Security in knowledge

BREAKING THE KILL CHAIN – AN EARLY WARNING SYSTEM FOR ADVANCED THREAT

Rashmi Knowles

RSA, The Security Division of EMC

RSA CONFERENCE EUROPE 2013

Session ID: SPO-W07

Session Classification: Intermediate

Security in knowledge

#RSAC

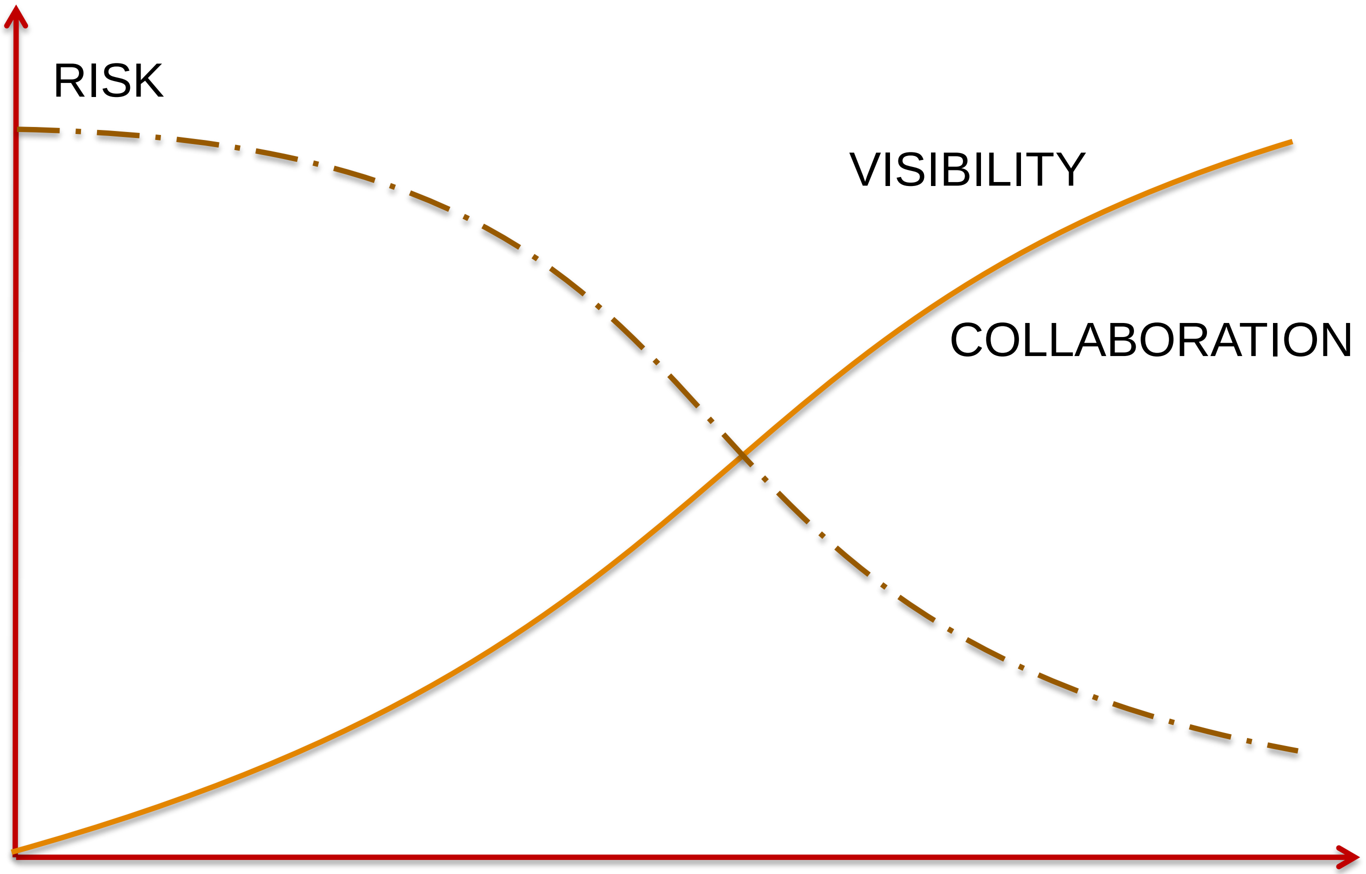
RSA CONFERENCE EUROPE 2013

"APT1 maintained access to victim networks for an average of 356 days. The longest time period APT1 maintained

access to a victim's network was 1,764 days, or four years and ten months."

Source Mandiant APT1 Report Feb 2013

Characteristics of Security Maturity



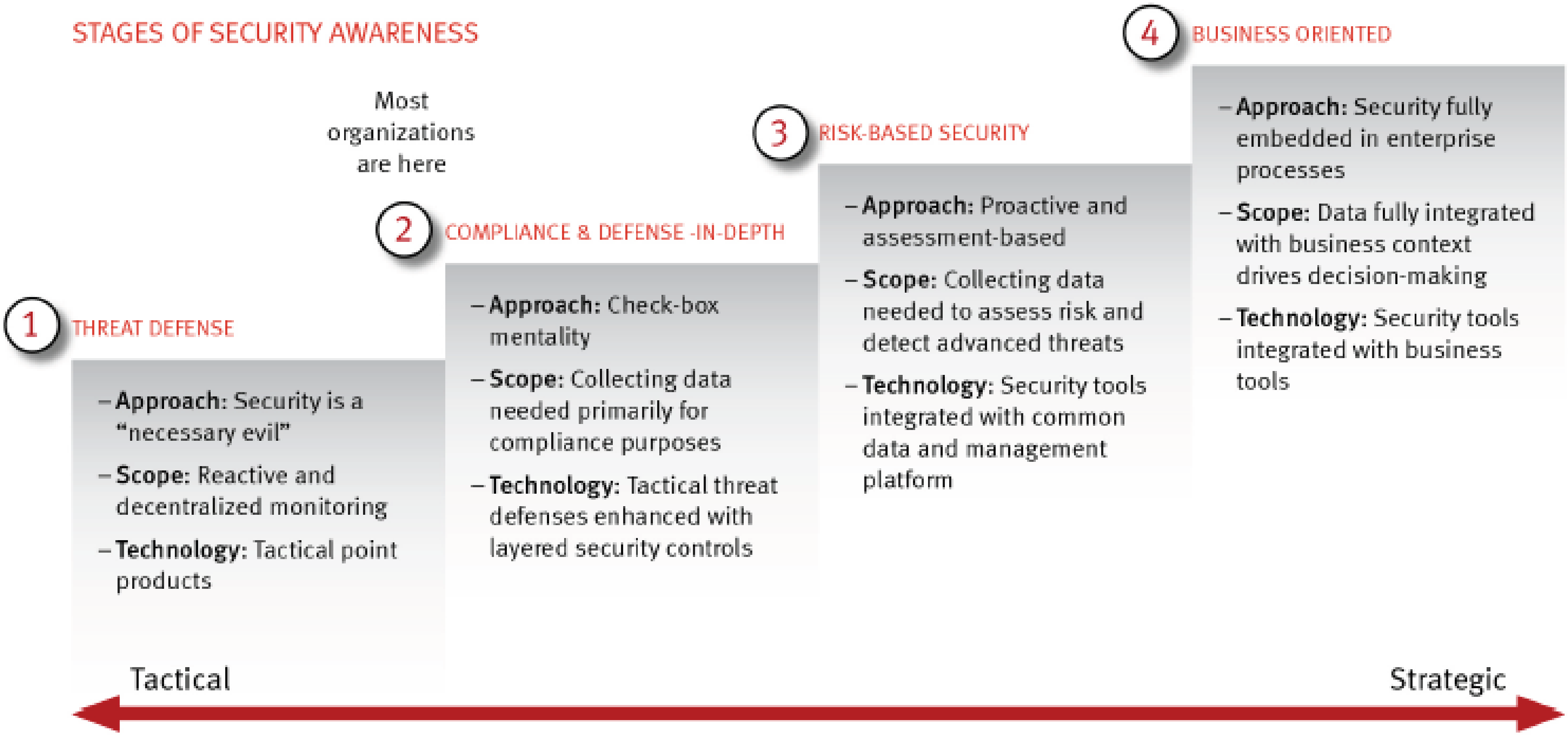
Step 1:
Threat Defense

Step 2:
Compliance and Defense-in-Depth

Step 3:
Risk-Based Security

Step 4:
Business-Oriented

Information Security Maturity Model



STAGES OF SECURITY AWARENESS

Most organizations are here

1 THREAT DEFENSE

- Approach: Security is a "necessary evil"
- Scope: Reactive and decentralized monitoring
- Technology: Tactical point products

2 COMPLIANCE & DEFENSE -IN-DEPTH

- Approach: Check-box mentality
- Scope: Collecting data needed primarily for compliance purposes
- Technology: Tactical threat defenses enhanced with layered security controls

3 RISK-BASED SECURITY

- Approach: Proactive and assessment-based
- Scope: Collecting data needed to assess risk and detect advanced threats
- Technology: Security tools integrated with common data and management platform

4 BUSINESS ORIENTED

- Approach: Security fully embedded in enterprise processes
- Scope: Data fully integrated with business context drives decision-making
- Technology: Security tools integrated with business tools

Tactical

Strategic

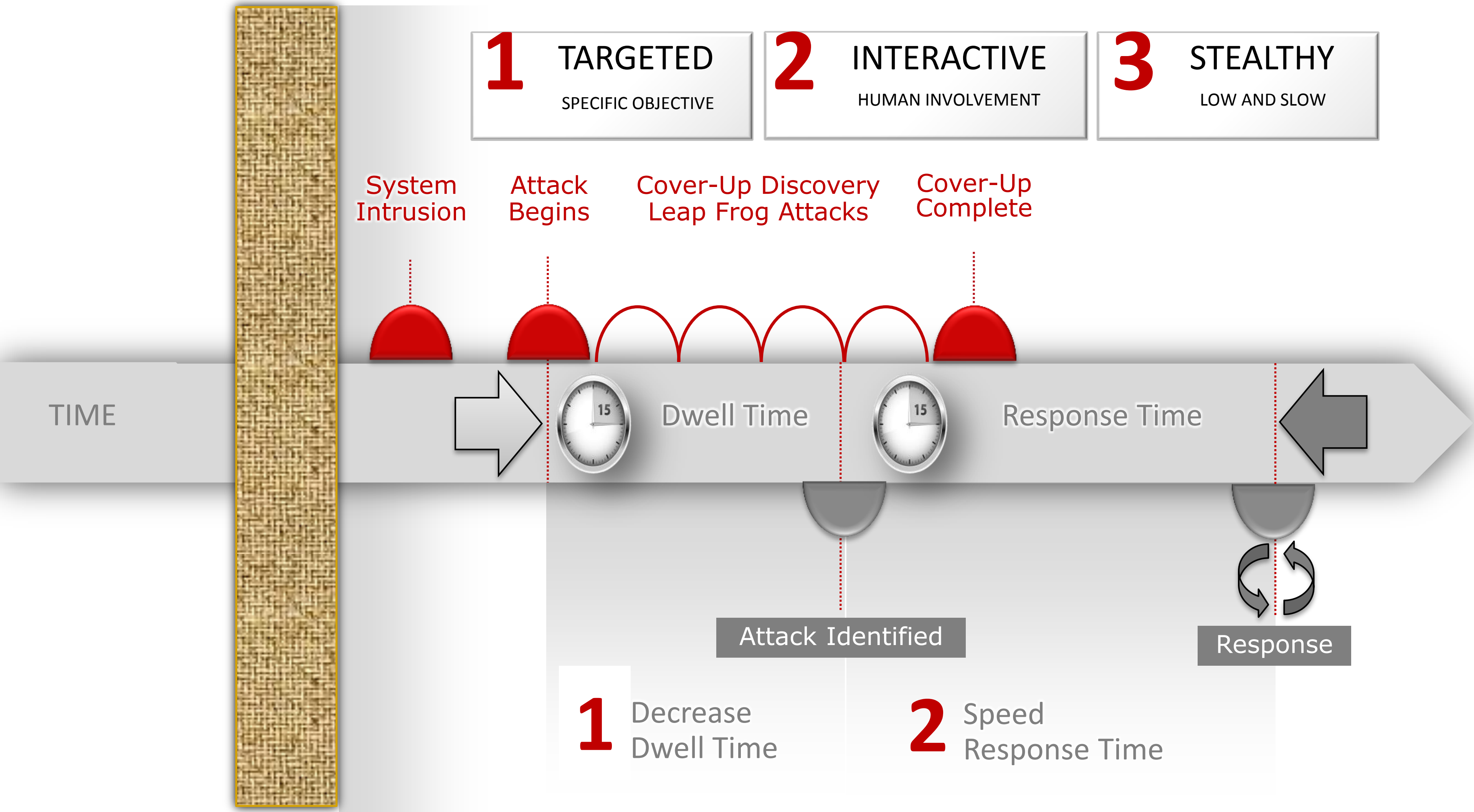
Source: Enterprise Strategy Group, 2013.

Security is becoming a Big Data problem

- More determined adversary means more data needed to identify attacks
- More complex IT environment means even simple attacks can hide in plain sight
- Security professionals are struggling to keep up[1]
  - 40% of all survey respondents are overwhelmed with the security data they already collect
  - 35% have insufficient time or expertise to analyze what they collect

[1] EMA, The Rise of Data-Driven Security, Crawford, Aug 2012
Sample Size = 200

Advanced Threats are Different



KNOW YOUR ENEMY

- What are the common threat vectors?
- What exploits are commonly used?
- Threat research groups and vendors
- Threat teams from competitors
- Industry working groups

KNOW YOUR PEOPLE

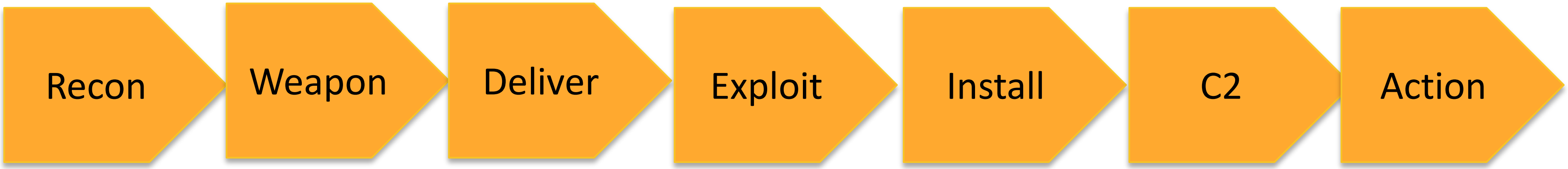
- Who has enhanced access?
- Security policy that covers common attack scenarios?
- Who are my likely targets?
- Am I continuously tracking employees that have been compromised?
- Is there a privacy issue?

KNOW YOUR NETWORK

The ability to pervasively know what your network looks like on a day-to-day basis is **critical** in helping to identify advanced threats

THE KILL CHAIN

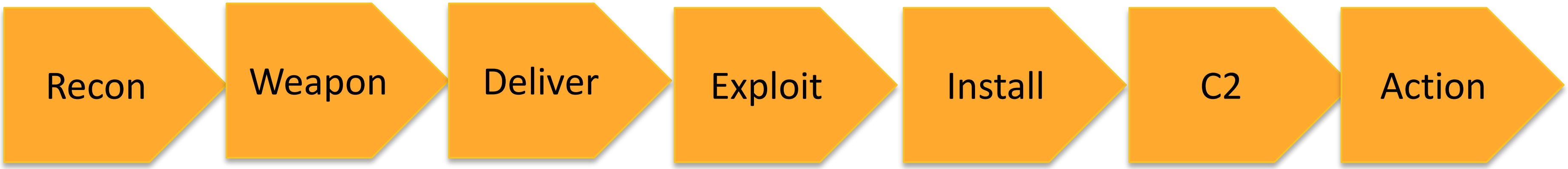
- Lockheed Martin methodology
- Seven steps
- Guides analysis to actionable intelligence



Recon → Weapon → Deliver → Exploit → Install → C2 → Action

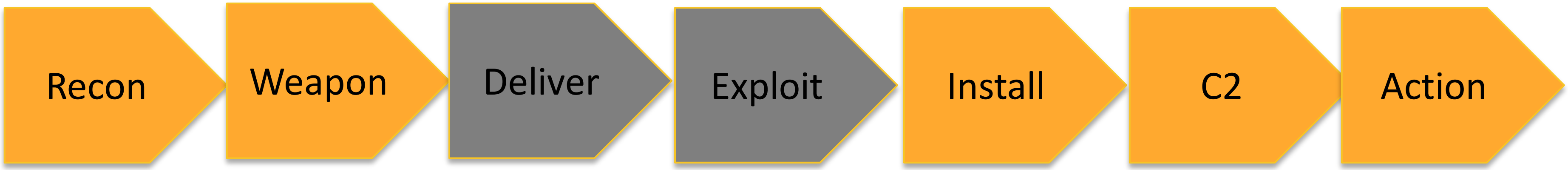
ORGANISATIONS MUST GET CREATIVE

- Focus on early detection of breaches to minimize your window of vulnerability.
- Move backward in the ‘Kill chain’
- The key is actively preserving, aggregating and reviewing data to detect a potential intrusion but also for post-event forensics.

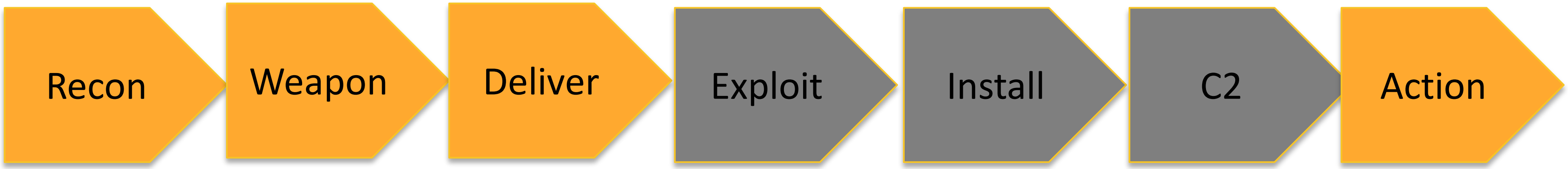


Recon → Weapon → Deliver → Exploit → Install → C2 → Action

SINGLE EVENT MENTALITY

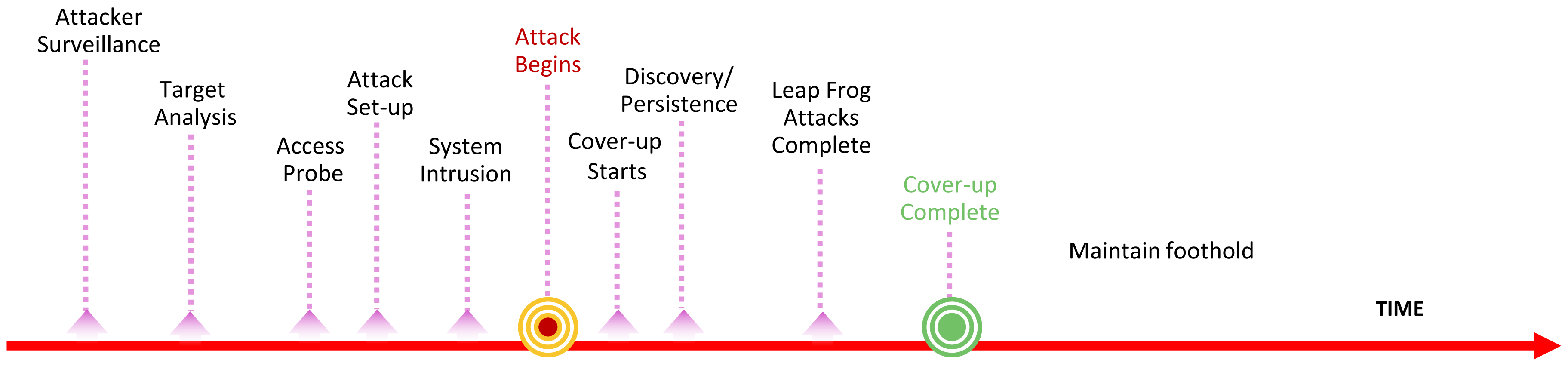


Recon Weapon Deliver Exploit Install C2 Action



Recon Weapon Deliver Exploit Install C2 Action

INVESTIGATION TODAY.....



Attacker Surveillance

Target Analysis

Access Probe

Attack Set-up

System Intrusion

Attack Begins

Cover-up Starts

Discovery/ Persistence

Leap Frog Attacks Complete

Cover-up Complete

Maintain foothold

TIME

Transactions

- Are we seeing suspicious transactions against sensitive/high value apps/assets

Sources

- WFD
- Transaction Monitoring
- SIEM
- SQL server logs

Information

- What kind of data does this system store, transmit, process?
- Is this a regulatory issue? High value IP?

Sources

- DLP
- Data Classification
- GRC

Infrastructure

- Has the server been manipulated?
- Is it vulnerable? Has its config changed recently?
- Is it compliant with policy?

Sources

- GRC System
- Config Mgmt
- Vul. Mgmt

Traffic

Are there traffic anomalies to/from these servers

- Protocol Distribution
- Encryption
- Suspicious destinations

Sources

- Netflow
- Network Forensics
- Web Proxy Logs
- SIEM

Identity

- Which users were logged onto them
- Have their priv. been escalated?
- Where did they log in
- What else did they touch?

Sources

- Active Directory
- Netflow
- Server Logs
- Asset Management
- SIEM

PERVASIVE VISIBILITY

- You must be able to see everything
- Full network packet capture
  - Identifying Malware
  - Tracking attackers' activities inside the environment
  - Presenting proof of illicit activity

DEEPER ANALYTICS

- Combine disparate data
- Behaviour patterns and risk factors
- Value of assets vs. risk
- Eliminate ‘known good’ activities
- Should not replace human judgement

MASSIVE SCALABILITY

- Volume and speed of data
- Internal and external feeds
- Analytics engine to normalise data
- Distributed storage architecture

UNIFIED VIEW

- Automated processes
- Correlated information
- Speeds up decision making
- Compliance becomes a by-product

CUSTOMER MATURITY MODEL

- Advanced Threats Become the Major Spend Driver as Customers Mature

	Security Level 1 Naïve/Cost-based	**Security Level 2** Compliance-driven	**Security Level 3** IT risk-driven	**Security Level 4** Business risk-driven
Approach	Security is "necessary evil"	Check-box mentality	Proactive and assessment-based	Security fully embedded in enterprise processes
Technology	Reactive and de-centralized monitoring	Implement security and collect data to be compliant	Assess risks and detect threats for organization as a whole	Assess business risks to drive security implementation
	Tactical threat defenses	Tactical threat defenses enhanced with tracking and reporting tools	Security tools integrated with common data and management platform	Security tools integrated with business tools e.g. eGRC
		Regulatory Environment	New leadership	Security breaches; customer demand

DETECTION AND RESPONSE

Cyber Threat Intelligence

- Open/All Source Actor Attribution
- Attack Sensing & Warning
- Social Media
- High Value Target (HVT)

Advanced Tools, Tactics & Analysis

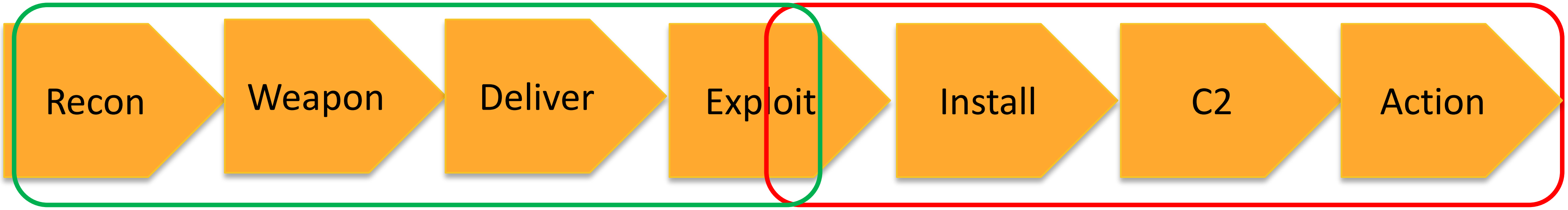
- Reverse Malware Engineering
- Host & Network Forensic
- Cause & Origin Determination
- Email operations

Critical Incident Response Team

- Eyes-on-Glass
- End User Intake
- Event Triage
- Incident Containment
- 24x7 Coverage

Content Analytics Team

- Integration
- Content Development
- Reporting
- Alert and Rule Creation



BREAKING THE KILL CHAIN

Recommendations

- Focus on Risk, Context and Agility
- Reduce ‘dwell time’
- Move back in the Kill Chain
- Continuous monitoring – see everything!
- Implement automation

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him.

- Sun Tzu, The Art of War

Thank you!

Rashmi Knowles

RSA, The Security Division of EMC

@knowlesRashmi
Rashmi.knowles@emc.com

www.emc.com