The Future of the Advanced SOC

Getting Ahead of Advanced Threats

Philip Aldrich, CISSP, CISM, CISA, CRISC, CIPP
Program Director, Risk Management
EMC

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

RSA

EMC²

Agenda

- Today’s Security Landscape
- Anatomy of an attack
- New Required Capabilities
- SOC vs. CIRC
- Security Management Program

Threats are Evolving Rapidly

Criminals

Petty criminals

Unsophisticated

Organized crime

Organized, sophisticated supply chains (PII, financial services, retail)

Nation state actors

PII, government, defense industrial base, IP rich organizations

Non-state actors

Terrorists

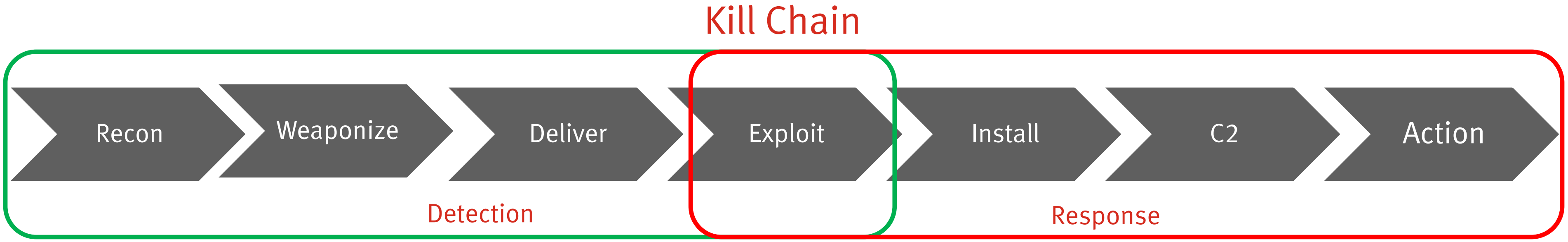
PII, Government, critical infrastructure

Anti-establishment vigilantes

"Hacktivists"
Targets of opportunity

The Reality in the Cyber World

- Malicious activity is increasing in:
  - Volume
  - Sophistication (TTP)
  - Intensity and focus (APT)
- Response after compromise creates an undesirable foot-race
  - Attackers seem to know our networks better than us
  - The damage may already be done
  - Can we be 100% sure we can keep attackers out
- Move backwards in the "Kill Chain" to move the defensive wall out



Kill Chain

Recon → Weaponize → Deliver → Exploit → Install → C2 → Action

Detection

Response

Business & IT are evolving rapidly too…

Traditional Security is Not Working

99% of breaches led to compromise within "days" or less with **85%** leading to data exfiltration in the same time

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

85% of breaches took "weeks" or more to discover

Source: Verizon 2012 Data Breach Investigations Report

Hacktivists Steal More Data Than Cybercriminals, Report Shows

-The Wall Street Journal, Tech Europe

Cyber-threats will become top worry, FBI director says

- Associated Press

Traditional Security is Unreliable

Signature-based

Perimeter oriented

Compliance Driven

Minimum Requirements of Security Management and Compliance

Critical Questions To Ask

Governance

What Matters?

Comprehensive Visibility

What is going on?

Actionable Intelligence

How do I address it?

Effective

Security Systems need to be:

Agile

Contextual

Risk-Based

Average Company's Readiness for Managing Advanced Threats

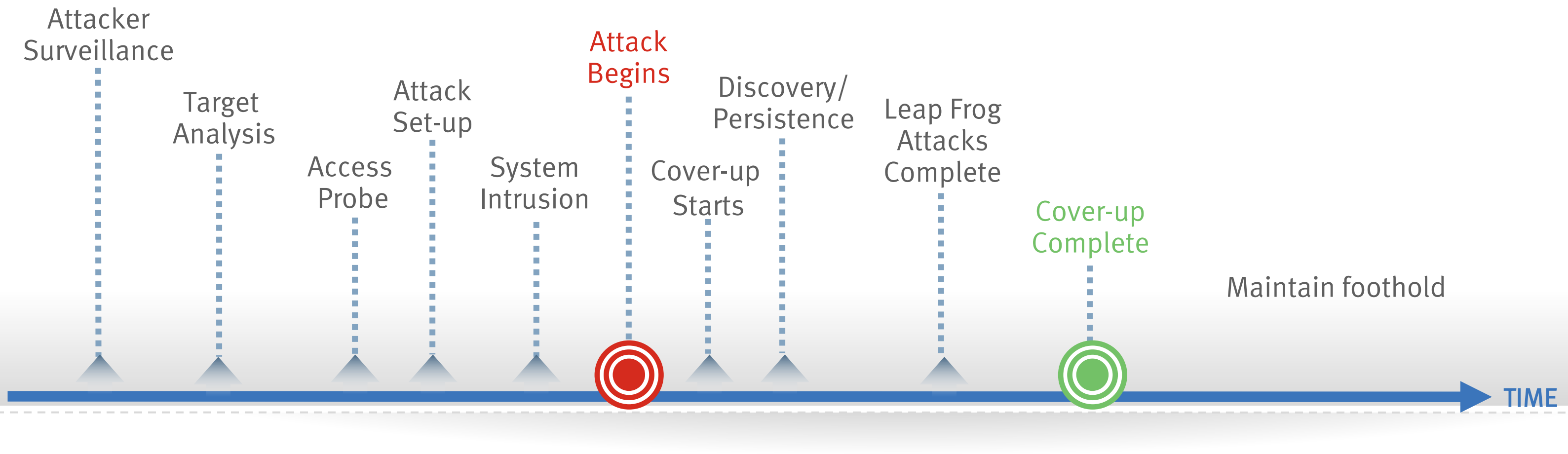
Poorly prepared for advanced threats

Inability to detect attacks in a timely manner

Response if often uncoordinated and chaotic

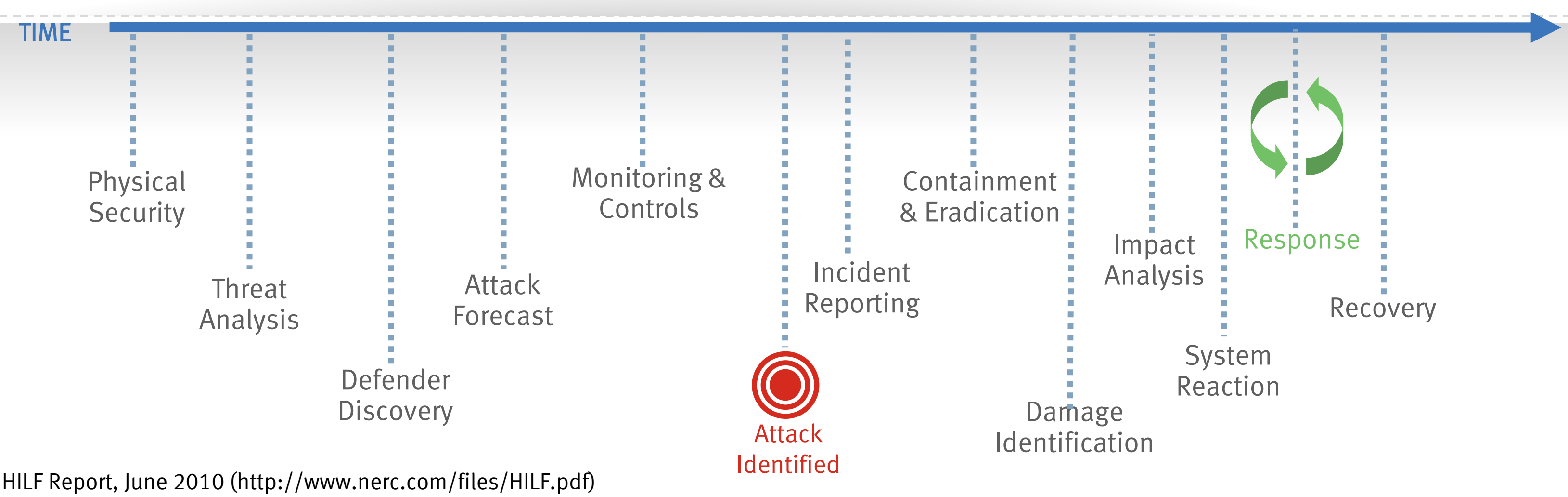
➡ **AUTOMATED INTELLIGENT CONTROLS,**
with real-time monitoring capabilities to spot anomalies are needed

Anatomy of an attack



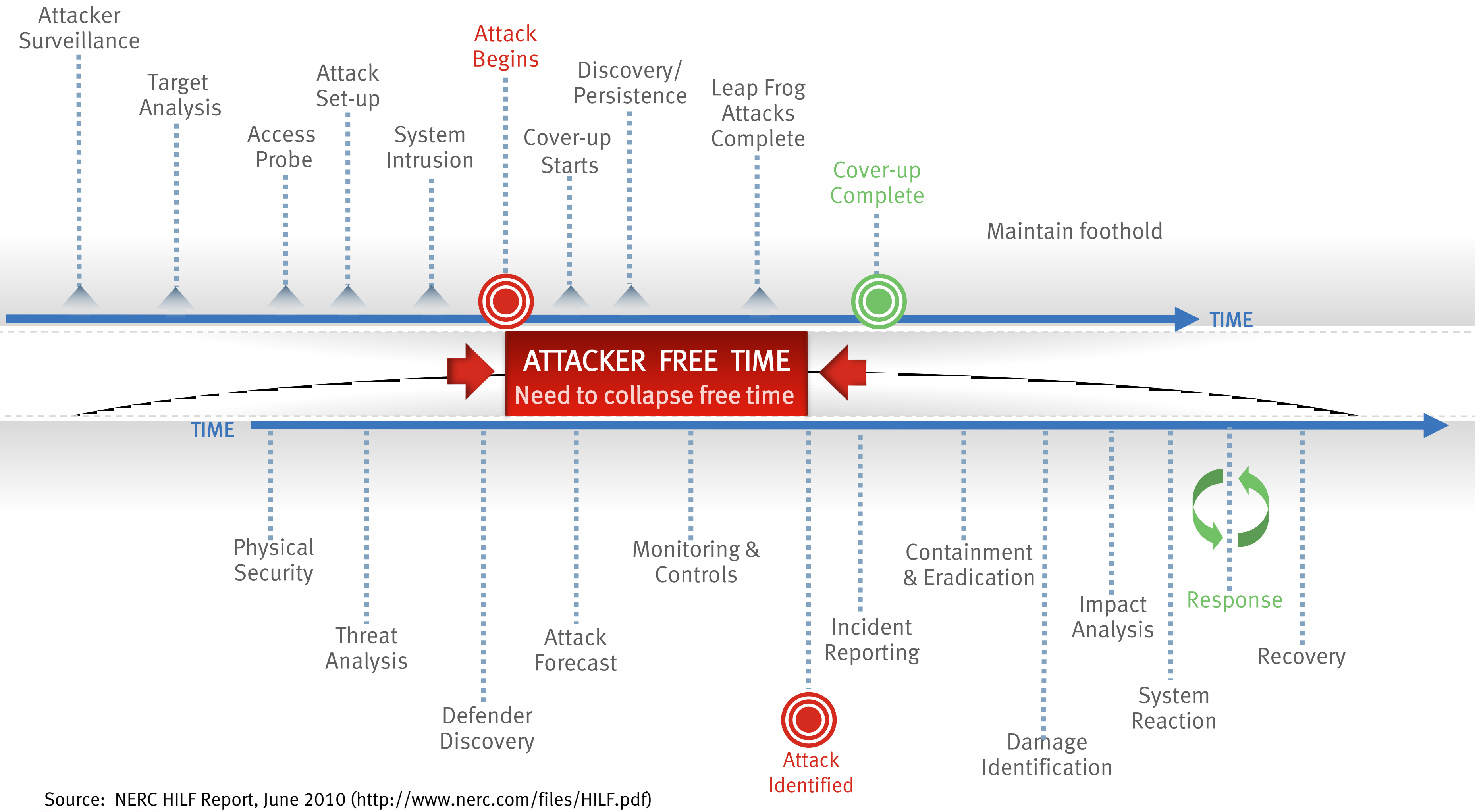
Source: NERC HILF Report, June 2010 (http://www.nerc.com/files/HILF.pdf)

Anatomy of a response

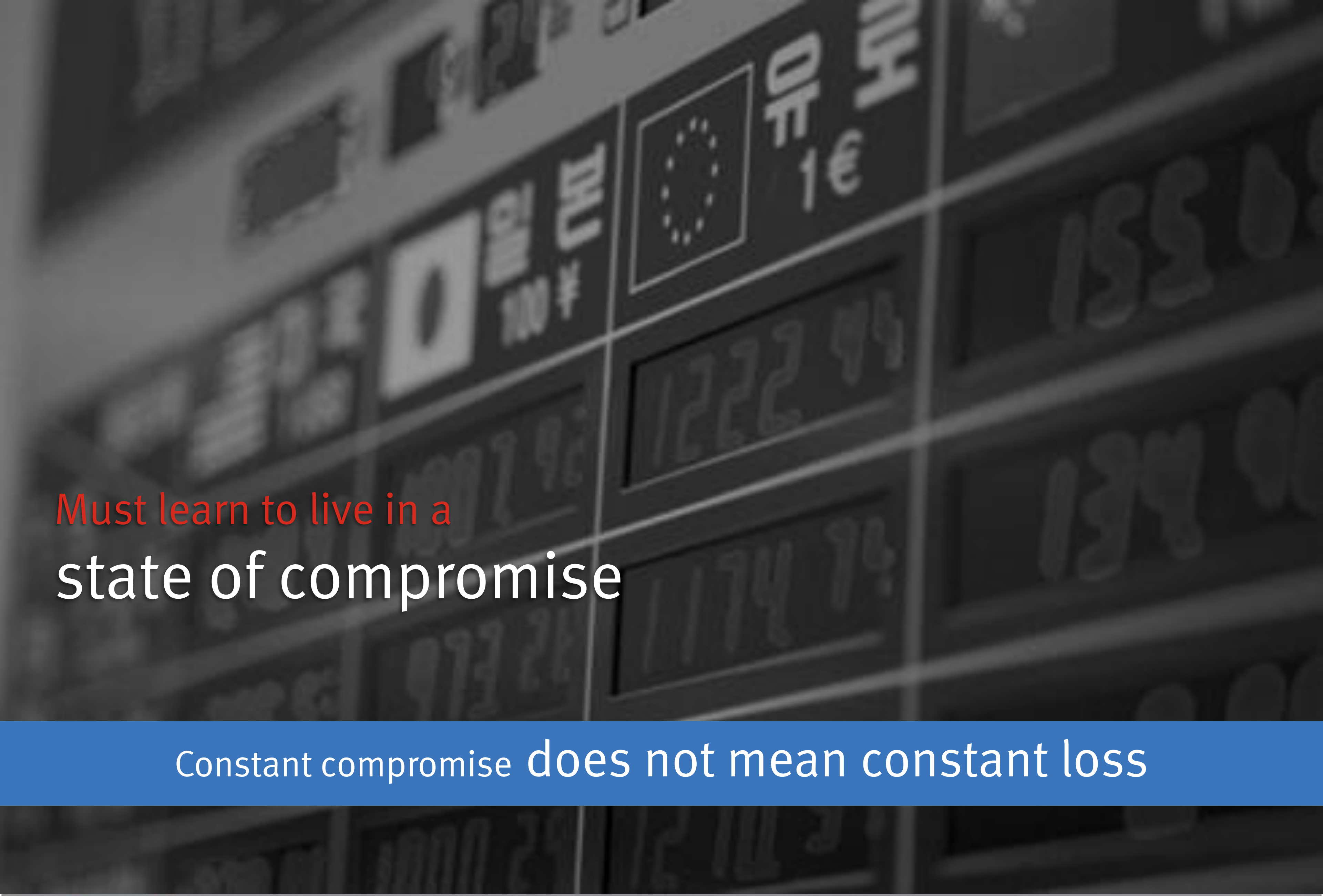


Source: NERC HILF Report, June 2010 (http://www.nerc.com/files/HILF.pdf)

Reducing Attacker Free Time



Source: NERC HILF Report, June 2010 (http://www.nerc.com/files/HILF.pdf)



Must learn to live in a state of compromise

Constant compromise does not mean constant loss

What is the approach for the future?

Companies require…

Comprehensive Visibility

“Analyze everything that’s happening in my infrastructure”

Agile Analytics

“Enable me to efficiently analyze and investigate potential threats”

Actionable Intelligence

“Help me identify targets, threats & incidents”

Optimize Incident Management

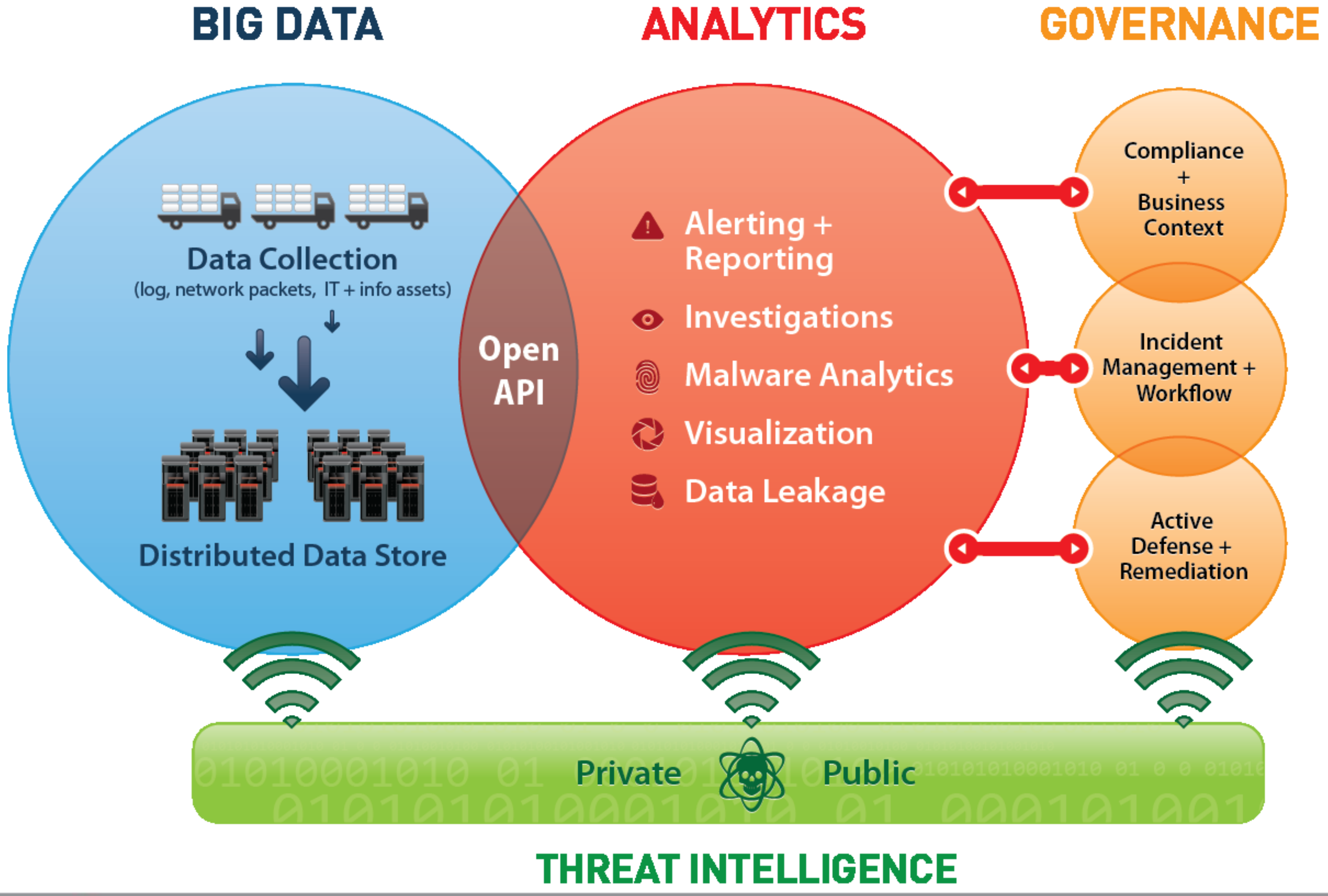
“Enable me to manage these incidents”

“Enterprises lack the resources to effectively respond to the overwhelming threat landscape and vendor solutions must ***expedite not impede incident response.*** *Incident response isn’t about point solutions; it’s about ecosystems.”*

Incident Response Isn’t About Point Solutions; It’s About An Ecosystem

Blog Posted by Rick Holland (Forrester analyst) on September 19, 2012

New Security Strategy
Agile, Contextual, Risk-based

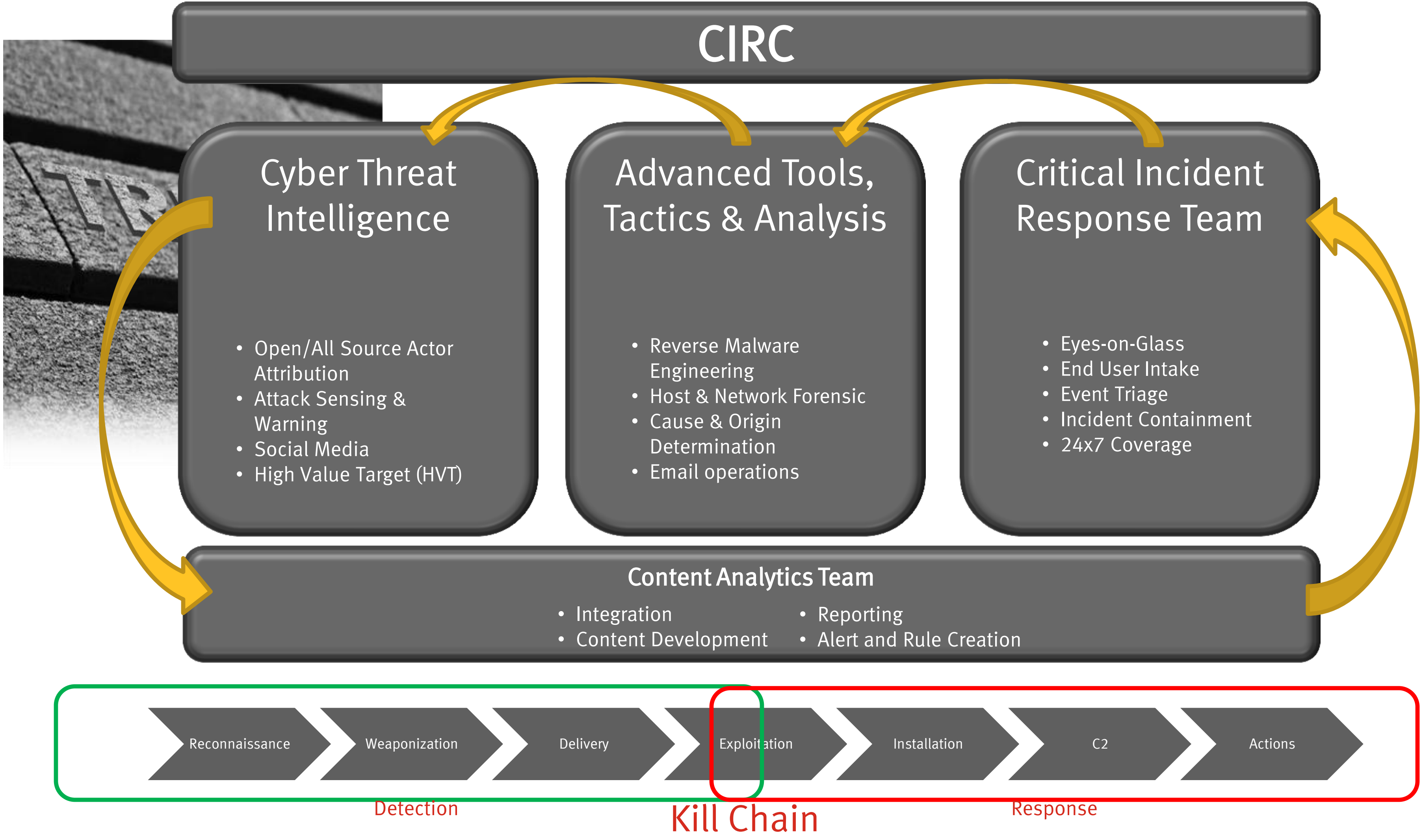


CIRT vs. SOC

SOC = *Security Operations Center*
Level 1 Security adds, moves and changes, security questions, device health, etc.

CIRT = *Critical Incident Response Team*
Manage security incidents, investigate suspicious behavior, vulnerability analysis, malware analysis, threat management, etc.

CIRC Program



CIRC

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

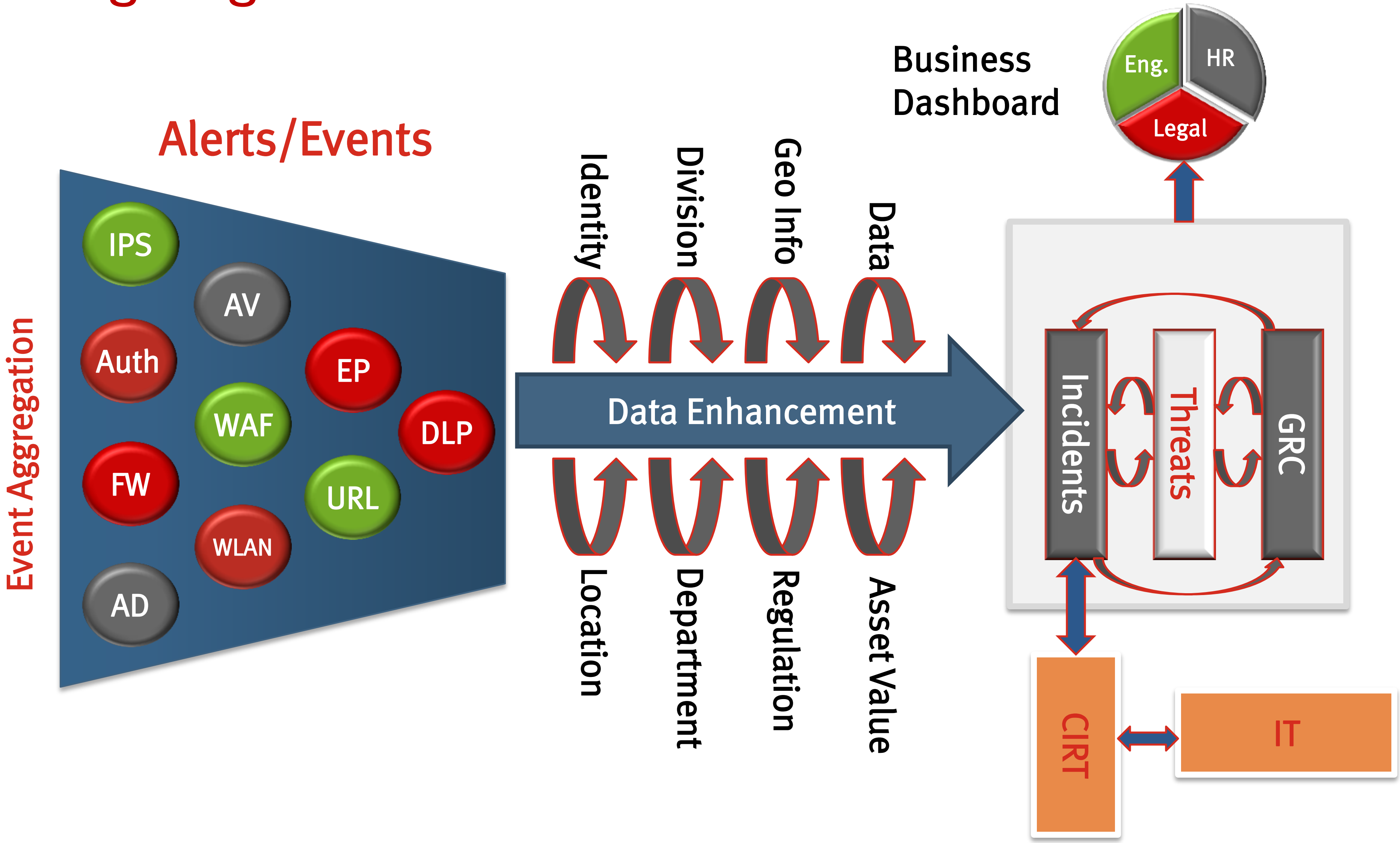
Reconnaissance → Weaponization → Delivery → Exploitation → Installation → C2 → Actions

Detection

Kill Chain

Response

Aligning Incident Data with Risks

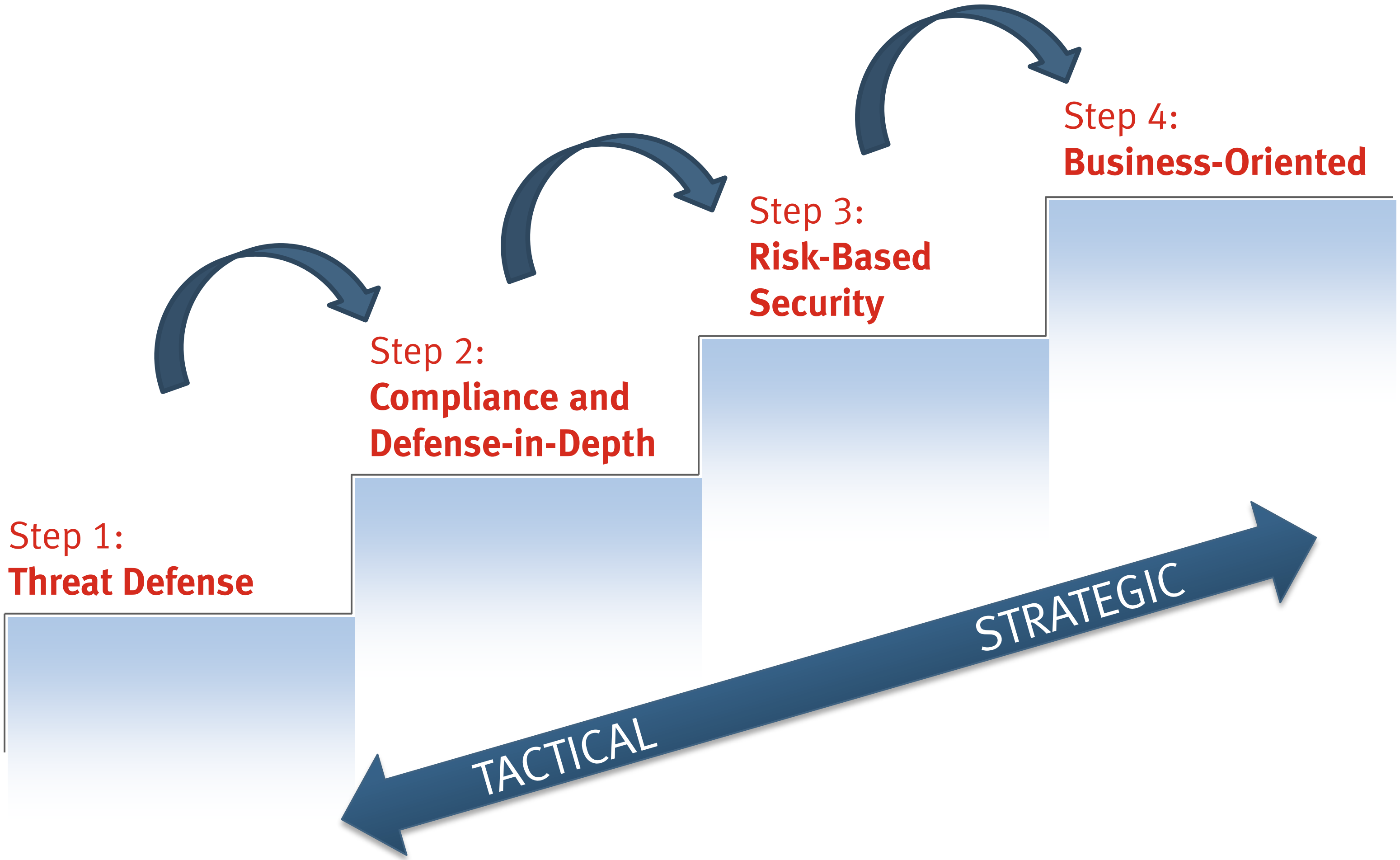


Security Management Program

RSA

EMC²

Incorporating the Maturity Model



Step 1:
Threat Defense

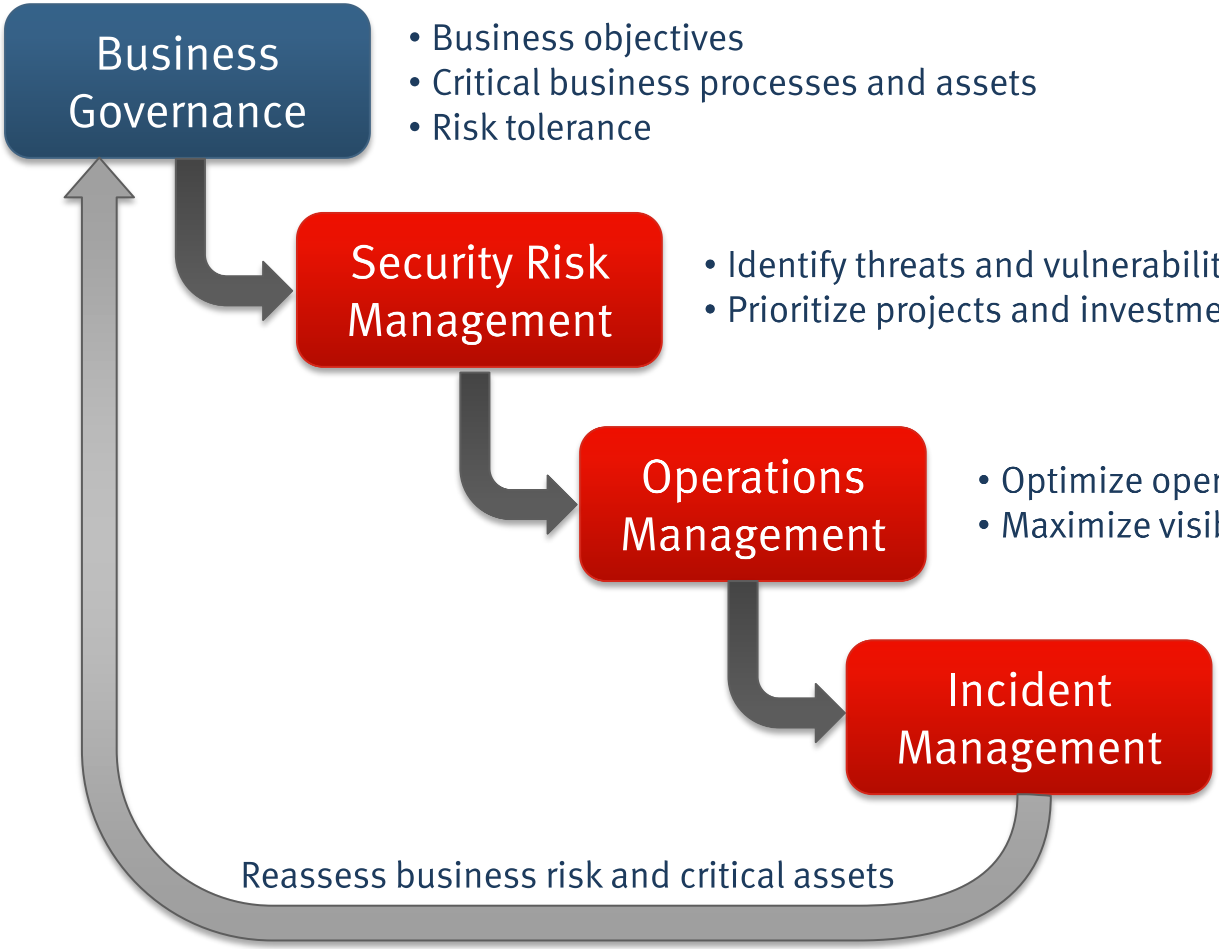
Step 2:
Compliance and Defense-in-Depth

Step 3:
Risk-Based Security

Step 4:
Business-Oriented

Security Management Framework

What do we need to consider?



- Business objectives
- Critical business processes and assets
- Risk tolerance

- Identify threats and vulnerabilities
- Prioritize projects and investments to mitigate risk

- Optimize operational efficiency
- Maximize visibility and monitoring

- Fast detection and response
- Incident lifecycle management

Security Management framework: ISO 27002

Create a Sustainable Long-term program

Recognize a new approach is needed

Focus on your high value assets

Examine the impact of people and processes

Quantify risks exposed through 3rd party vendors

Integrate advanced threat activity into overall security program.

[1] Suzanne Wildup, “The leaking vault: Five years of data breaches,” Digital Forensics Association. July 2010. Available online at http://www.digitalforensicsassociation.org/storage/The_Leaking_Vault-Five_Years_of_Data_Breaches.pdf.

Key Takeaways…

1. You’ll need a Big Data strategy…no avoiding it
2. Look how to integrate and transform your security toolset into an Ecosystem
3. Add Business Context to your assets
4. Determine if you’re goal is a SOC or a CIRC
5. Ensure you have the skill sets and tools to support your goal
6. Be Agile…or you will sink

“Risk comes from not knowing what you're doing”

— Warren Buffett

THANK YOU

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
CRISC
CGEIT
CISM
CISA
RSA
EMC²