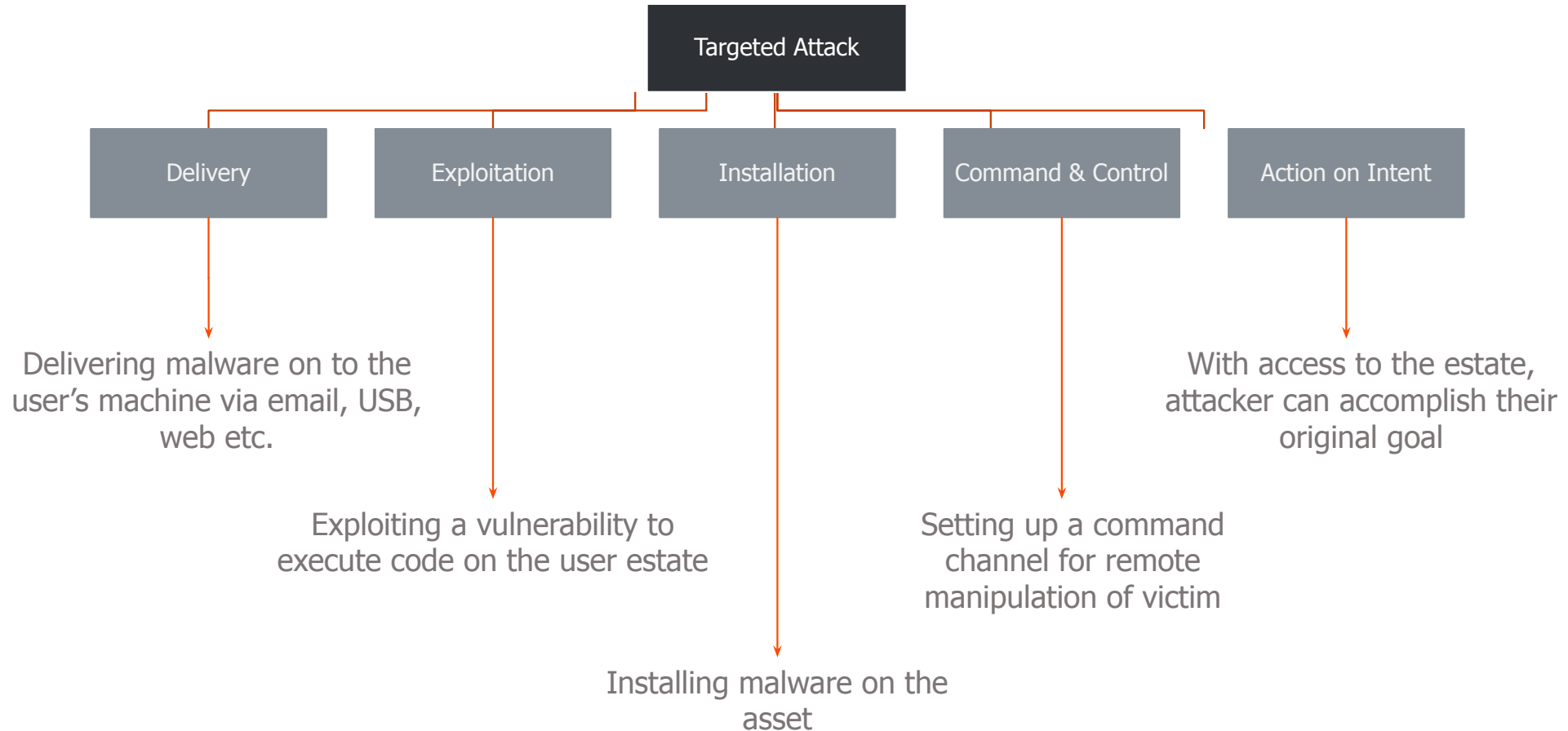
Time range vs
point in time



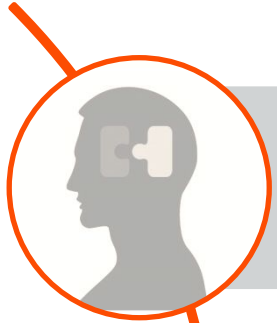
General vs specific case

■ Detection needs to driven by a Threat model

Analytics are categorised by 'attack technique'. These are the stages an attacker has to go through to successfully complete an attack on a network.



Cyber Preparedness



How To Get Started



Take A Proactive Stance



Be Ready to Respond



I Response



Having proper **analysis capabilities** requires both trained personnel and the proper tools to perform the analysis.



A PLAN VS A FRAMEWORK



*"No plan of operations
extends with certainty
beyond the first encounter
with the enemy's main strength"*

-- Helmuth Karl Bernhard Graf von Moltke



FRAMEWORK

- Authority and Scope
- Team Members and Responsibilities
- Logistics
- Process to determine severity and escalation
- Post-Incident Activities
- Supporting Documentation



The **most critical** component
in any Incident Response
Practice ...

Authority and backing from
executive management.



IR Team

- Primary team
- Extended team
- Third parties



Primary

- Security Team
- IR Lead
- Operations Team
- Service Desk Team



Extended

- Executives
- Legal
- Communications
- Human Resources
- Compliance
- Physical Security



3rd Parties

- Outsourced IT (help desk, server support)
- Forensic Firms
- ISPs
- Legal Counsel
- Law Enforcement
- Public Relations Teams

LOGISTICS



Often overlooked items:

- Succession of Command
- Catering
- Shipment of Evidence
- OpTempo

- E-Mail Distro / Call bridge for communication
- War Room
- Computing equipment
- Evidence Locker

Testing Incident Response

- High Level Audit
- Objective Based Assessment
- Table top Exercise
- War Game



■ Cyber Preparedness – Key Takeaways



Begins With Preparedness Culture



Balancing Act; Varied Techniques



Turn IR Plan Into an IR Framework

Thank You



Q&A

BAE Systems
Surrey Research Park
Guildford
Surrey
GU2 7YP
United Kingdom

T: +44 (0)1483 816000
F: +44 (0)1483 816144

Unpublished Work Copyright © 2015 BAE Systems. All Rights Reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc.

The information in this document contains proprietary information of BAE Systems. Neither this document nor any of the proprietary information contained therein shall be (in whole or in part) published, reproduced, disclosed, adapted, displayed, used or otherwise made available or accessible (in each case, in any form or by any means) outside of BAE Systems without the express written consent from the document originator or an approved representative of BAE Systems.

BAE Systems Applied Intelligence Limited registered in England and Wales Company No. 1337451 with its registered office at Surrey Research Park, Guildford, England, GU2 7YP.

FREEDOM OF INFORMATION ACT

This document (<projectreference><documentnumber>) contains confidential and commercially sensitive material which is provided for the Authority's internal use only and is not intended for general dissemination.

The information contained herein pertains to bodies dealing with security, national security and/or defence matters that would be exempt under Sections 23, 24 and 26 of the Freedom of Information Act 2000 (FOIA). It also consists of information which describes our methodologies, processes and commercial arrangements all of which would be exempt from disclosure under Sections 41 and 43 of the Act.

Should the Authority receive any request for disclosure of the information provided in this document, the Authority is requested to notify BAE Systems Applied Intelligence. BAE Systems Applied Intelligence shall provide every assistance to the Authority in complying with its obligations under the Act.

BAE Systems Applied Intelligence's point of contact for FOIA requests is:

Chief Counsel
Legal Department
BAE Systems Applied Intelligence
Surrey Research Park
Guildford Gu2 7YP
Telephone 01483 816082