

# Enterprise Security

Advanced Threat Detection & Response

Bert Hayes



# Agenda

- Agenda
- Introduction
- Security Program Critical Path
- Collecting Data to identify breaches
- Incident Response





**CYBER  
CRIMINALS**



**MALICIOUS  
INSIDERS**



**NATION  
STATES**

# Advanced Threats Are Hard to Find



**Cyber Criminals**



**Nation States**



**Insider Threats**



**100%**

Valid credentials were used



**40**

Average # of systems accessed



**229**

Median # of days before detection

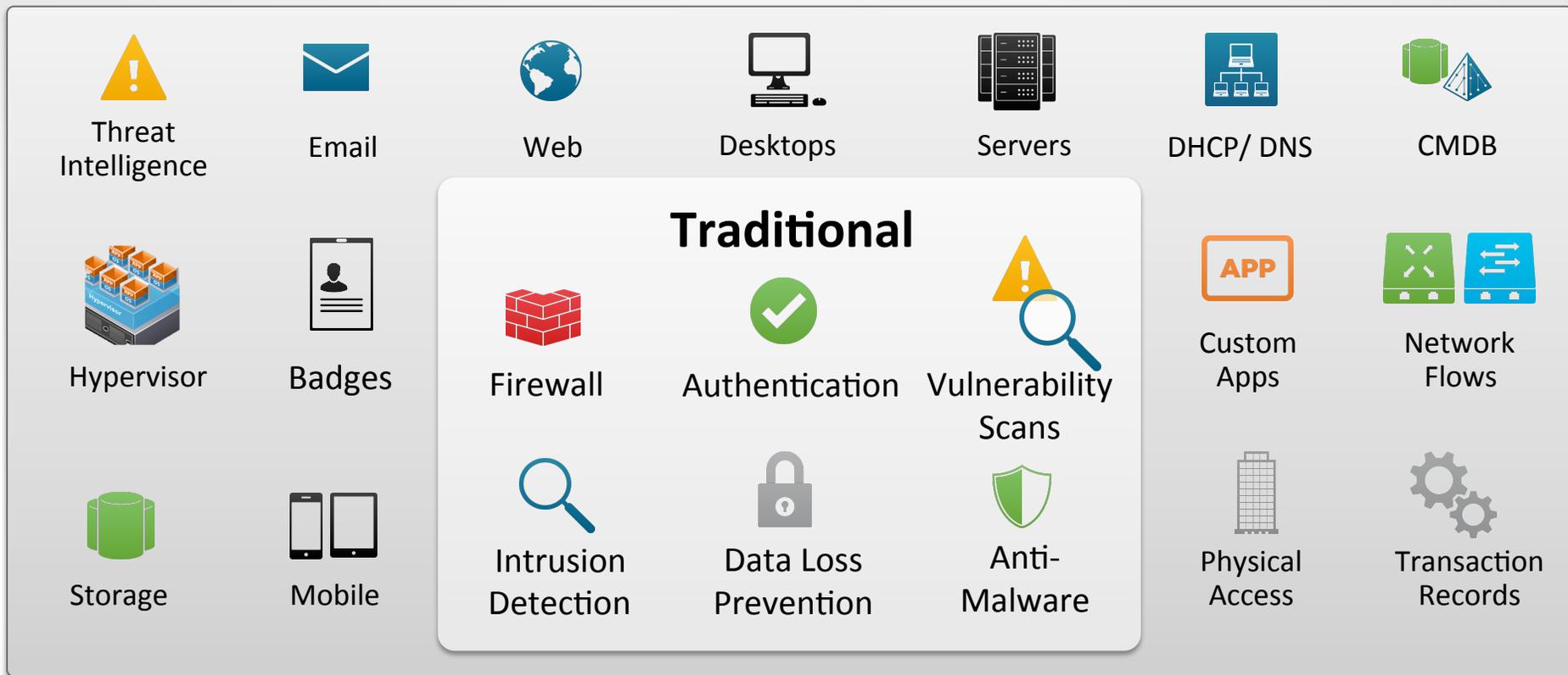


**67%**

Of victims were notified by external entity

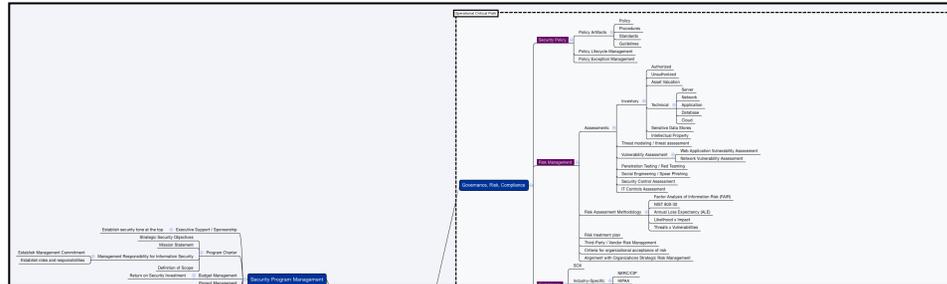
Source: Mandiant M-Trends Report 2012/2013/2014

# All Data is Security Relevant = Big Data

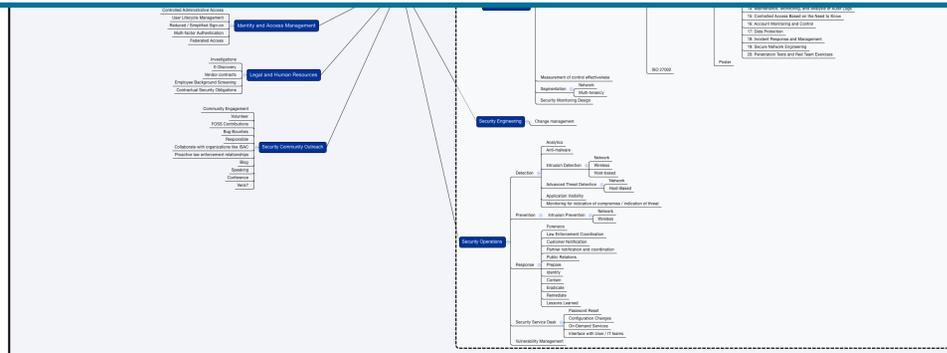




# Security Program: The Big Picture



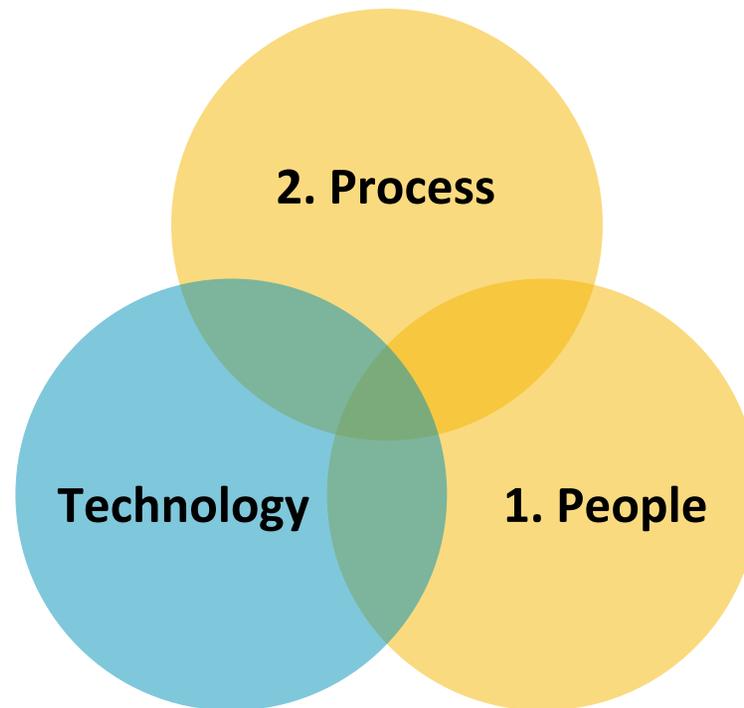
It's complicated...







# Then what?







# Security Critical Path



## Risk and Compliance

- Asset identification
- Risk
  - Assets
  - Threats (Actors, Actions, Modeling)
  - Vulnerabilities (Vulnerability management)
- Compliance
- **Outcome: Prioritized list of what to protect**









# Security Critical Path



## Risk

- Risk is an often misunderstood concept and term
- From a conversational perspective, think of risk like this
  - Risk = Likelihood X Impact
  - Risk = Threats X Vulnerabilities
- Significant Risk only exists with the potential for significant Loss
- If done properly, risk can (and should) be measured in monetary terms, literally: \$ £ €
- Risk frameworks to know:
  - Annualized Loss Expectancy (ALE) to be used as a counter-example (and to pass the CISSP exam!)
  - Factor Analysis of Information RISK (FAIR)

```
62 - - [02/Feb/2011:16:00:23] "GET /product.screen?product_id=FW-428;JSESSIONID=SD9SL4FF4ADFF8 HTTP/1.1" 200 3439 Windows NT 5.1; SV1; JET CL 11.0.0.200; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; JET CL 11.0.0.200) http://www.myflowershop.com/category_id=FLOWERS*  
category_id=FLOWERS* Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; JET CL 11.0.0.200) http://www.myflowershop.com/category_id=FLOWERS*  
d=TEDDY8;JSESSIONID=SD9SL4FF4ADFF8 HTTP/1.1" 200 3439 Windows NT 5.1; SV1; JET CL 11.0.0.200; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; JET CL 11.0.0.200) http://www.myflowershop.com/category_id=TEDDY*  
category_id=TEDDY* Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; JET CL 11.0.0.200) http://www.myflowershop.com/category_id=TEDDY*
```



# Security Critical Path

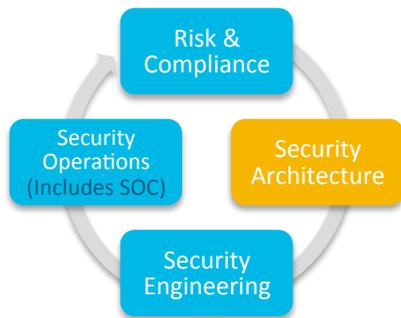


## Compliance

- Compliance is often prescriptive, not driven purely by risk analysis
- Controls and activities that do not effectively lower security risk are sometimes required
- If an organization does not have an experienced security team, sometimes compliance is more prominent than risk management
- Compliance is driven by
  - Region
  - Industry/vertical
  - Activities (Credit card processing, etc.)

Compliance can be just as important as Risk as a driver for future phases in the security critical path.

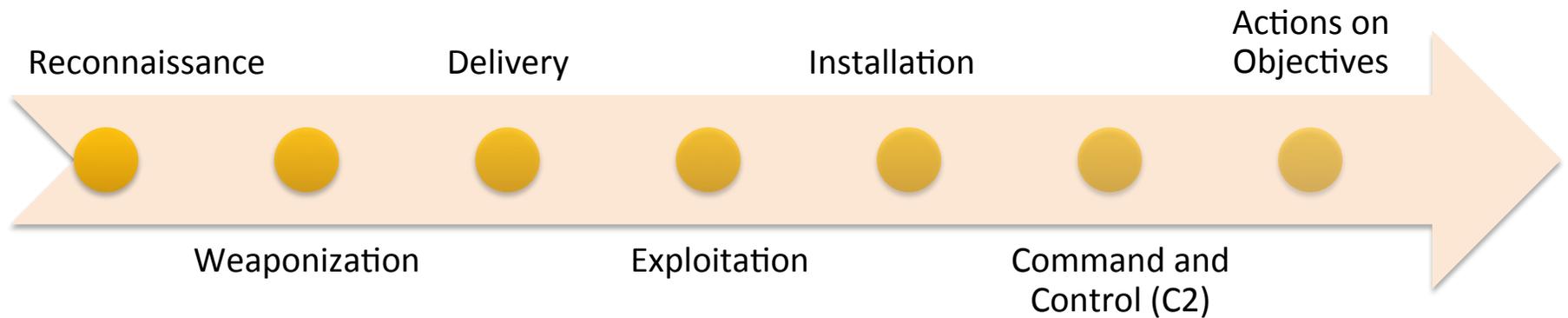
# Security Critical Path



## Security Architecture

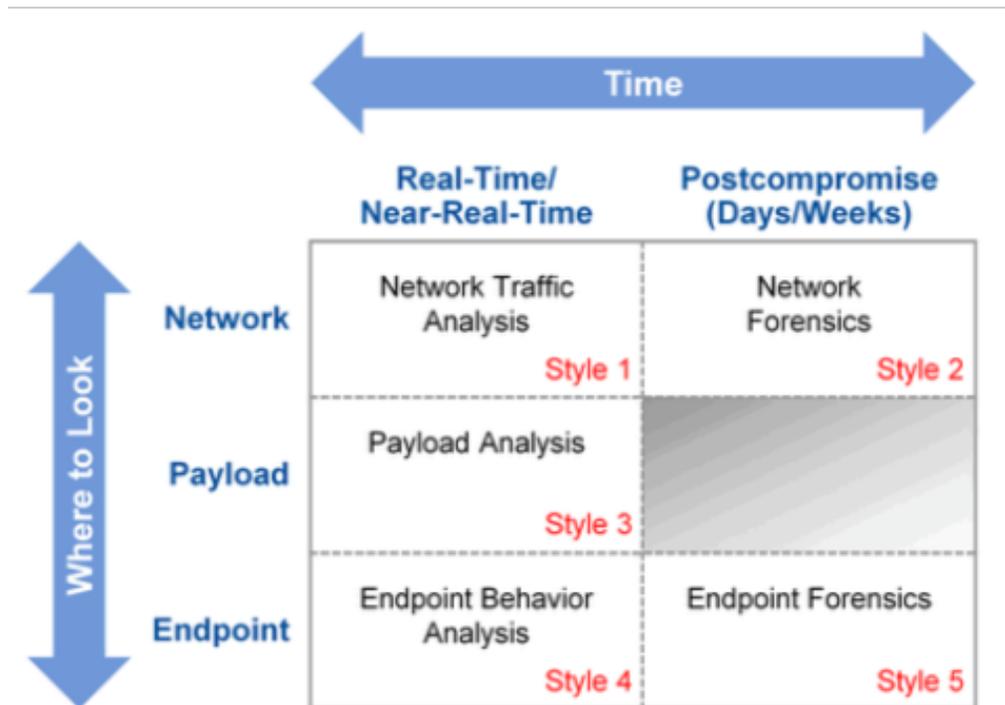
- Control Selection / Design
  - Defense in depth
  - CIS (SANS) 20 Critical Controls
  - ISO/IEC 27002
- Controls are also known as **countermeasures**
- Cost of the countermeasure should be less than the risk facing the organization
- Network security and monitoring architecture
- Interface with other teams
- **Outcome: What controls will be implemented, and where**

# Adversary Perspective - Attack Kill Chain



<http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>

# Gartner's Five Styles of APT Defense



Source: Gartner (August 2013)

















...product\_id=FI-SW-01...  
...category\_id=FLOWERS...  
...JSESSIONID=SD9SL4FF4DFF8...  
...category\_id=TEDDY...  
...JSESSIONID=SD1SL6FF3ADFF8...  
...category\_id=GIFTS...  
...JSESSIONID=SD4SL5FF2ADFF1...  
...LI-02...  
...category\_id=FLOWERS...  
...JSESSIONID=SD9SL4FF4DFF8...  
...category\_id=TEDDY...  
...JSESSIONID=SD1SL6FF3ADFF8...  
...category\_id=GIFTS...  
...JSESSIONID=SD4SL5FF2ADFF1...  
...LI-02...  
...category\_id=FLOWERS...  
...JSESSIONID=SD9SL4FF4DFF8...  
...category\_id=TEDDY...  
...JSESSIONID=SD1SL6FF3ADFF8...  
...category\_id=GIFTS...  
...JSESSIONID=SD4SL5FF2ADFF1...  
...LI-02...  
...category\_id=FLOWERS...  
...JSESSIONID=SD9SL4FF4DFF8...  
...category\_id=TEDDY...  
...JSESSIONID=SD1SL6FF3ADFF8...  
...category\_id=GIFTS...  
...JSESSIONID=SD4SL5FF2ADFF1...  
...LI-02...



Questions





# Best Practices – Breach Response Posture

- Bring in data from (minimum at least one from each category):
  - Network – next gen firewall or web proxy, email, dns
  - Endpoint – windows logs, registry changes, file changes
  - Threat Intelligence – open source or subscription based
  - Access and Identity – authentication events, machine-user mapping
- Employ a security intelligence platform so analysts can:
  - Contextualize events, analytics and alerts
  - Automate their analysis and exploration
  - Share techniques and results to learn and improve

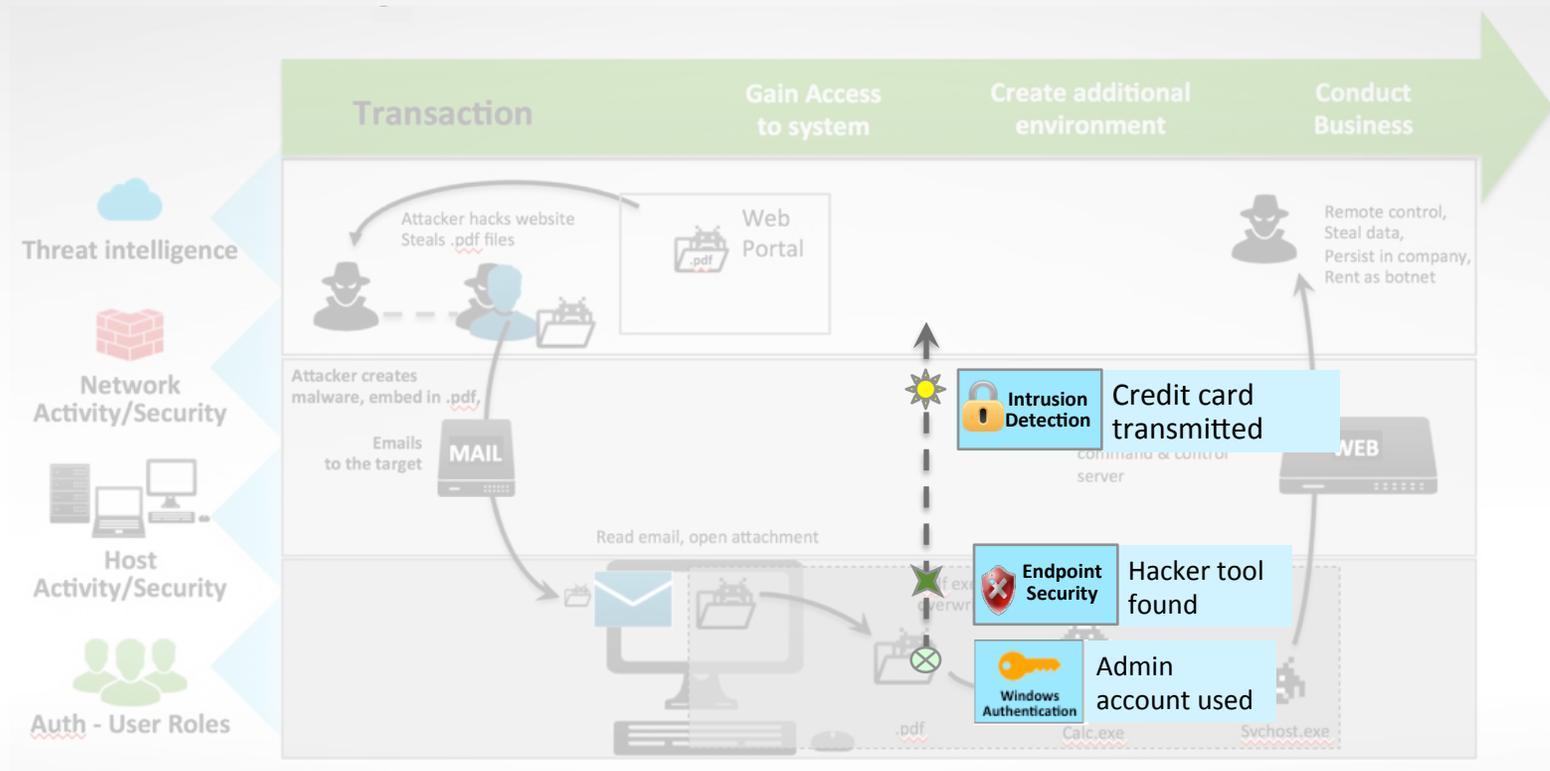
```
62 - - [02/Feb/2011:16:00:23] "GET /product.screen?product_id=FI-FW-428;JSESSIONID=SD9SL4FF4ADFF8 HTTP/1.1" 200 3439 Windows NT 5.1; SV1; JET CL 11.0.027.001; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; JET CL 11.0.027.001) Safari/534.112.102.7
```



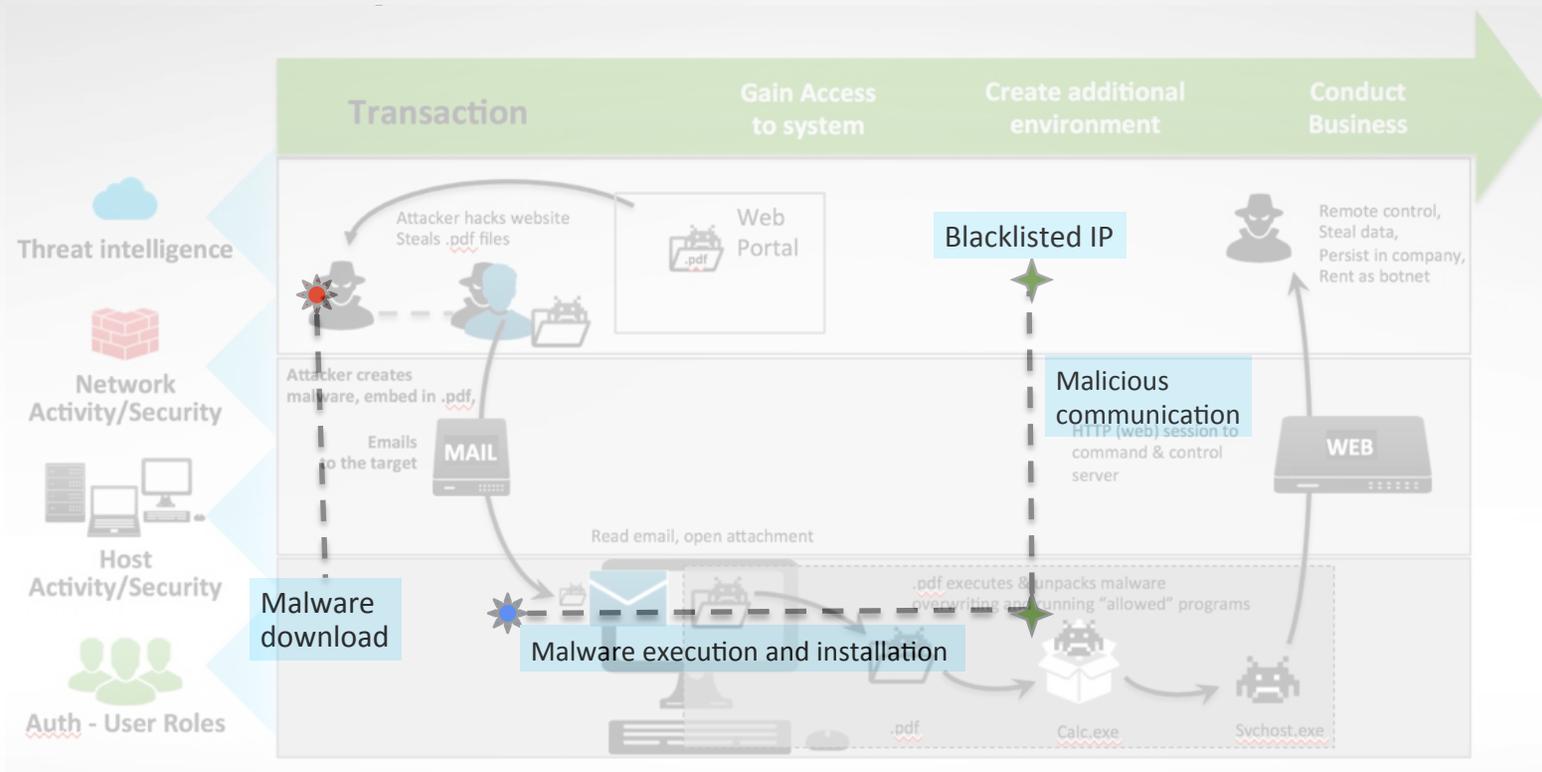




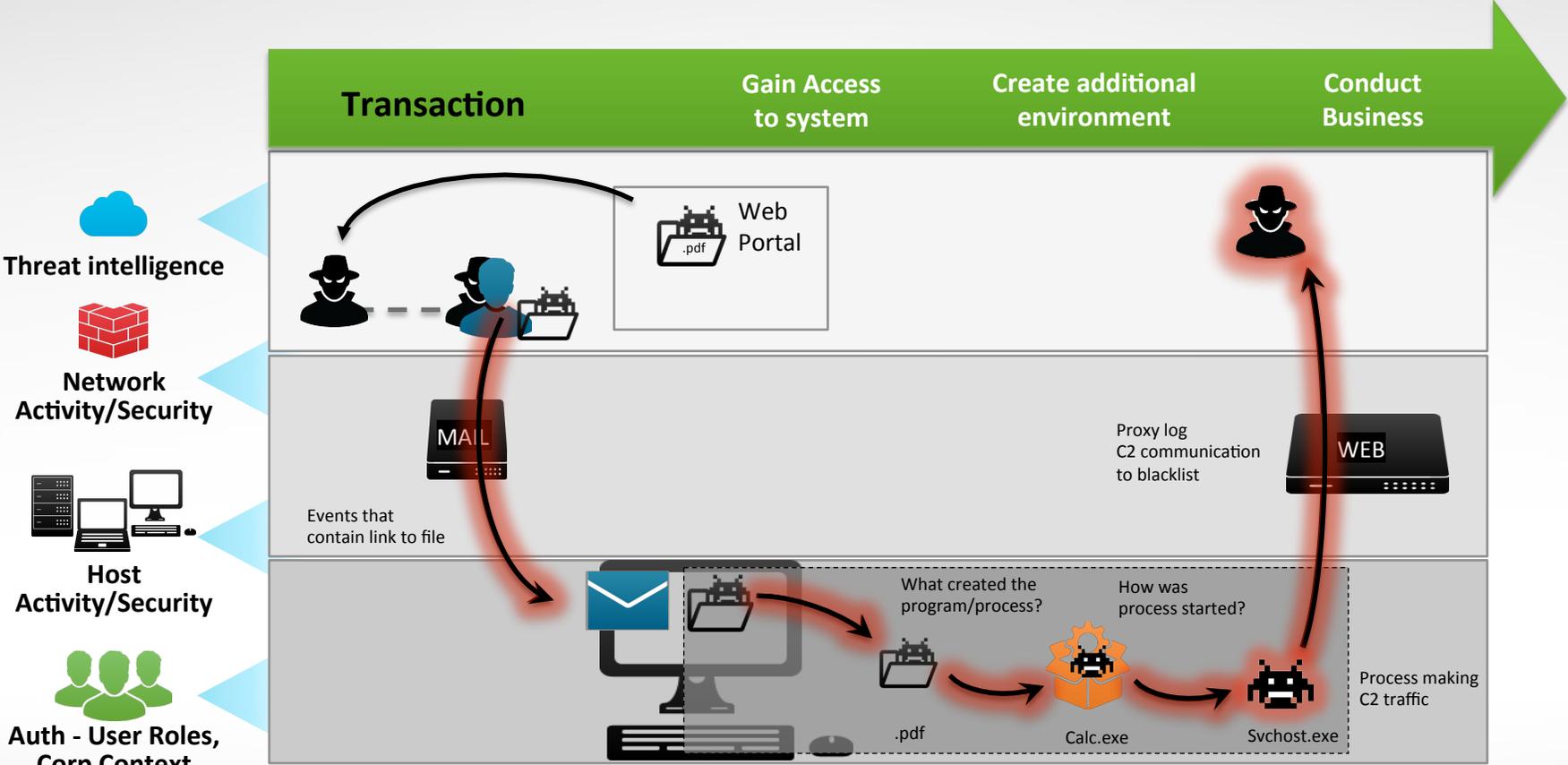
# Job Continues – Need to Perform Incident Investigation



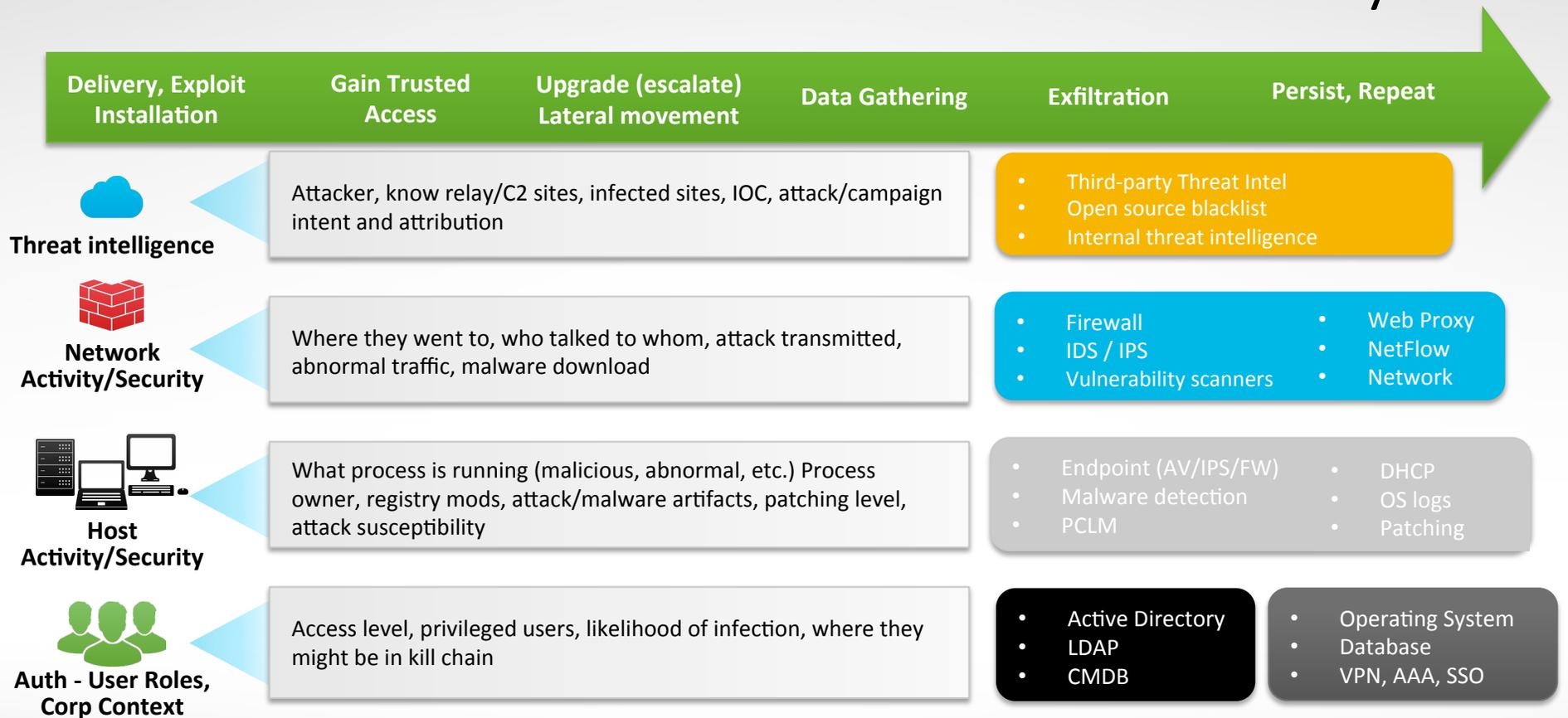
# Use Multiple Data Sources to Link Events



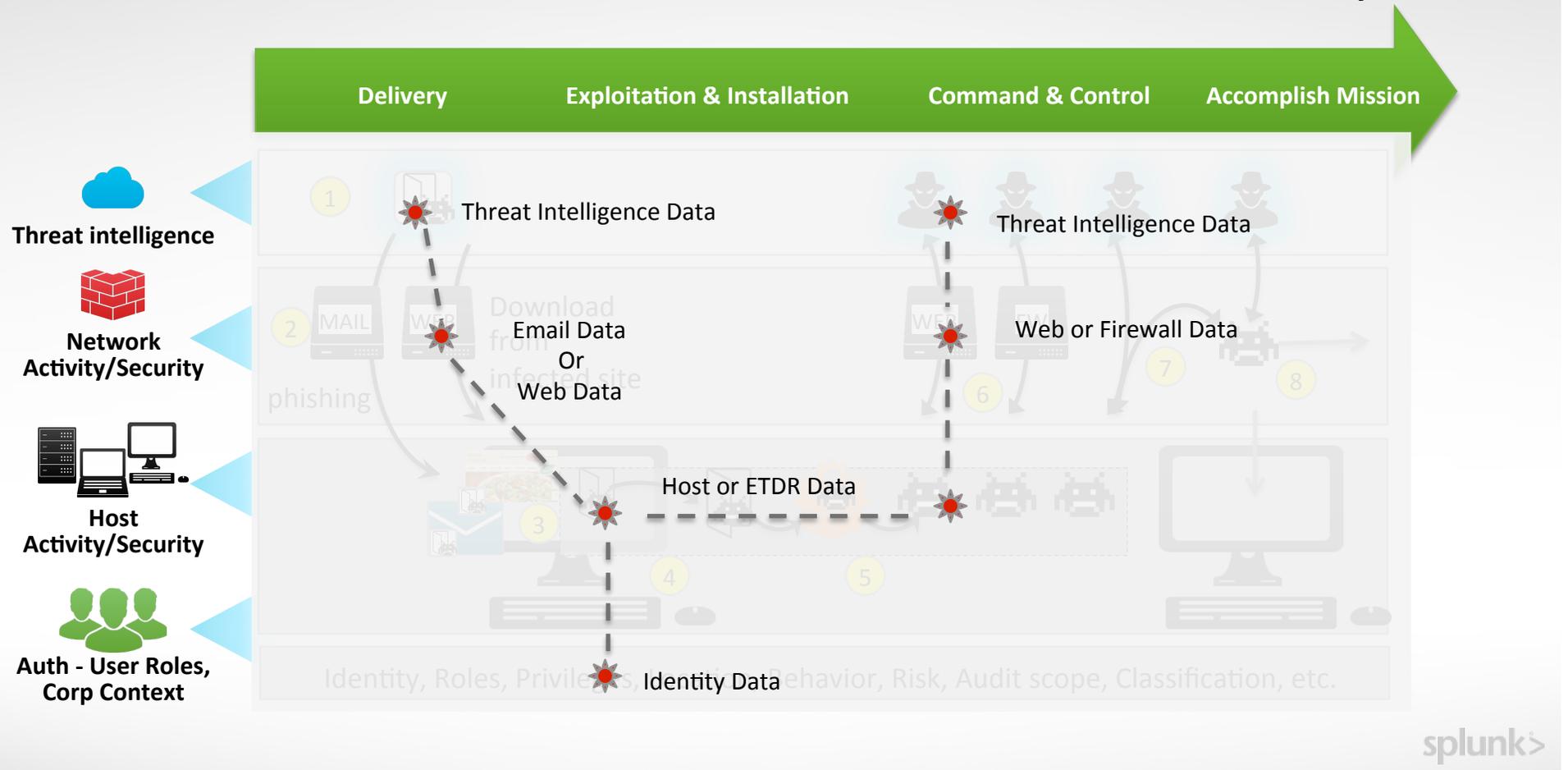
# Advanced Threat Detection & Response



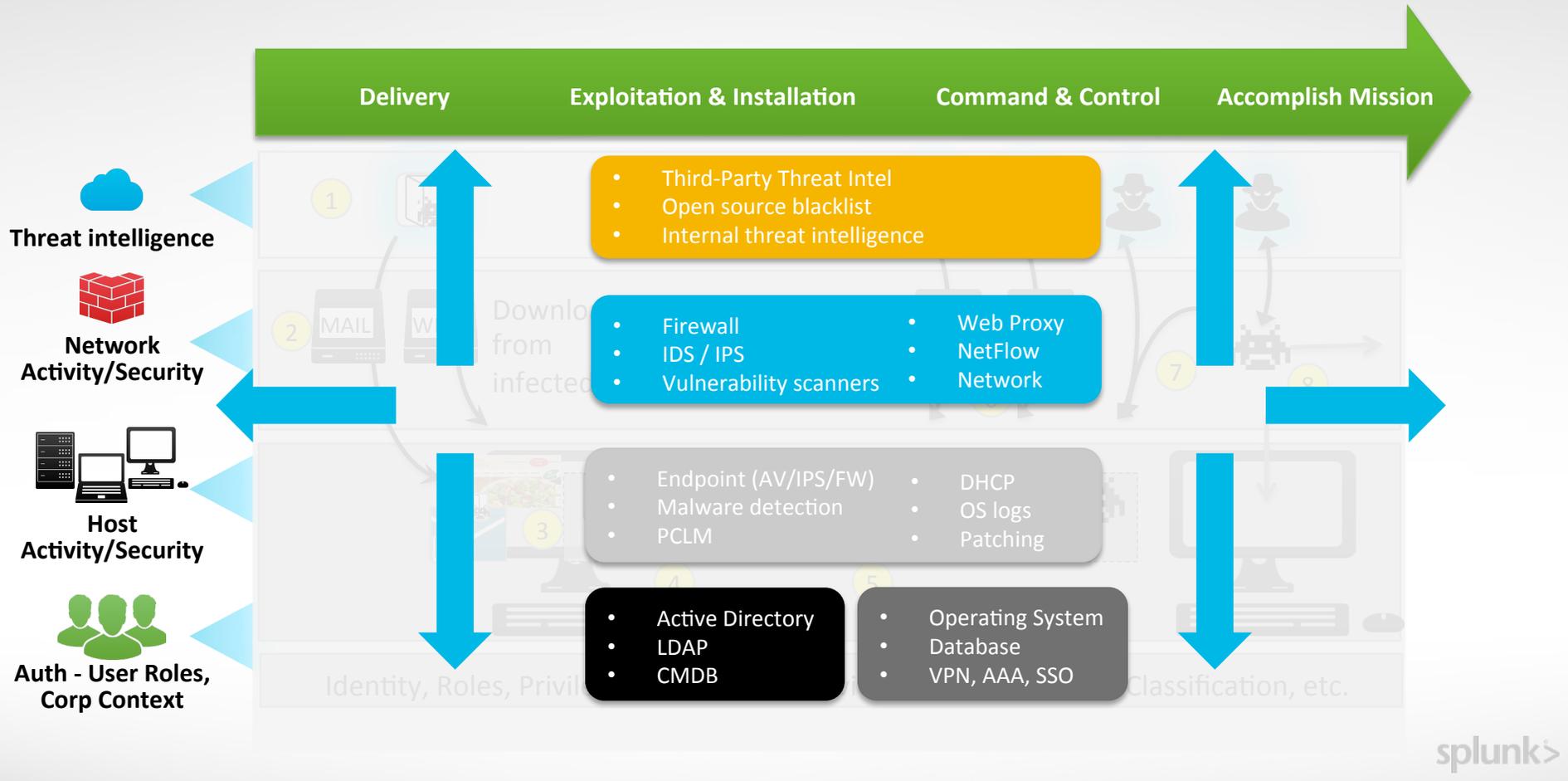
# Connect the “Data-Dots” to See the Whole Story



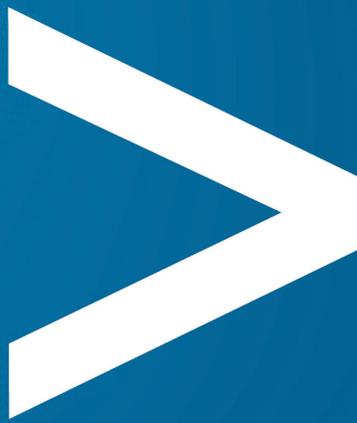
# Connect the “Data-Dots” to See the Whole Story



# Start Anywhere, Analyze Up-Down-Across-Backwards-Forward



...product\_id=FI-SW-01...  
...category\_id=FLOWERS...  
...JSESSIONID=SD9SL4FF4DFF8...  
...category\_id=TEDDY...  
...JSESSIONID=SD1SL6FF3ADFF8...  
...category\_id=GIFTS...  
...JSESSIONID=SD4SL5FF2ADFF1...  
...LI-02...  
...category\_id=FLOWERS...  
...JSESSIONID=SD9SL4FF4DFF8...  
...category\_id=TEDDY...  
...JSESSIONID=SD1SL6FF3ADFF8...  
...category\_id=GIFTS...  
...JSESSIONID=SD4SL5FF2ADFF1...  
...LI-02...  
...category\_id=FLOWERS...  
...JSESSIONID=SD9SL4FF4DFF8...  
...category\_id=TEDDY...  
...JSESSIONID=SD1SL6FF3ADFF8...  
...category\_id=GIFTS...  
...JSESSIONID=SD4SL5FF2ADFF1...  
...LI-02...  
...category\_id=FLOWERS...  
...JSESSIONID=SD9SL4FF4DFF8...  
...category\_id=TEDDY...  
...JSESSIONID=SD1SL6FF3ADFF8...  
...category\_id=GIFTS...  
...JSESSIONID=SD4SL5FF2ADFF1...  
...LI-02...



Thank You



# Rapid Ascent in the Gartner SIEM Magic Quadrant\*

**2015** Leader and the only vendor to improve its visionary position

**2014** Leader

**2013** Leader

**2012** Challenger

**2011** Niche Player

\*Gartner, Inc., SIEM Magic Quadrant 2011-2015. Gartner does not endorse any vendor, product or service depicted in its research publication and not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.





# Thriving Community

800+ apps

40,000+ questions  
and answers

Local User Groups  
and  
SplunkLive! events

Dev.splunk.com

