Implementing an Intelligent SOC

Paul Stamp
RSA

Session ID: SPO-208
Session Classification: Security Architecture

Objectives of a Security Operations Center

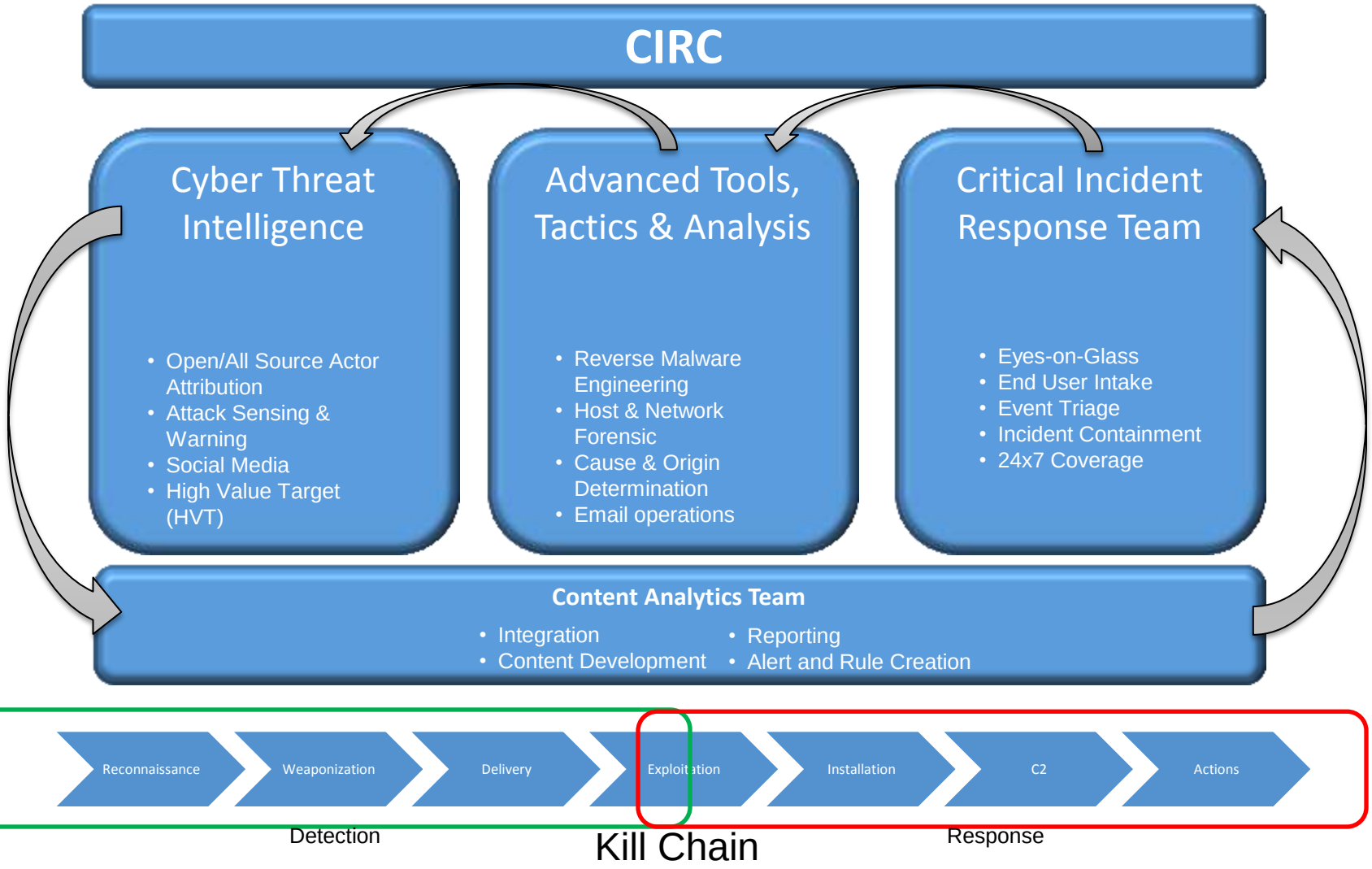
- Ensure security controls are:
  - Up and running
  - Functioning correctly
  - Configured according to business need
- Make sure threats and incidents are:
  - Detected quickly
  - Responded to swiftly and efficiently
  - Remediated before they impact the business

SOC vs CIRC

- Many companies differentiate between a Security Operations Center and a Computer Incident Response Center

	SOC	CIRC
Tasks	•Tool Administration •Vulnerability Scanning •Tier 1 Event Support •Break-Fix	•Incident Investigation •Threat Intelligence •Malware Analytics •Response Coordination
Skill set required	•Intermediate security knowledge •Good tool & process knowledge •Generic company knowledge	•Deep threat knowledge •Advanced technical capability •Investigative experience •Deep company knowledge
Role of a service provider	•Can successfully be outsourced to an MSSP	Tough to outsource as a standalone function

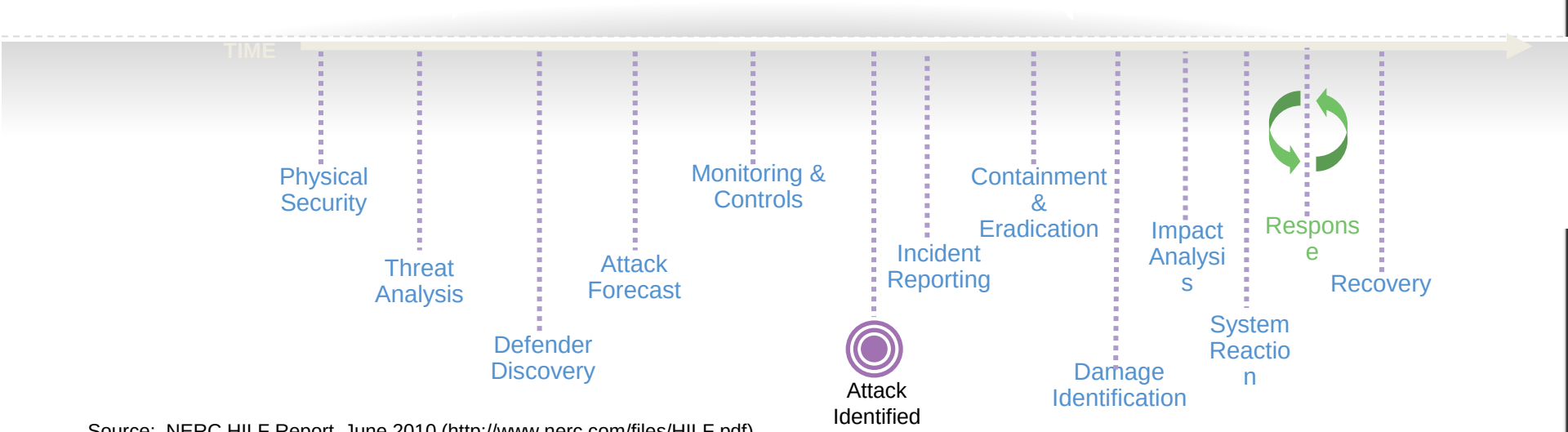
CIRC Program Example



Anatomy of an attack

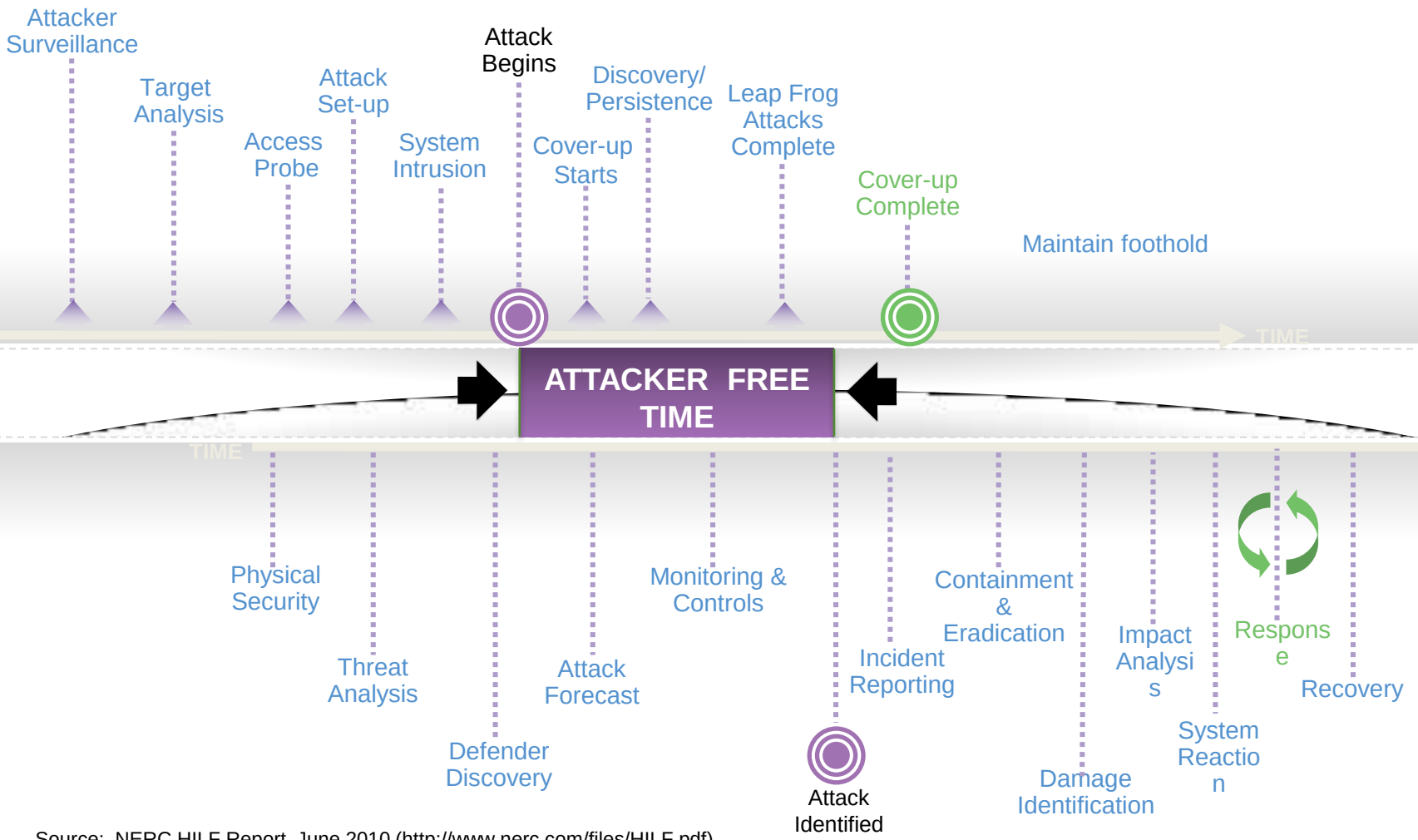
Source: NERC HILF Report, June 2010 (http://www.nerc.com/files/HILF.pdf)

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)

Rethinking Security Operations Toolset

Advanced Challenges	Advanced Requirements for the SOC
Multiple Investigative tools and products in “silos of information”	Single data view with a unambiguous and extensible database design, and deep correlation capabilities.
Persistent internal/external threats	Situational awareness through breadth, depth and scalability across network content, logs and threat intelligence feeds.
Slow response due to legacy requirements	Security analytics that are accurate + real-time + exhaustive.
Poor use of human assets for intelligence	Fast, intuitive investigations augmented with community and threat intelligence feeds.
Volume of Data is Huge and getting Bigger	Collect, retain, and manage TBs of data over ANY required time frame as required by the enterprise

Companies require…

Comprehensive Visibility

"Analyze everything that's happening in my infrastructure"

Agile Analytics

"Enable me to efficiently analyze and investigate potential threats"

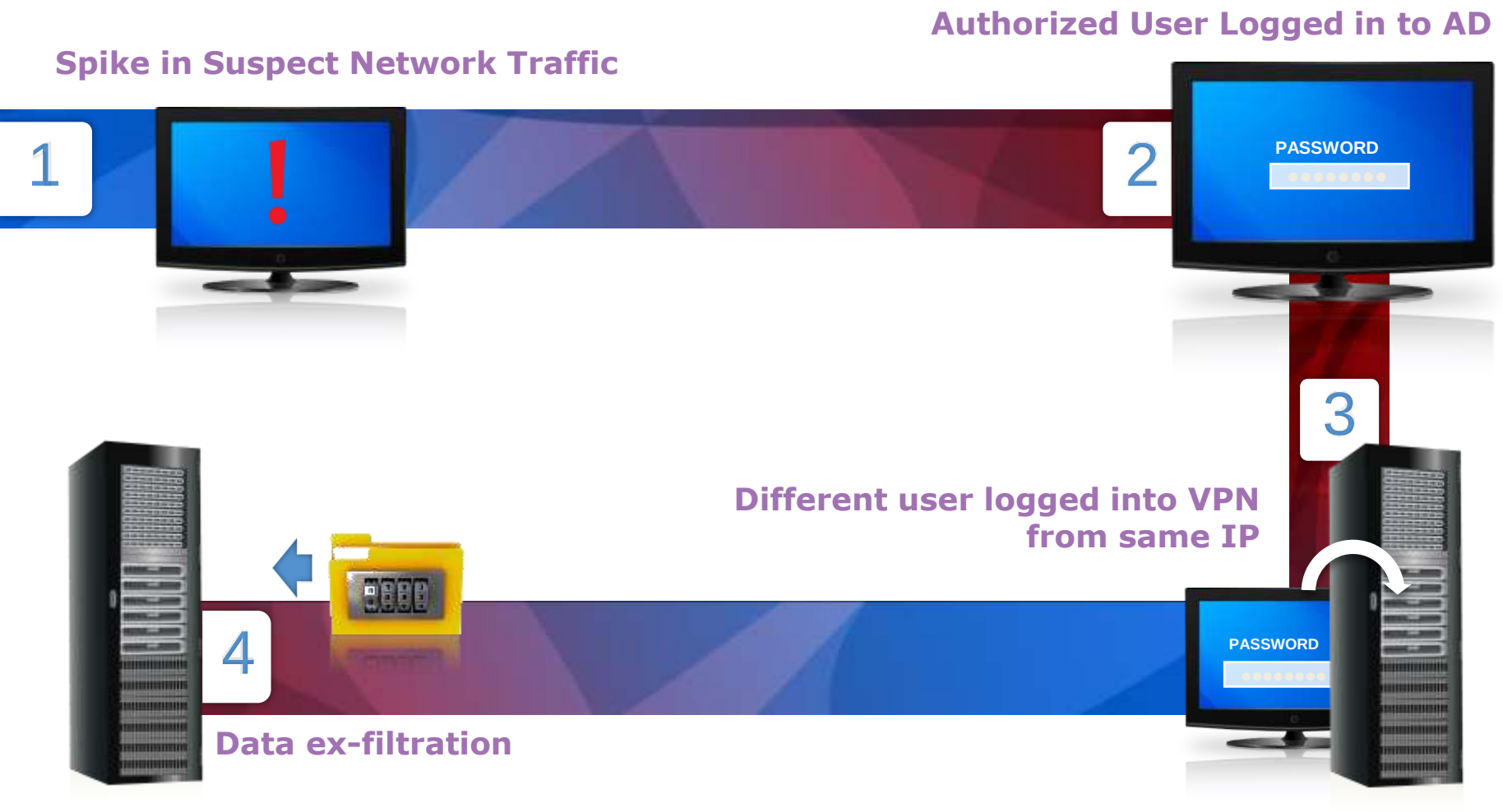
Actionable Intelligence

"Help me identify targets, threats & incidents"

Optimized Incident Management

"Enable me to manage these incidents"

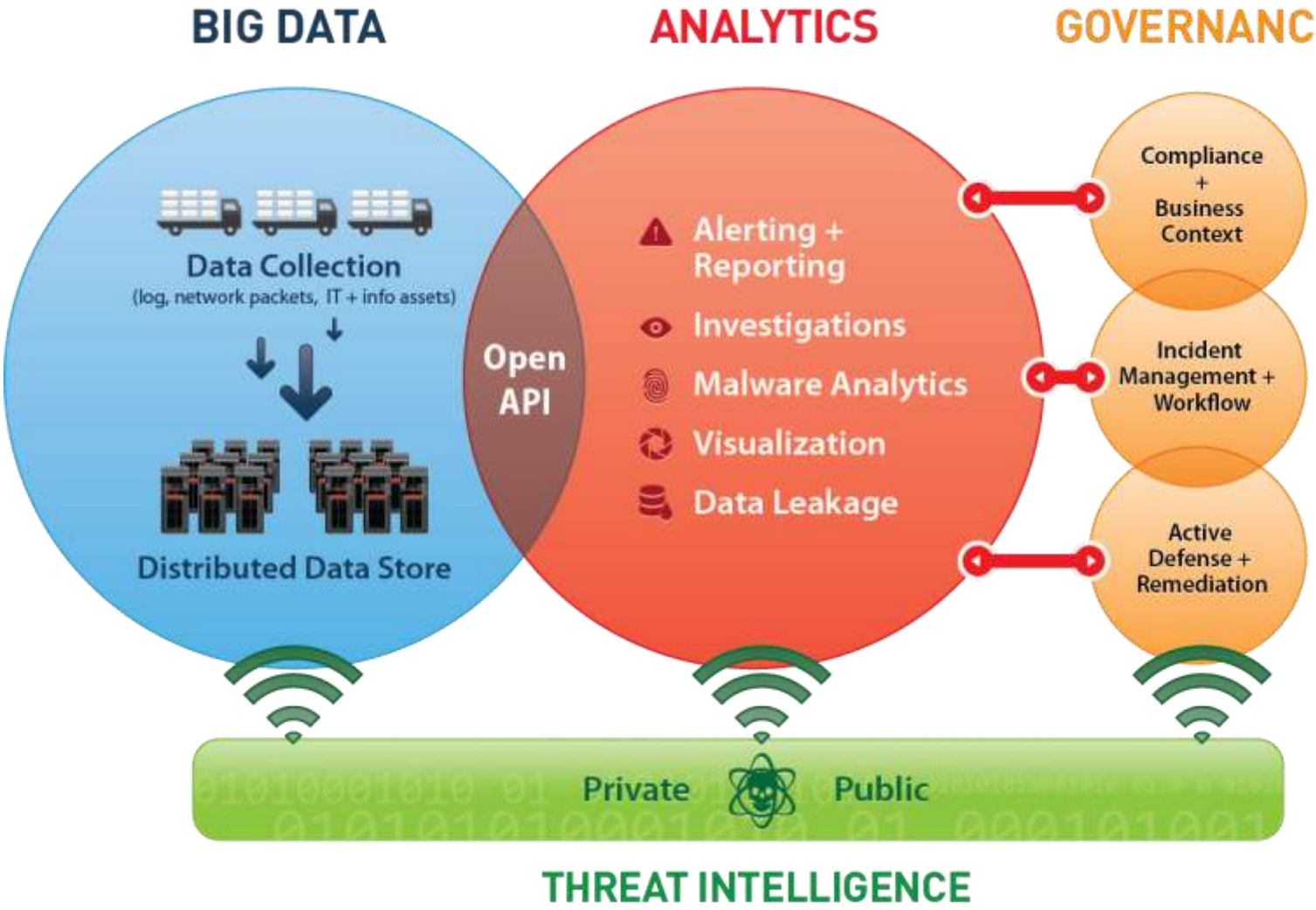
Suspect Attack Scenario



How do we detect and investigate?

Attack Step	SIEM Only	Logs and Network Packet Capture
Alert for RDP tunneled over non-standard port	No	Yes
Recreate activity of suspect IP address across environment	No	Yes
Show user activity across AD and VPN	Yes	Yes
Alert for different credentials used for AD and VPN	Yes	Yes
Reconstruct exfiltrated data	No	Yes

RSA Security Management Architecture



Deployment methodology

Real Example - NA Financial Insitution

The Situation…

- Attack initially detected via a call to the help desk
  - Bug in malware caused browser to fail
- Initial attack infected approximately 20 users
  - Investigations / responses took too long
  - Additional machines were affected after initial attack
- Limited historical context providing visibility to these type of attacks or 0 day attack
  - Security team were confident in initial containment
  - Days later additional machines were involved.
- The tools used were ineffective in providing the answers

Attack Investigation

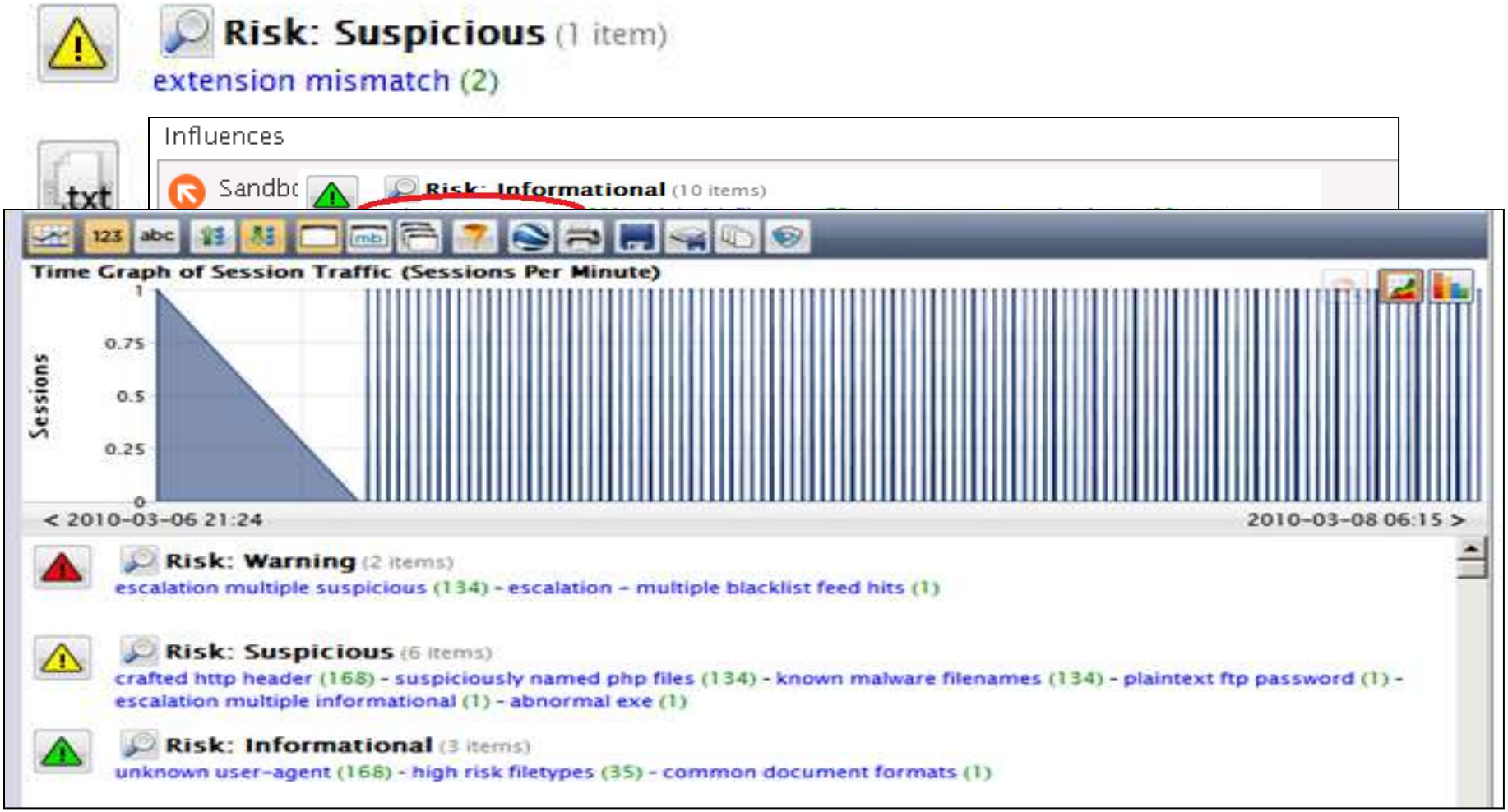
Downloaded through DLL disguised as HTML, TMP

Malware made changes to registry settings

Communicates with C2C server for further instruction

Propagated through null user sessions

With RSA Security Analytics



Taking this knowledge home

- When you get back to the office:
  - Evaluate the last 3 major security incidents you've had
  - Map out the people and data you used to detect and investigate
  - Evaluate which tasks took the longest
  - Create a map of all the data and skills you didn't have – but wish you had
- Create a plan for SOC improvement:
  - Define the resources you'd need to speed up resolution
  - Evaluate your current people, process and technologies' ability to handle incident data
  - Identify the low hanging fruit – the tedious non value-added tasks
  - Start with those tasks and create a roadmap to close gaps