

Filip Nowak – Security Incident Response SME

26-27 November 2014



Security Case Study Conference 2014

The Incident **Edge**

Executive Summary

Traditional security defenses focus so heavily on tactical tasks, that there is no time and effort to organize, coordinate and lead a detection-containment actions.

A brief history of security clearly prove that emerging attacks are multi-staged, persistent, and only possible to detect when you guess the plot threat.

By analyzing dependencies between events defenders are given the force multiplier - holistic view combined with situation awareness.

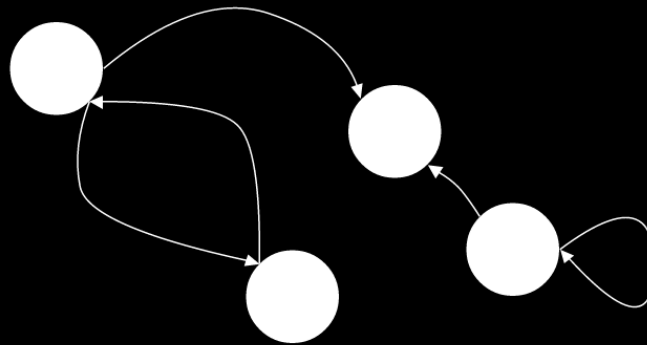
Organization that is using new methodology for event analysis is prepared to track dependent actions, quicker identify environmental dynamics, find historical correlation and drastically decrease MTTD.

Introduction

understand **history**
see the **present**
protect the **future**

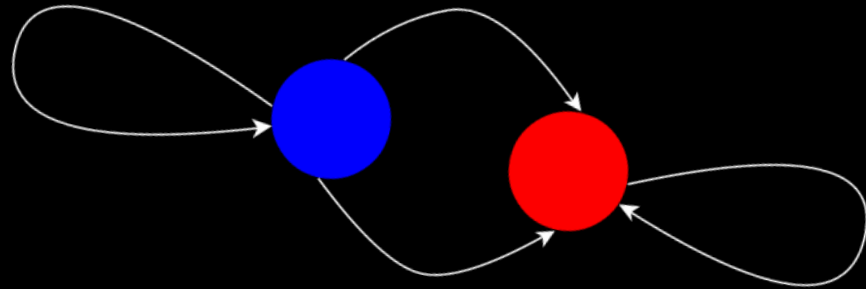
The purpose of this case study:

- ✓ present current research into ICS and operational level of defense
- ✓ describe problems with threat detection in big infrastructures
- ✓ explain how to analyze security events
- ✓ recommend new approach to event management and SA



Background concepts

- intrusion chain
- situational awareness
- one man SOC / hero model
- signal to noise improvement
- incident response process
- correlation amnesia vs. processing window



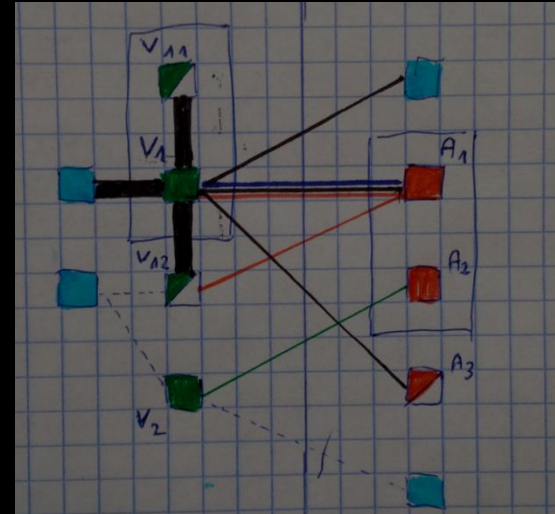
Challenges:

- Big Data (amnesia issue)
- heterogeneity and complexity of defense lines
- lack of the CJA
- IRP immaturity
- *noise to signal ratio (sensitivity)*
- *false positive (fidelity)*
- context vs. dynamics
- *signature-based, scenario-based (stages and time)*
- *mean time to detect*
- ...

Methodology

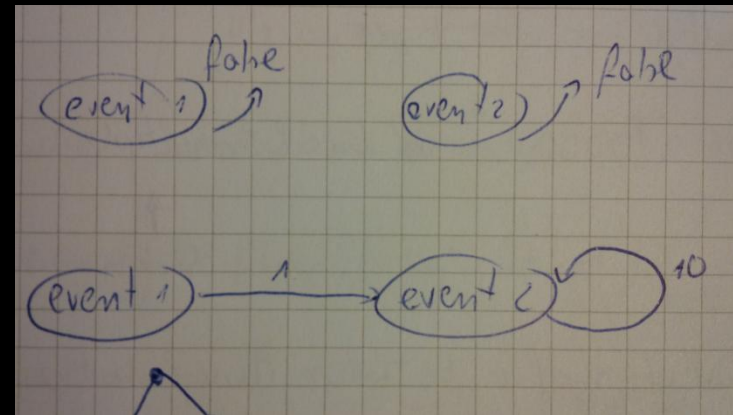
test samples:

- ✓ persistent attackers
- ✓ blue teaming
- ✓ tuning
- ✓ security events
- ✓ smash-and-grab



case analysis:

- ✓ retrospective investigation
- ✓ security breach analysis
- ✓ adversary campaign tracking
- ✓ extensive documentation and observation
- ✓ collaboration



Observation

where is the **Master Record**?



Observation

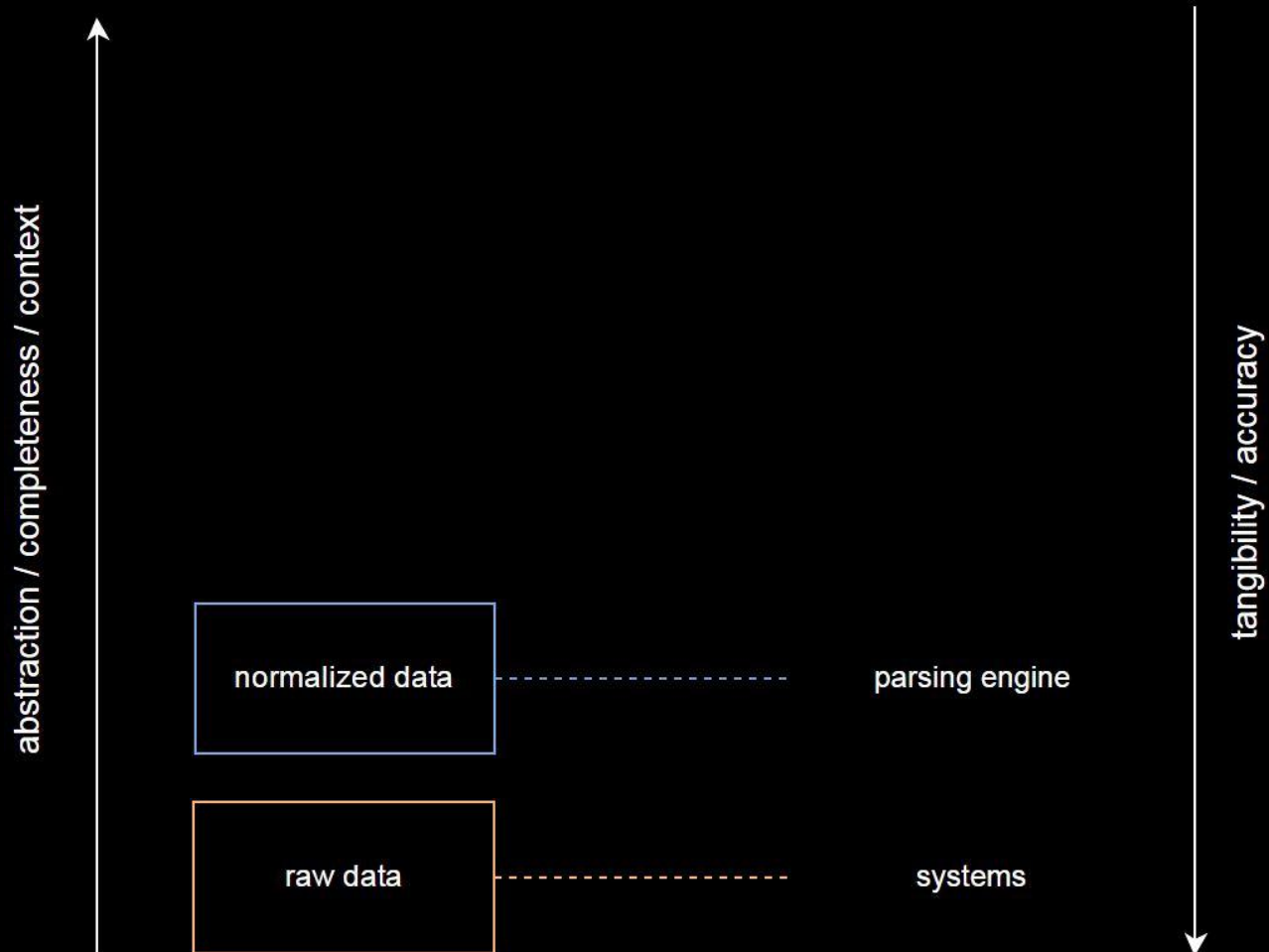
where is the **Master Record**?



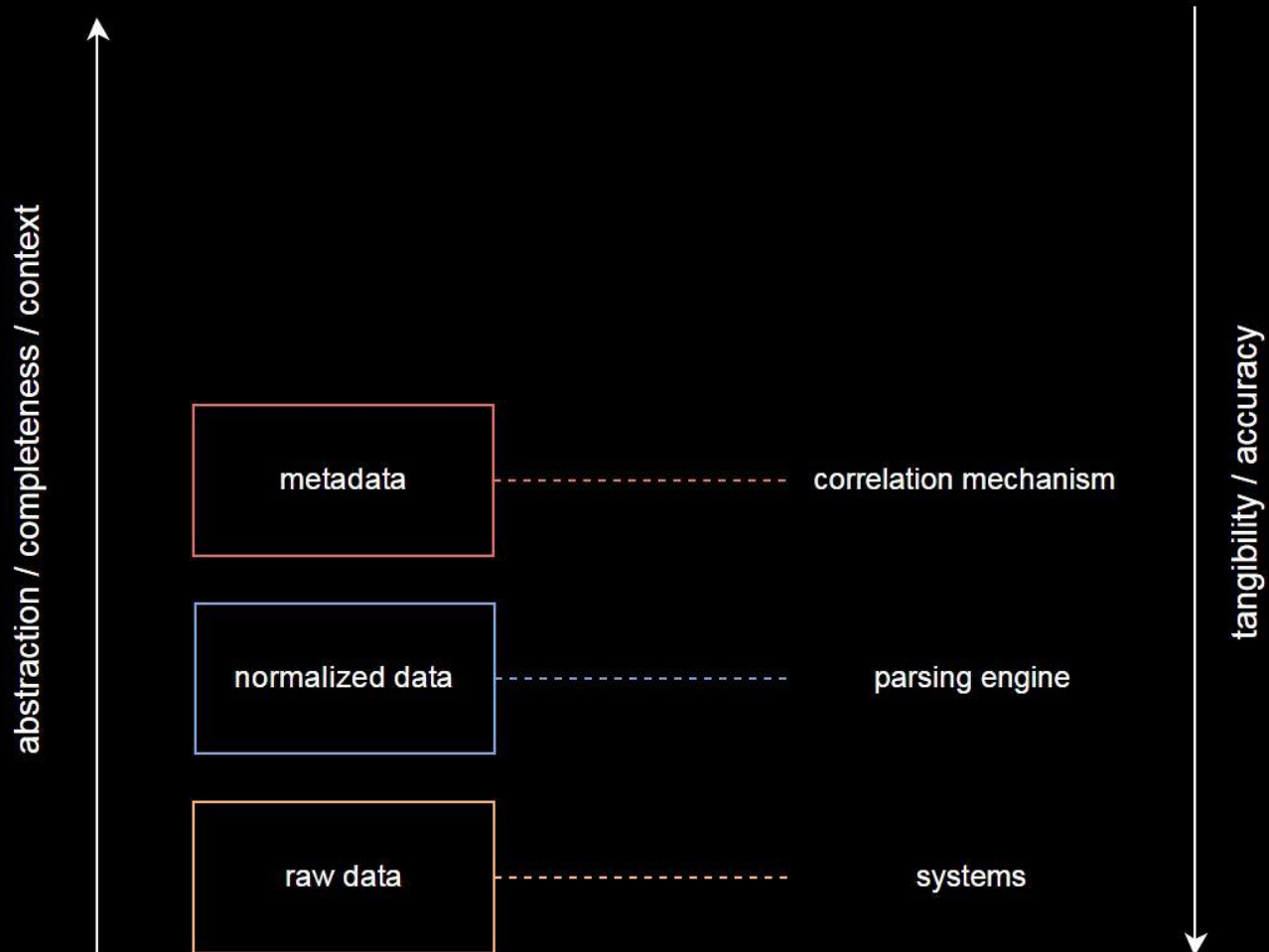
Observation



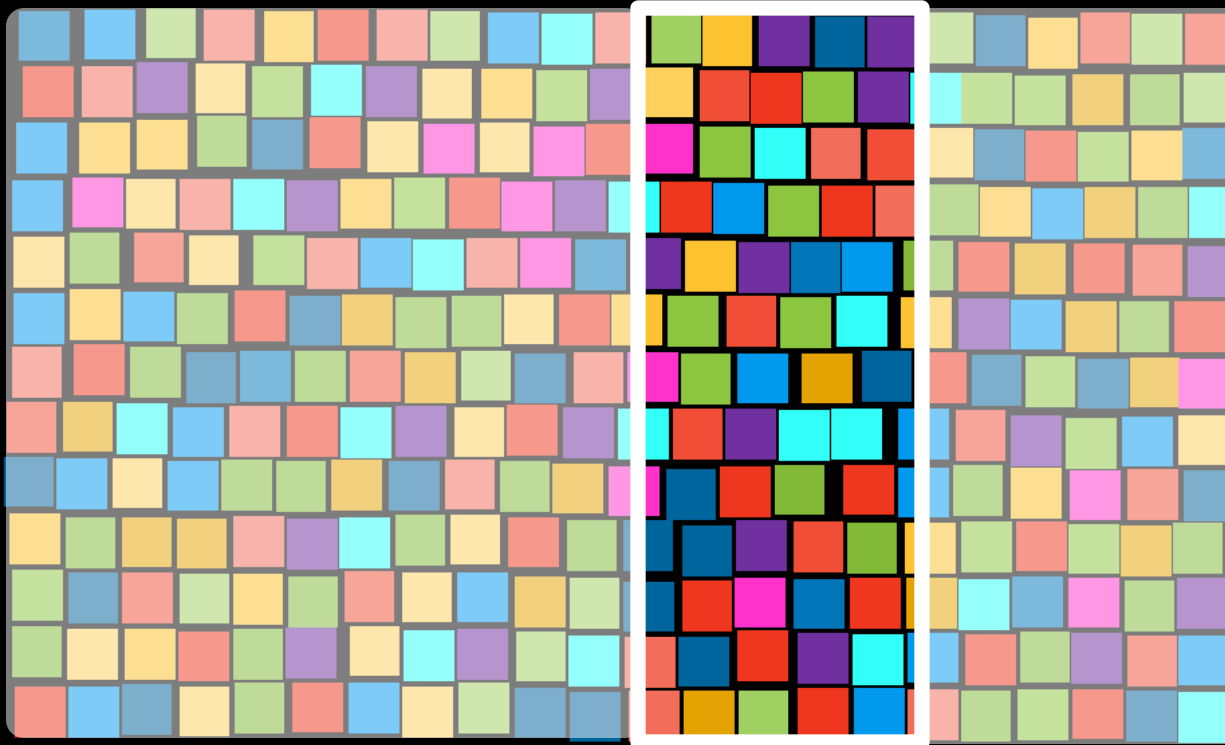
Observation



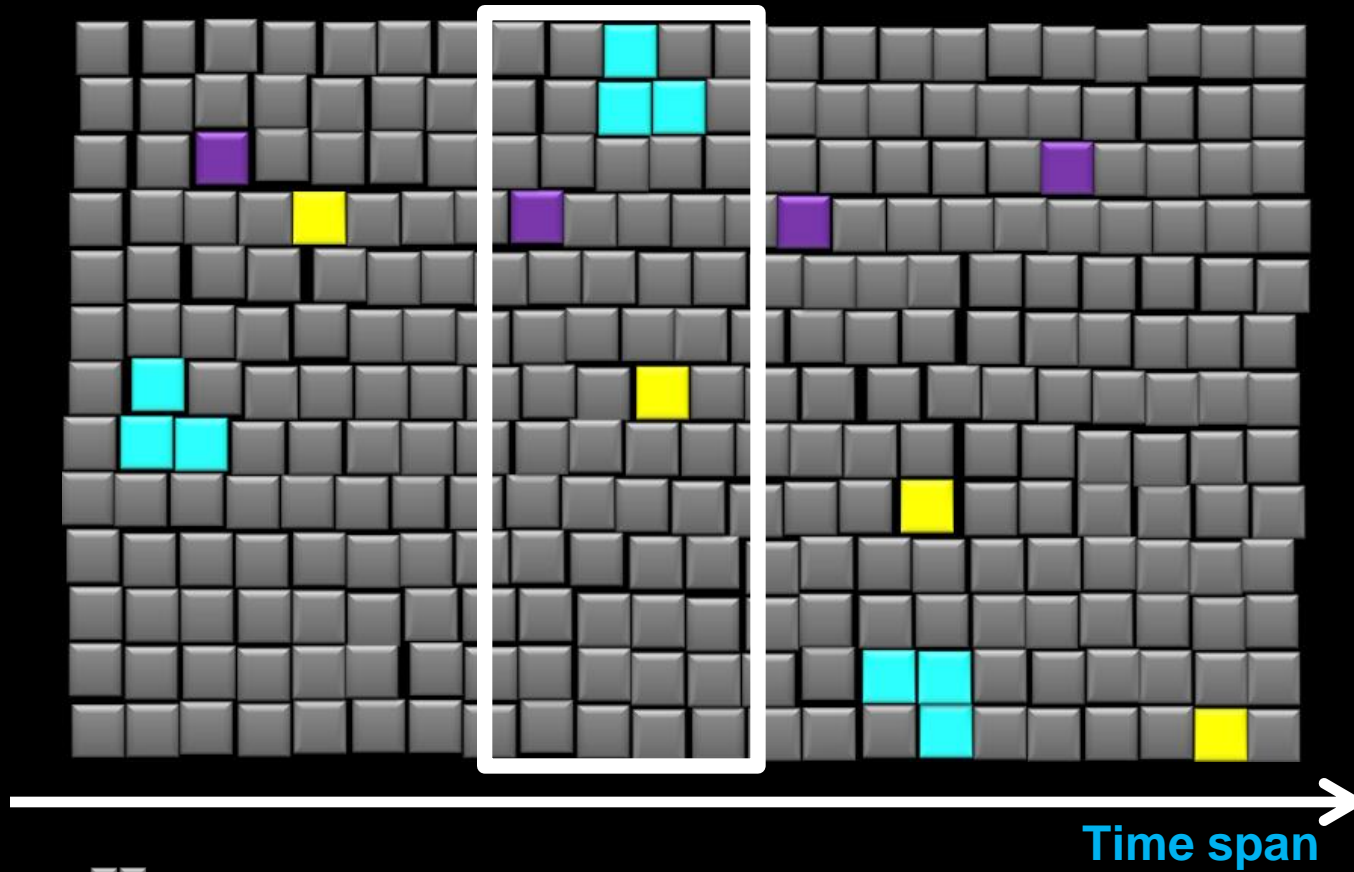
Observation




Event Horizon

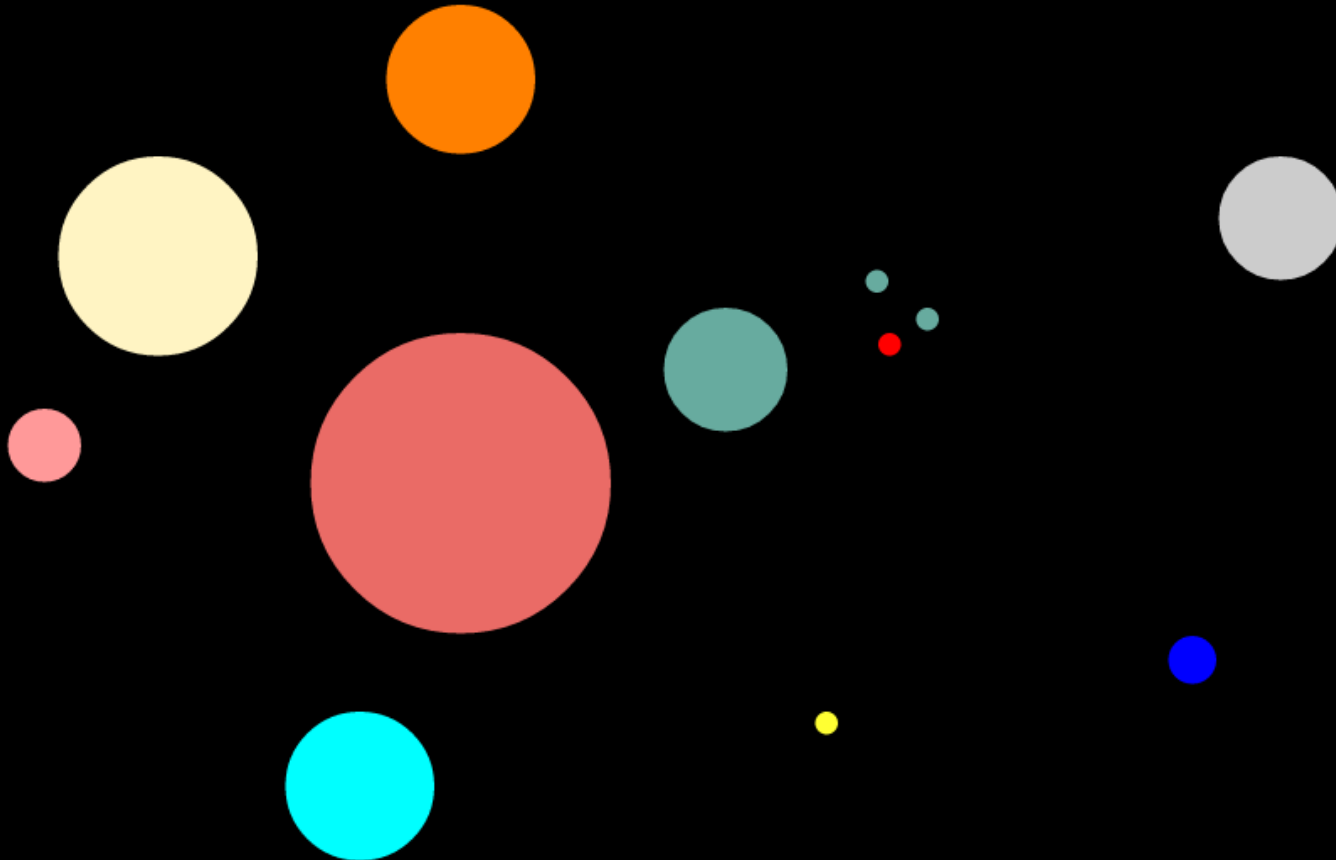


Security Event Tuning

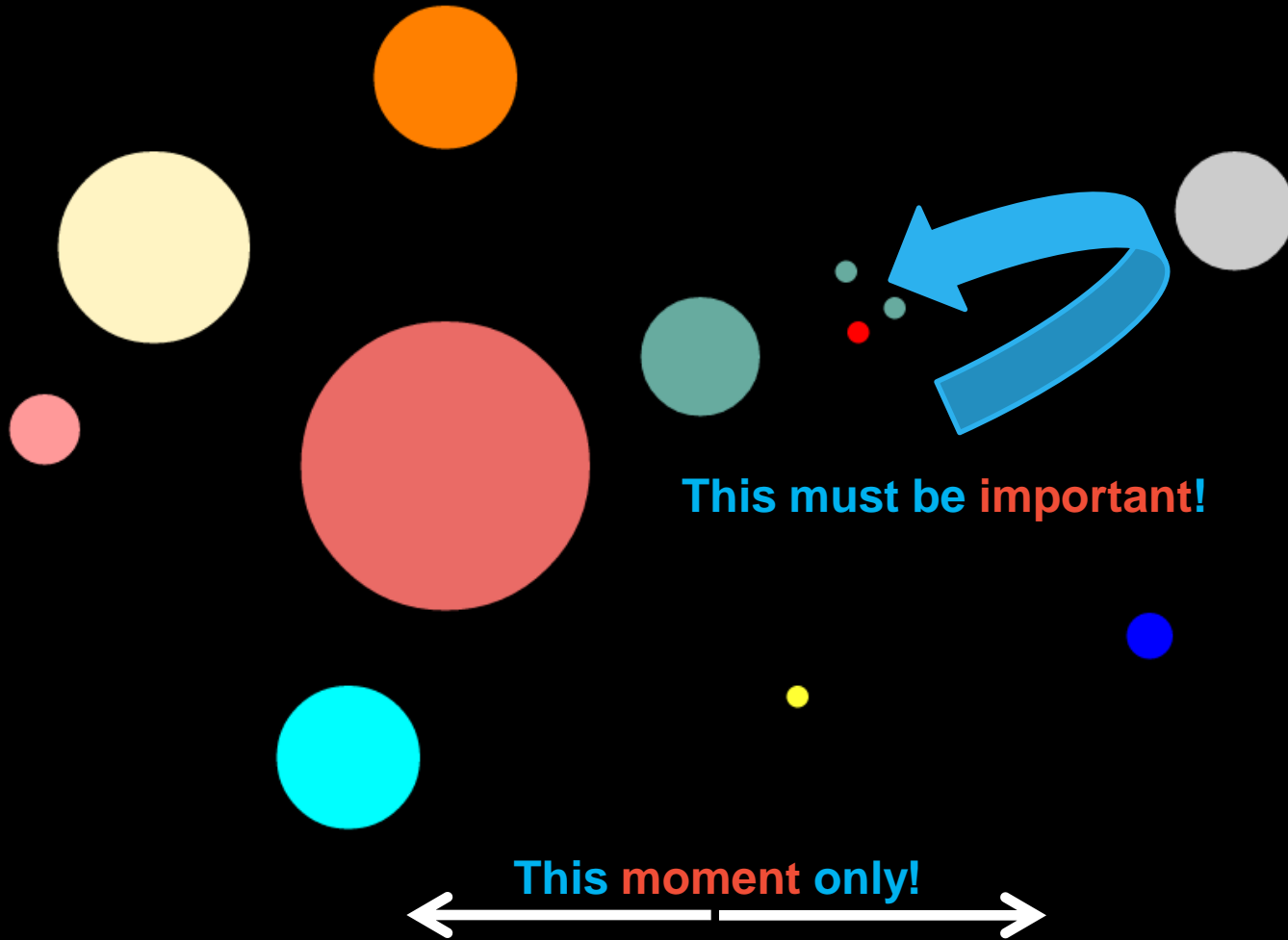


-  irrelevant events
-  detected activity
-  unseen actions

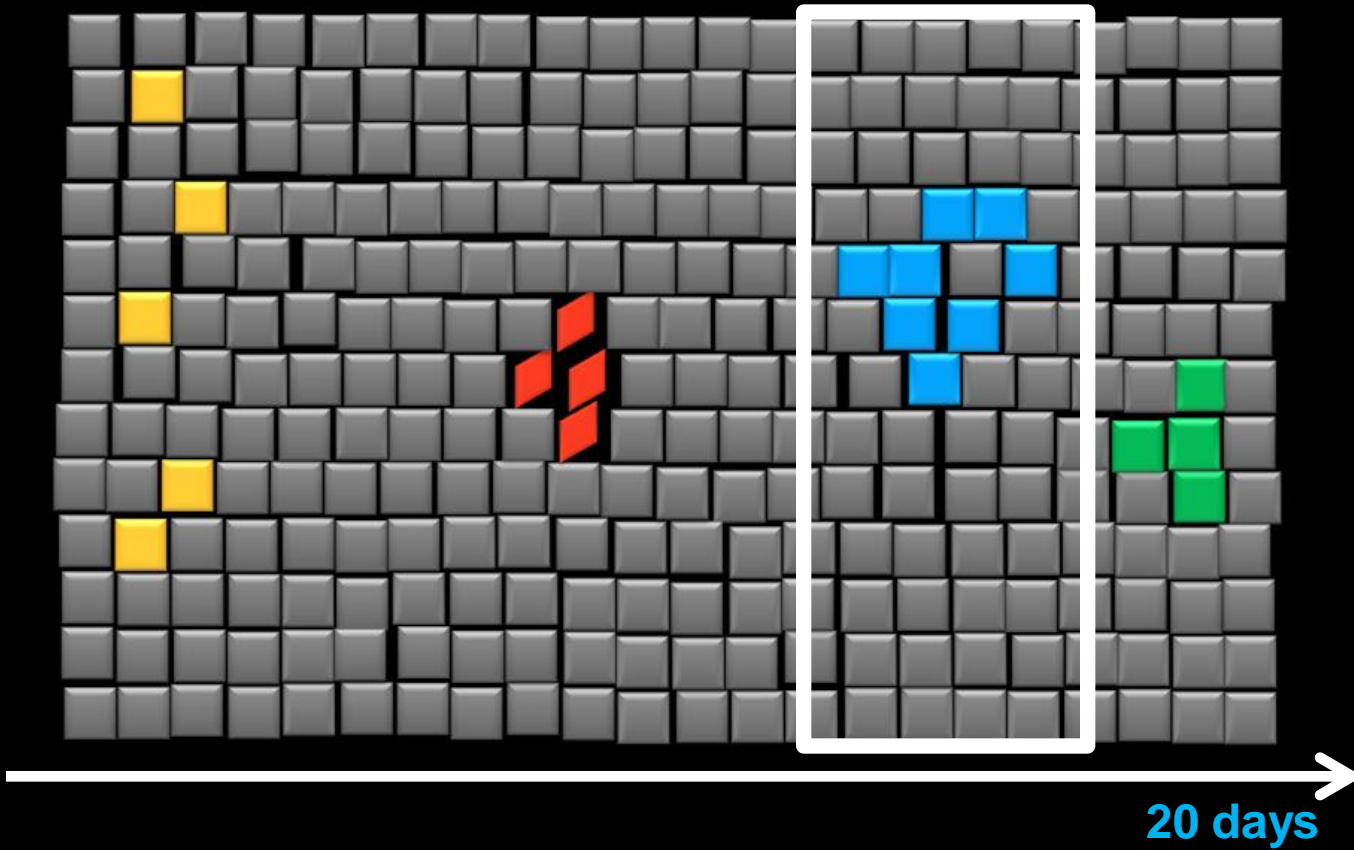
Findings and discussion #1



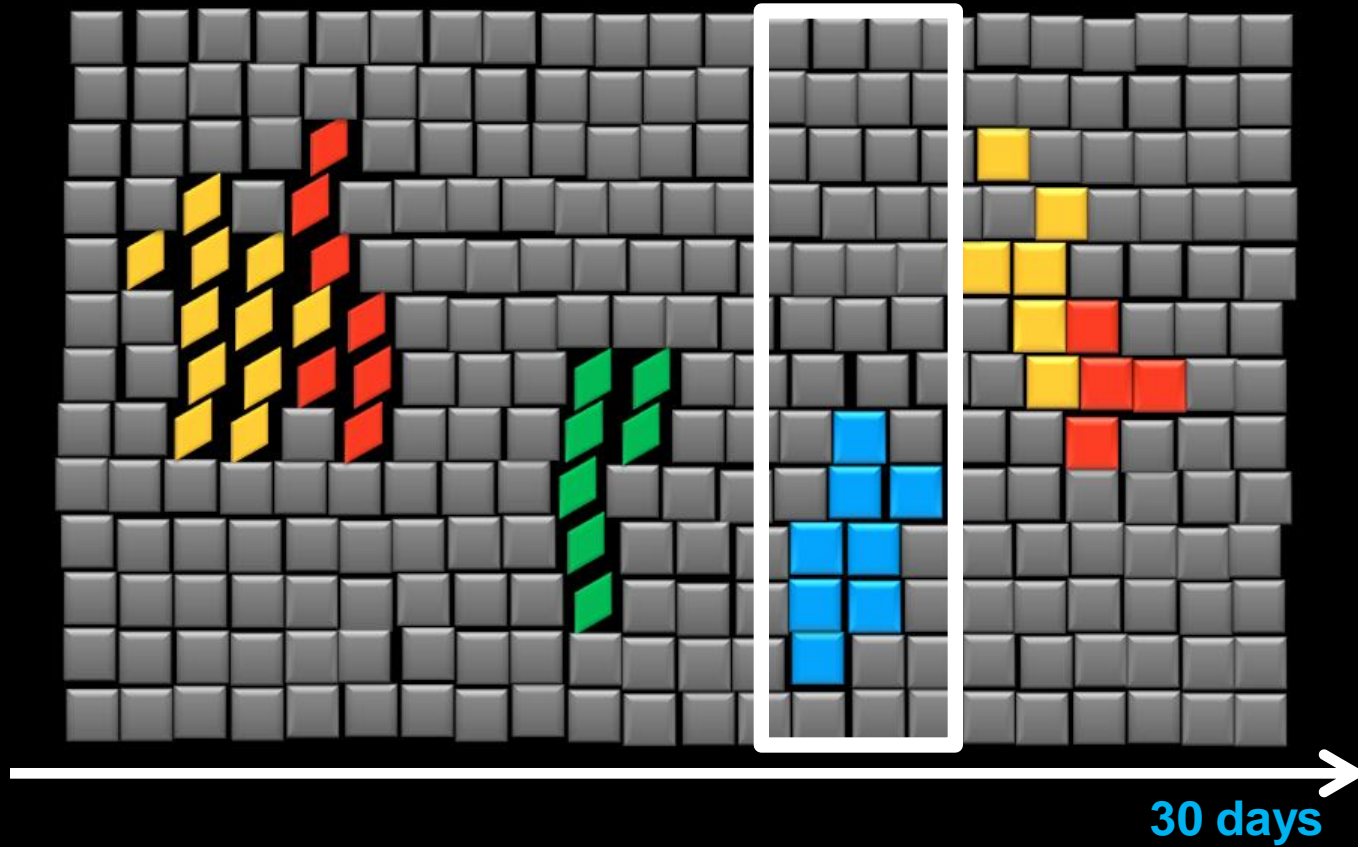
Findings and discussion #1




Adversary campaign

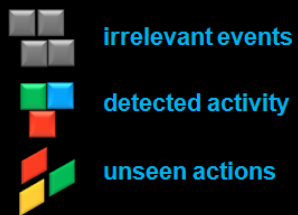
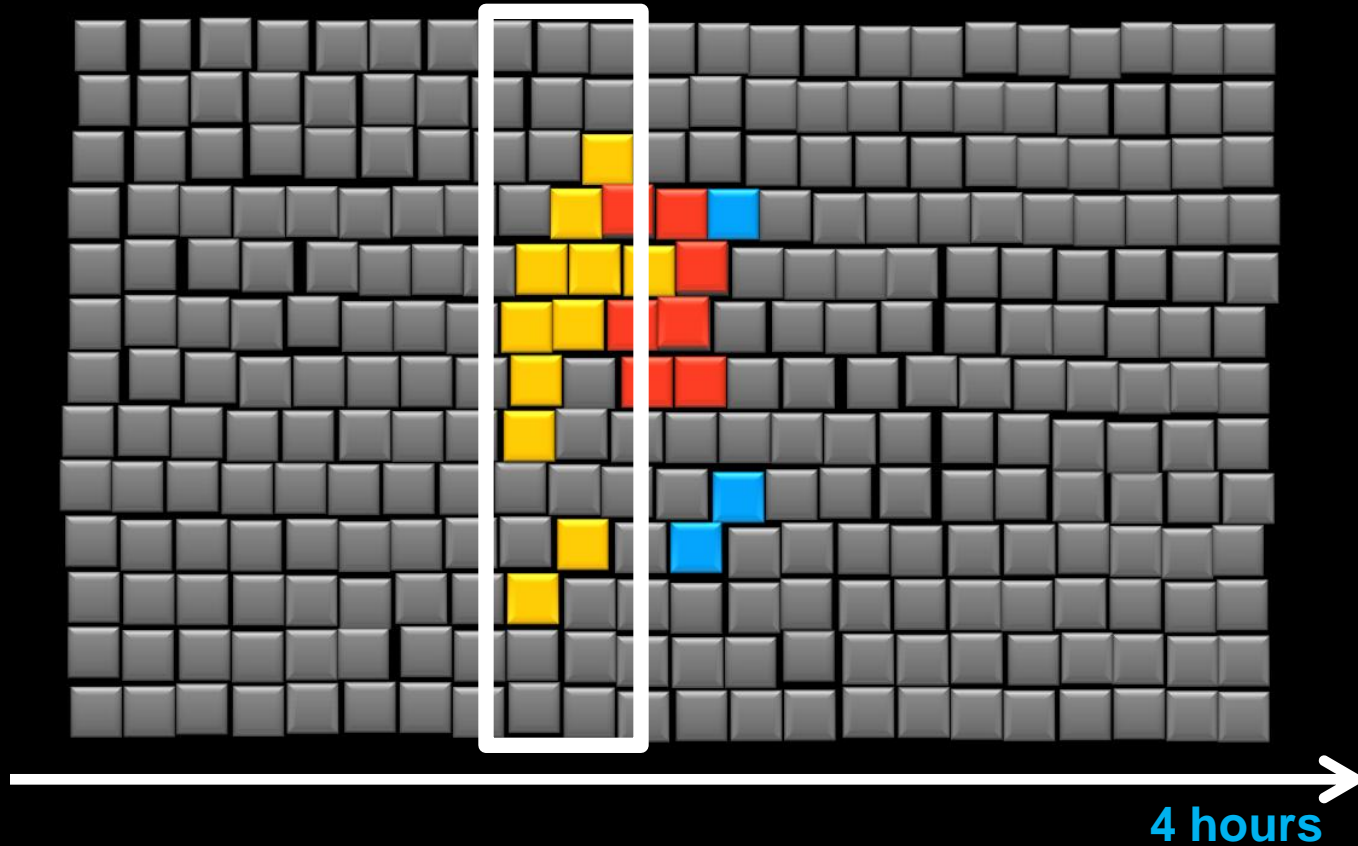


Persistent attacker

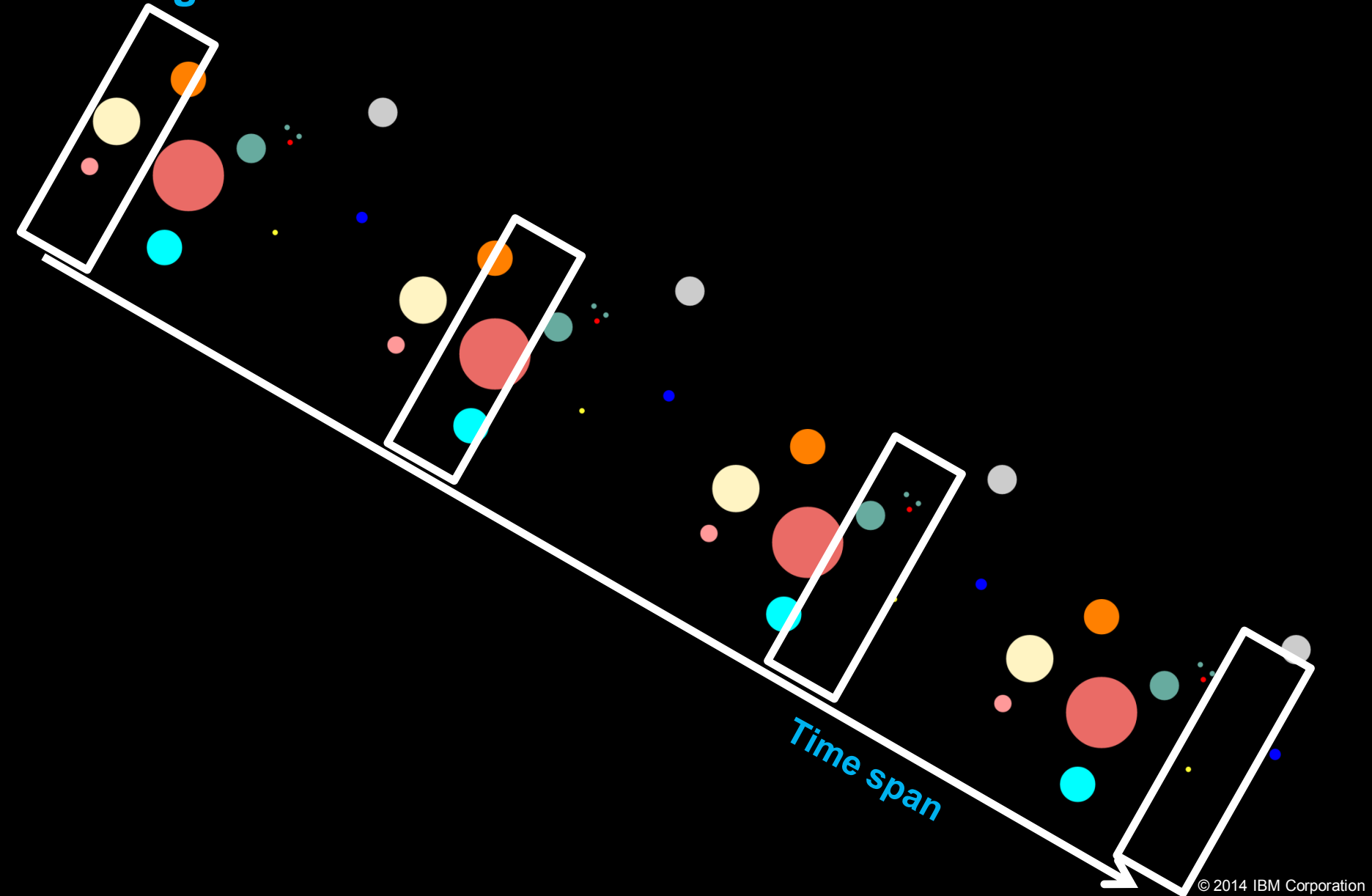


-  irrelevant events
-  detected activity
-  unseen actions

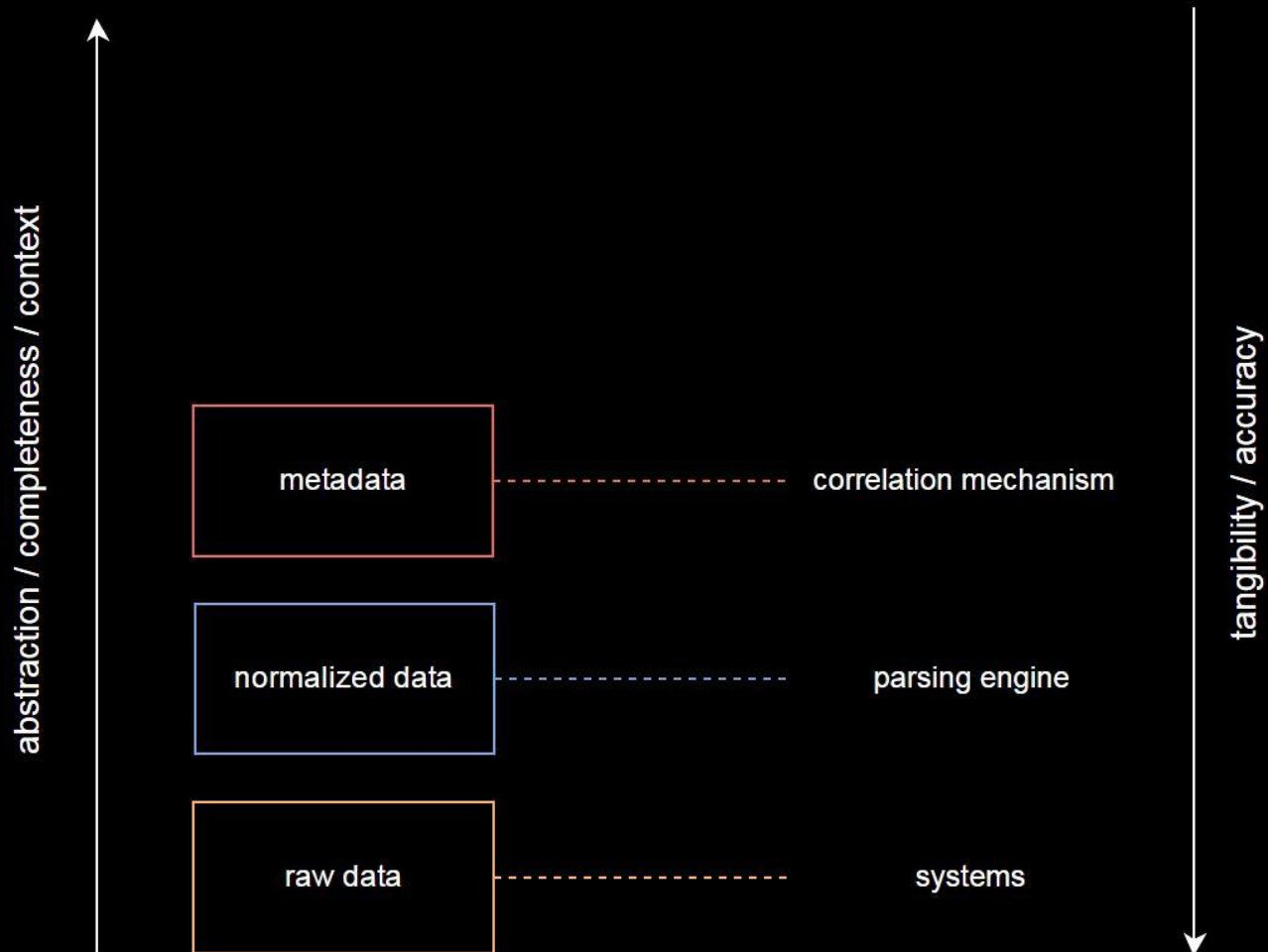
Smash-and-Grab



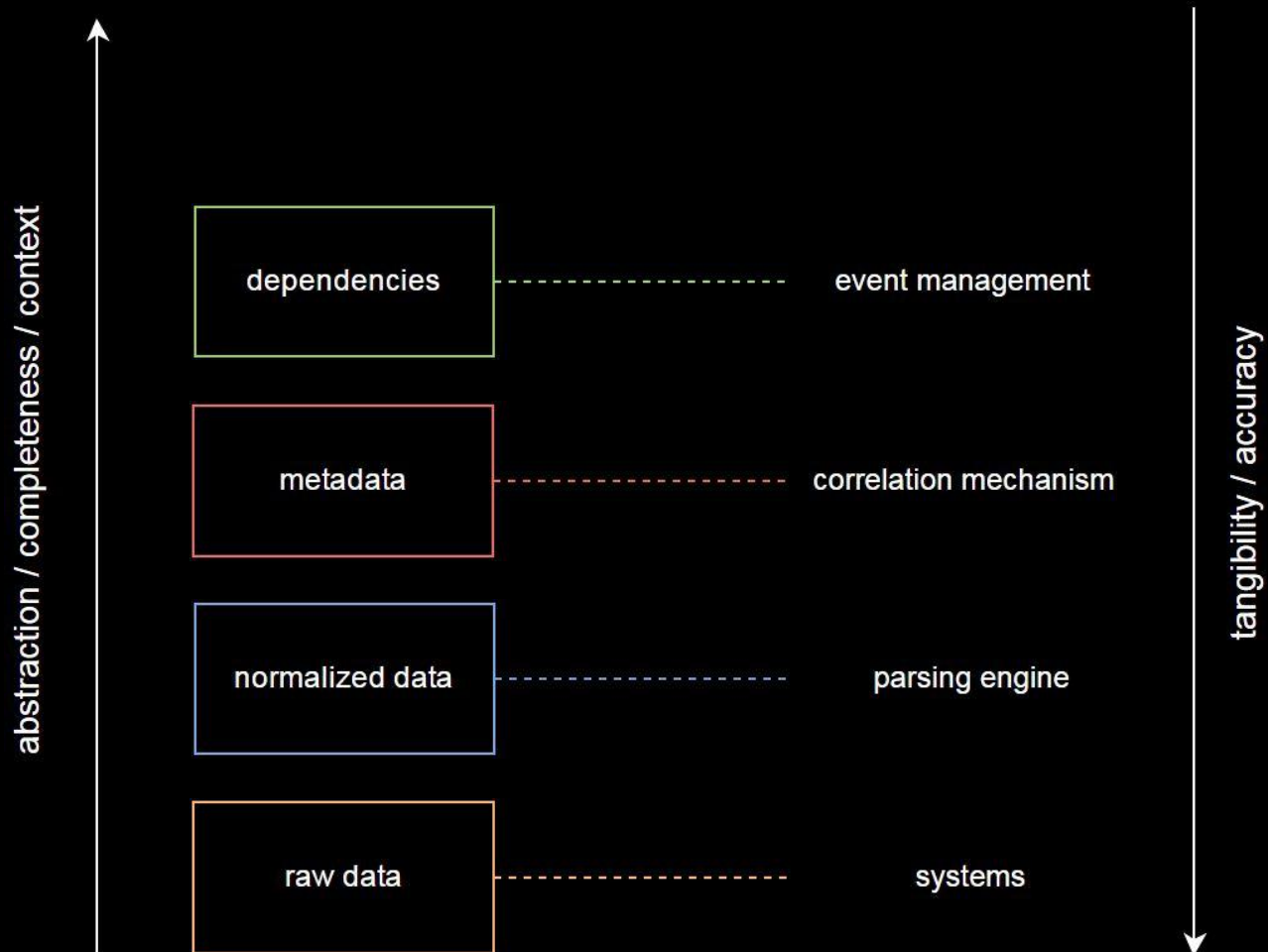
Findings and discussion #2



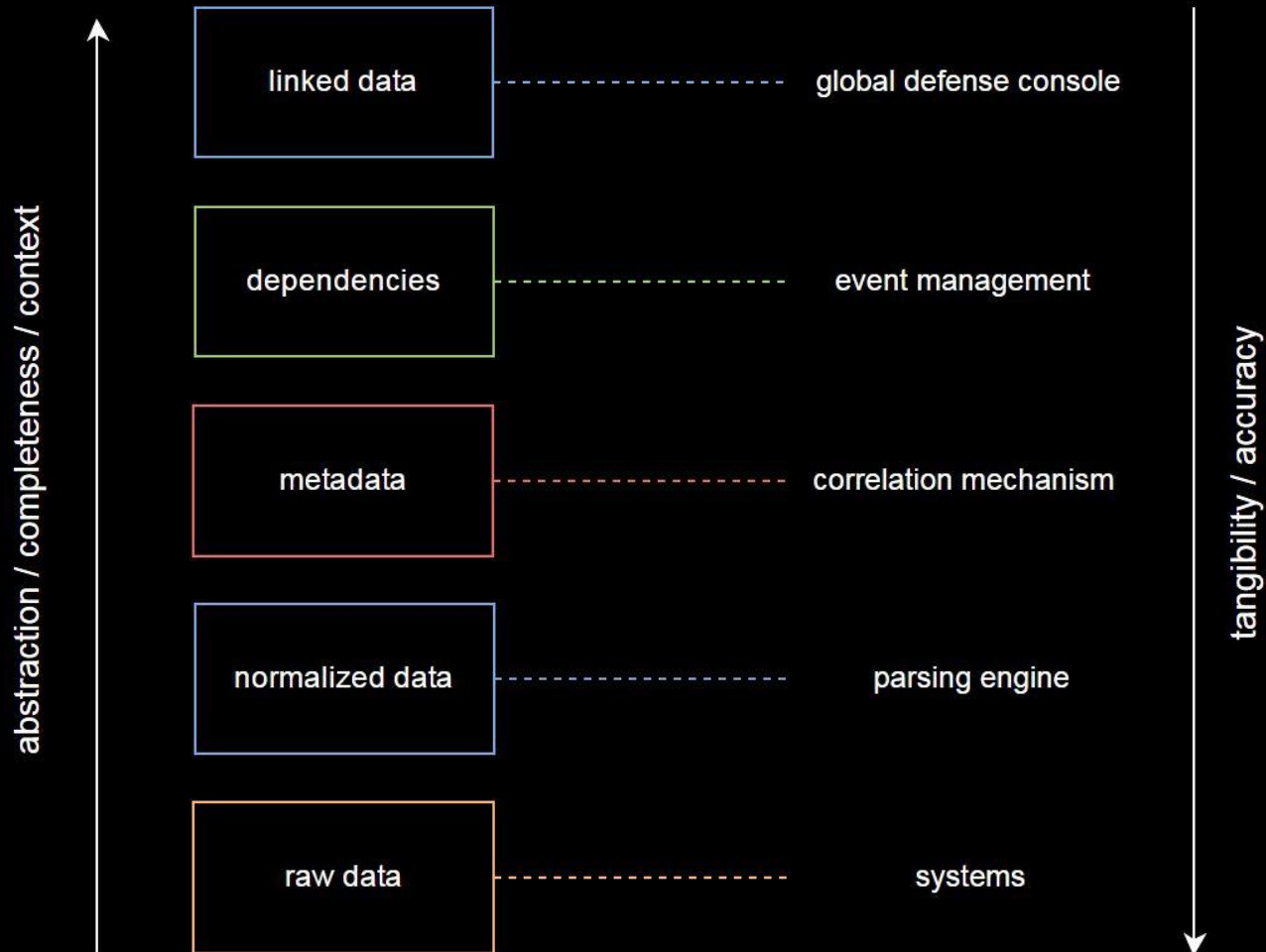
The Correlation Chain



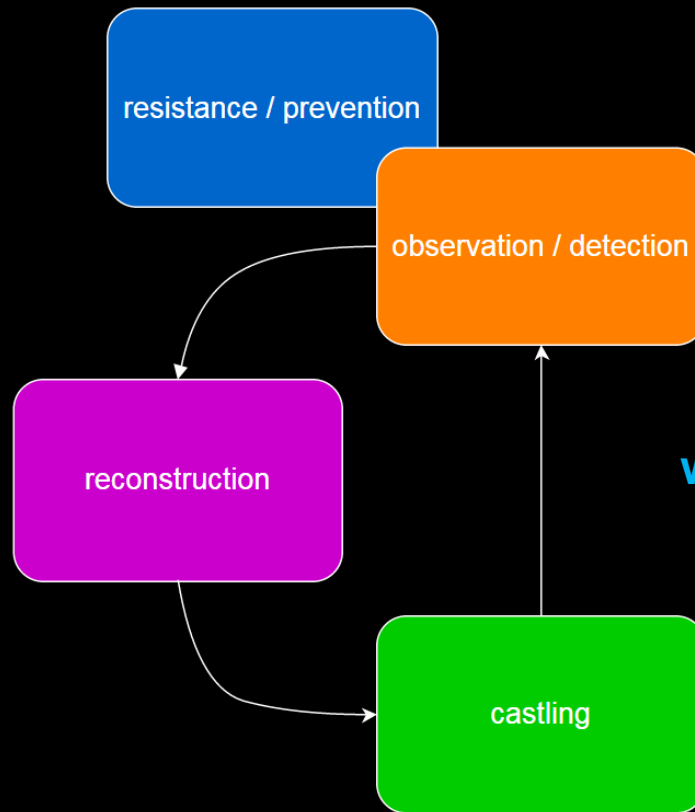
The Correlation Chain



The Correlation Chain



Summary



where is the **Master Record**?

Recommendations

protect the future

1. Map each data type with category tag.
2. Focus on documentation management.
3. Organize your operations before tactical maneuvers.
4. Establish connectivity between detection system and the IR tracking system.
5. Use the reconstruction-observation phases and develop your system and network on the basis of the discovered or observed IOA.

Filip Nowak – filip.m.nowak@pl.ibm

26-27 November 2014



Security Case Study Conference 2014

Thank You