INTRUSION ALONG THE KILL CHAIN

four

- My name is four
- I work at facebook
- I'm obsessed with the problem of intrusion detection

This talk is a little bit different.

ACT I

... on the state of things ...

... and how well do they work?...


verizon

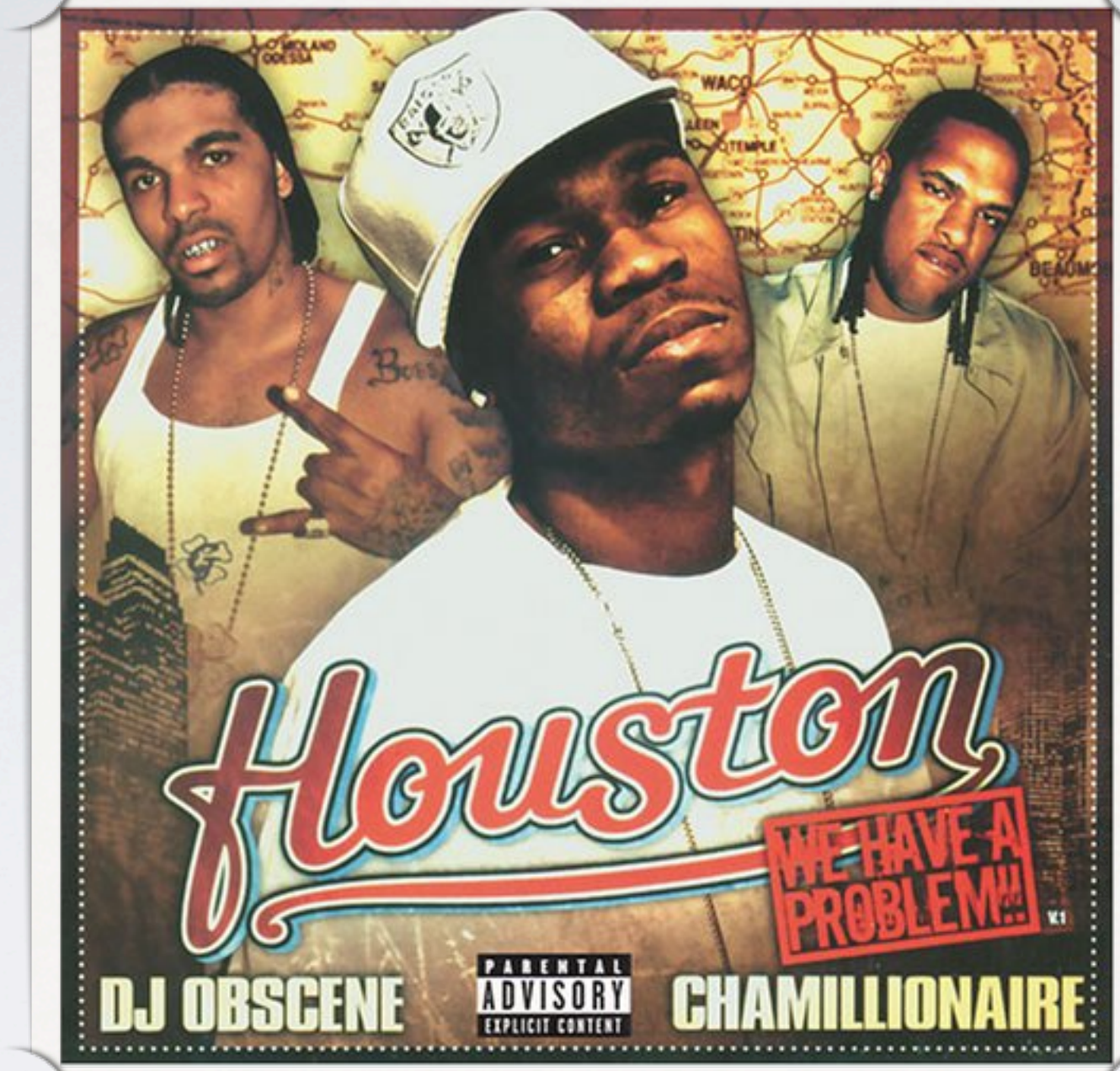
VERIZON

- 7 out of 10 targeted attacks against larger orgs
- Half of intrusions took *months* or *years* to discover
- Initial attack to compromise: 71% of the time in minutes or less
- 75% of the time: days or longer to exfil in larger orgs

VERIZON

- Discovery in larger orgs: Half are from 3rd parties.

- About 1/3: "hay something is weird"
- "Fraud detection" systems: 5%
- "Routine log review": 8%


WACO
Houston
WE HAVE A PROBLEM!!!
DJ OBSCENE
PARENTAL ADVISORY EXPLICIT CONTENT
CHAMILLIONAIRE

6% of advanced intrusions
detected by an internal process


Huston, we haz a problem
ICANHASCHEEZBURGER.COM

maybe the numbers are wrong?

ACT II

... a glimmer of hope ...

The art and science of finding actionable deviations between normal behavior and attacker behavior

Maximize your chance of getting lucky.

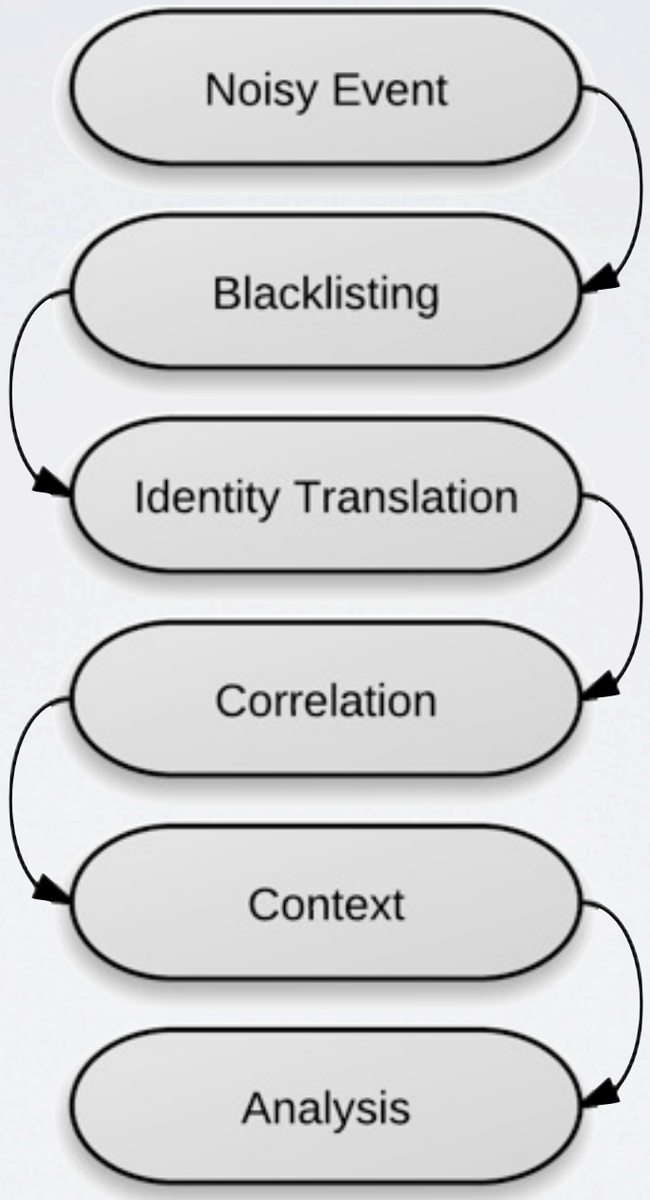
...intrusion events are not binary...

THE FALSE POSITIVE FALLACY

ALL EVENTS WELCOME

1. Snort event for a high confidence dns domain
2. Malicious PDF sent to a user
3. Logins for the same user from disparate geolocations
4. Netflow based alerts for known bad ip addresses
5. Specific Registry Modifications (i.e. Persistence)
6. Antivirus Alerts
7. Snort event for a blank useragent
8. Windows RDP successful login event
9. Snort event that alerts on all encrypted outbound traffic
10. Pcap data, Raw Logs, Netflow, etc.

THE EVENT PIPELINE



BLACKLISTING

IDENTITY TRANSLATION

ACT III

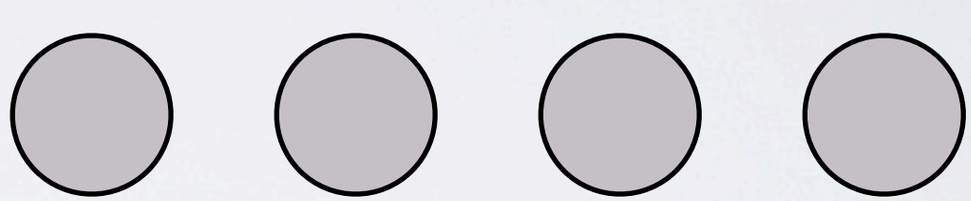
... advanced correlation ...

CORRELATION

group low confidence events
to find high confidence events

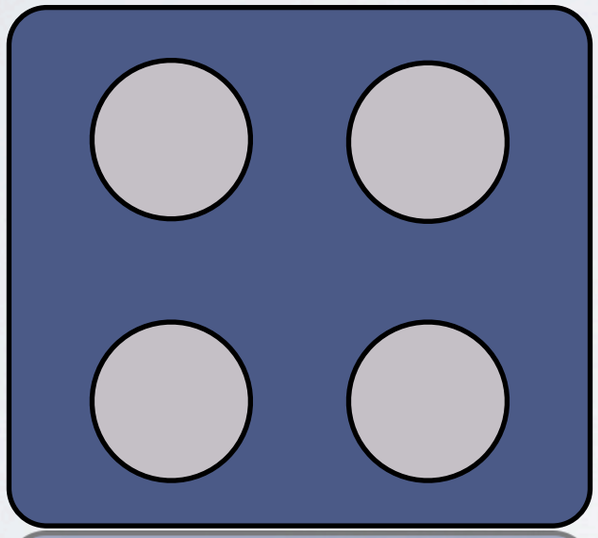
ATTACK PLANE

ATTACK PLANE ILLUSTRATED

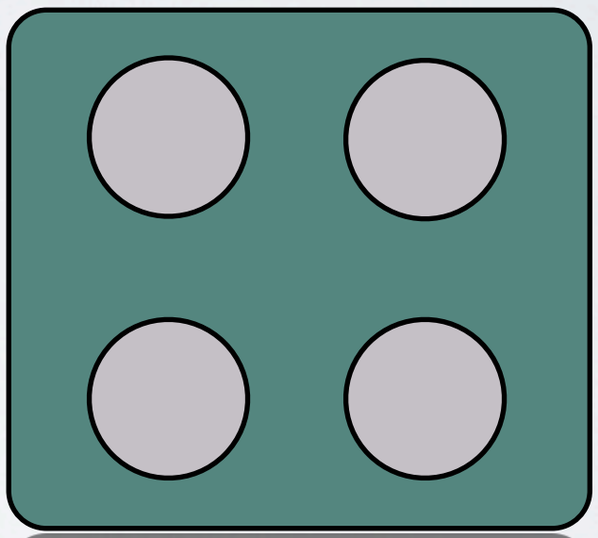


1.2.3.4

ATTACK PLANE ILLUSTRATED

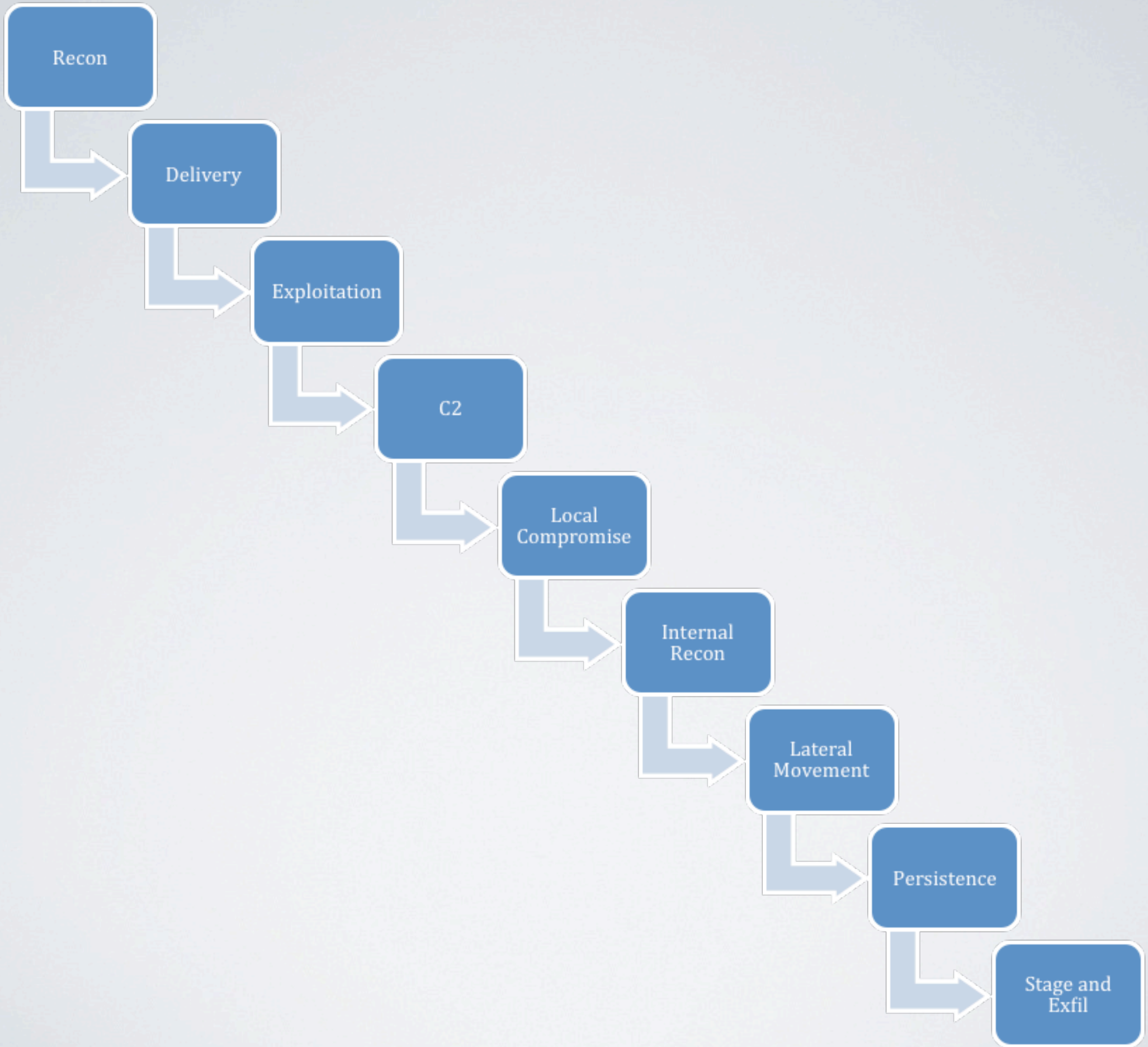


1.2.3.4



4.3.2.1

THE KILL CHAIN


Recon
Delivery
Exploitation
C2
Local Compromise
Internal Recon
Lateral Movement
Persistence
Stage and Exfil

KILL CHAIN AS ATTACK PLANE

uid:bob

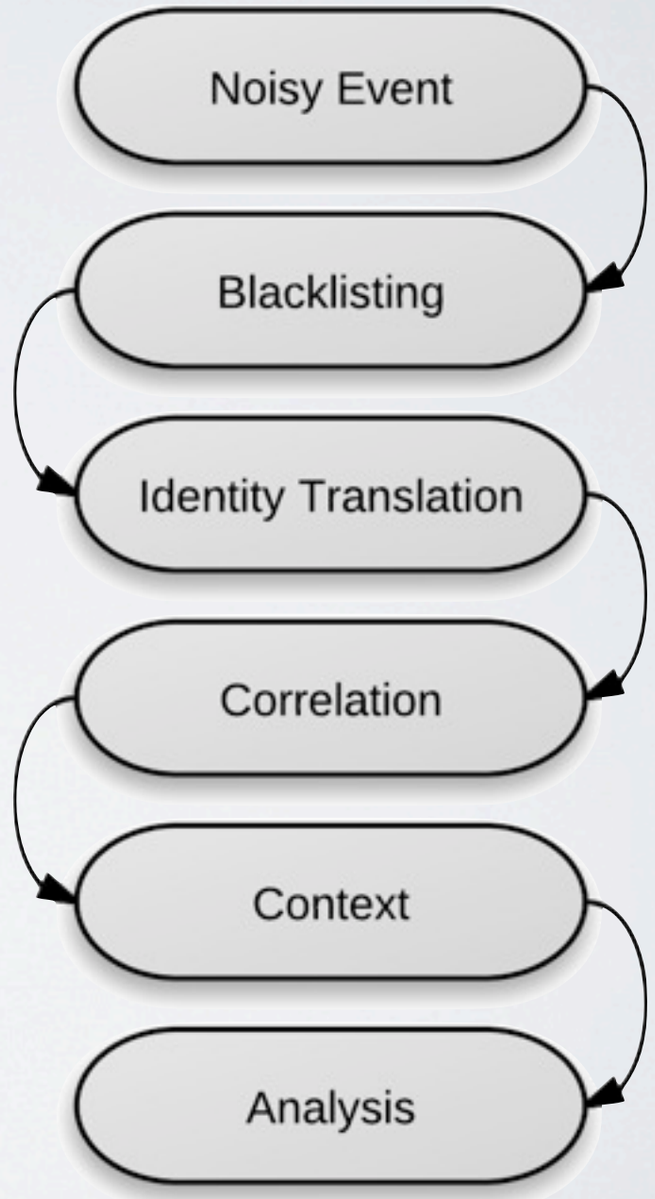
RECAP

- Love noisy events
- Reduce noise by blacklisting
- Correlation is your friend

CONTEXT

CONTEXT

- Context can speed up analysis
- Your products aren't just for making events
- Vendor products are an ecosystem
- Capabilities can provide events and context



FINAL THOUGHTS