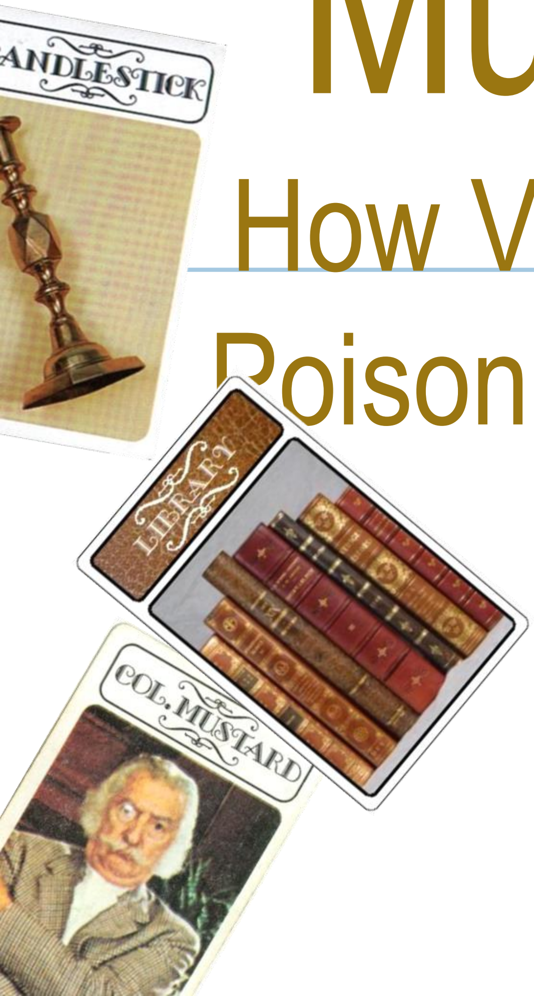
Murder Mystery

How Vulnerability Intelligence is Poisoning Your InfoSec Program

BSides CDMX 2018

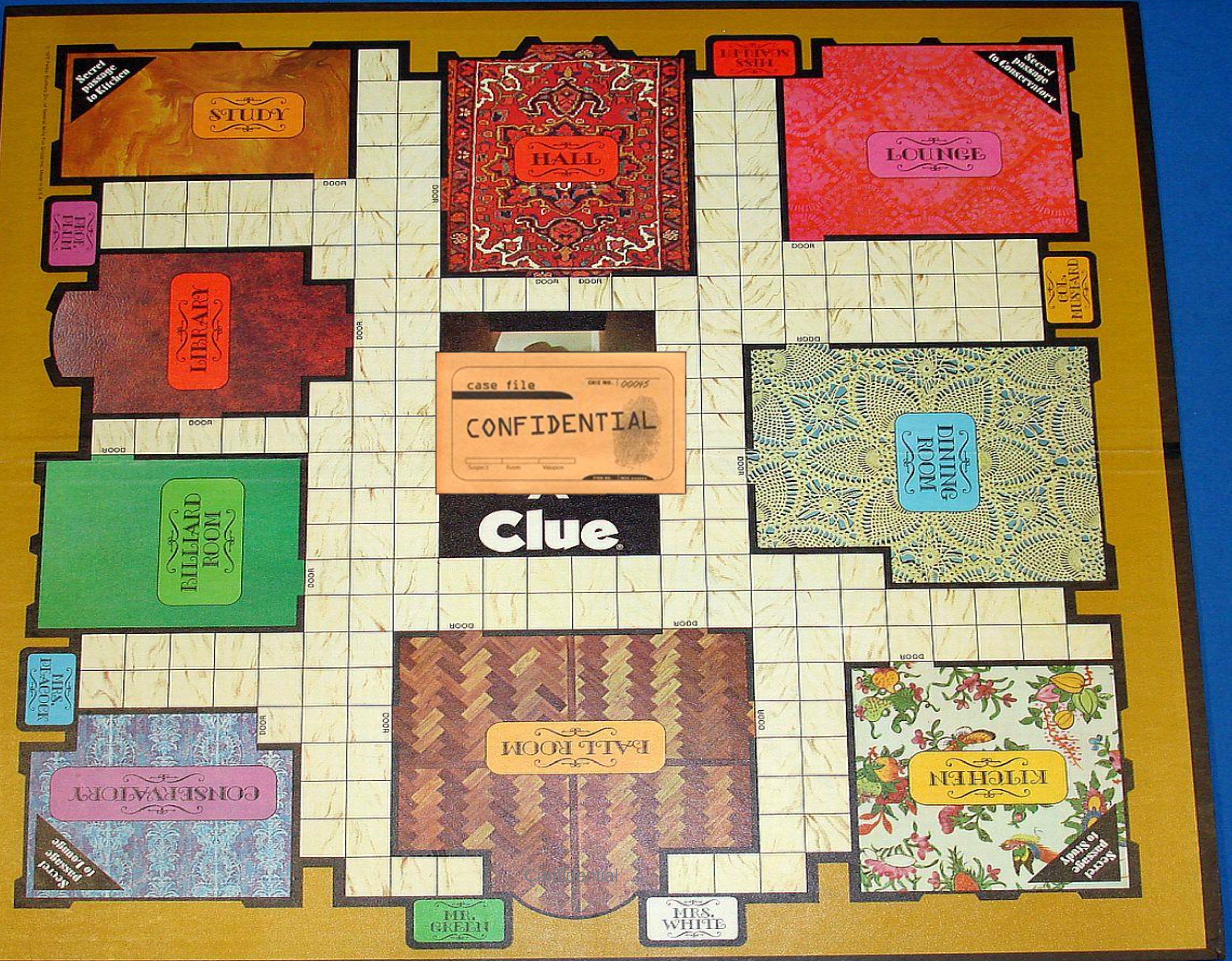
Gordon Mackay - CTO Digital Defense Inc. (DDI)
Twitter: @gord_mackay
Email: gordon.mackay@digitaldefense.com



Overview

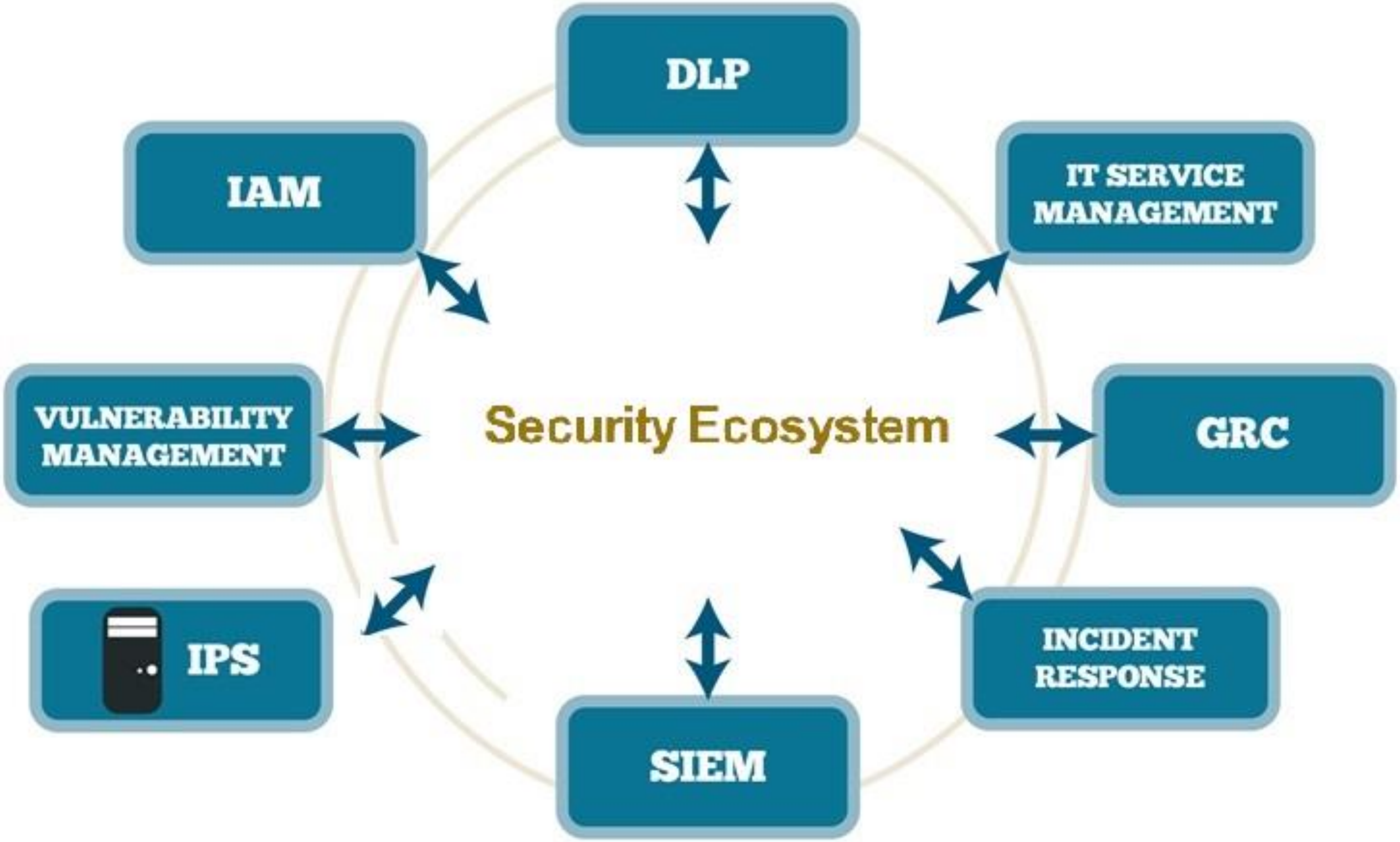
- Murder Mystery - Clue Game Overview
- The Crime Scene - Infosec Risk Use Case
- Detective Tools - VM Technology Background
- Circumstantial Evidence
  - Tracking Endpoints Over Time
  - Ms. Scarlett’s Testimony
  - The Study Room
- Who Dunnit? Root Causes Revealed
- The Victims, The Consequences
- Avoiding Future Crimes

Clue
Parker Brothers Detective Game
STUDY
HALL
LOUNGE
LIBRARY
DINING ROOM
BILLIARD ROOM
BALL ROOM
KITCHEN
CONSERVATORY
Clue
CONFIDENTIAL

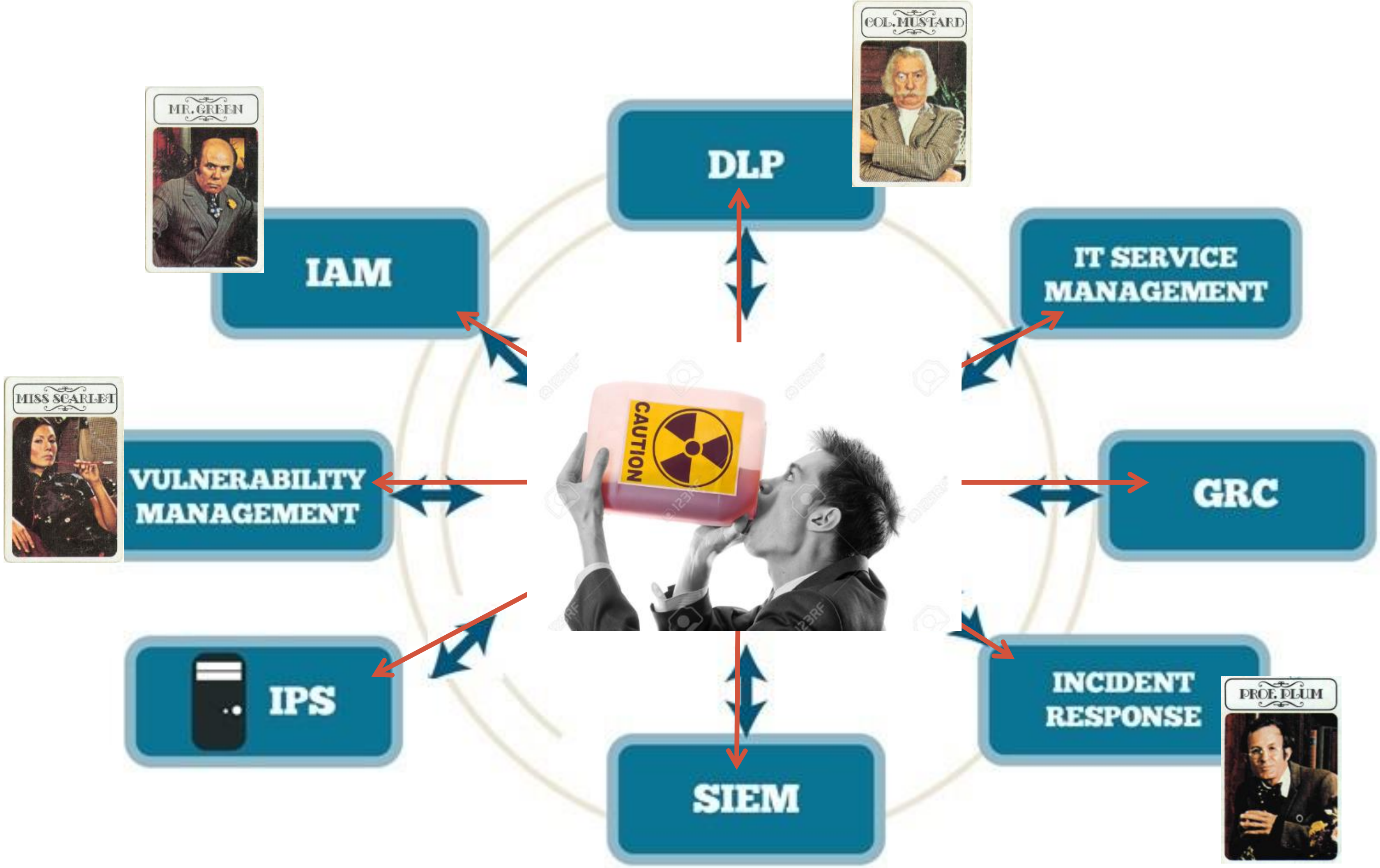

Secret passage to Kitchen
STUDY
HALL
MISS SCARLET
Secret passage to Conservatory
LOUNGE
PROF. PLUM
LIBRARY
COL. MUSTARD
case file
CONFIDENTIAL
DINING ROOM
BILLIARD ROOM
Clue
MRS. PEACOCK
CONSERVATORY
BALL ROOM
KITCHEN
Secret passage to Lounge
Secret passage to Study
MR. GREEN
MRS. WHITE
DOOR

Information Security Risk Use Case

Detective 2.0
Integrated Security Ecosystem

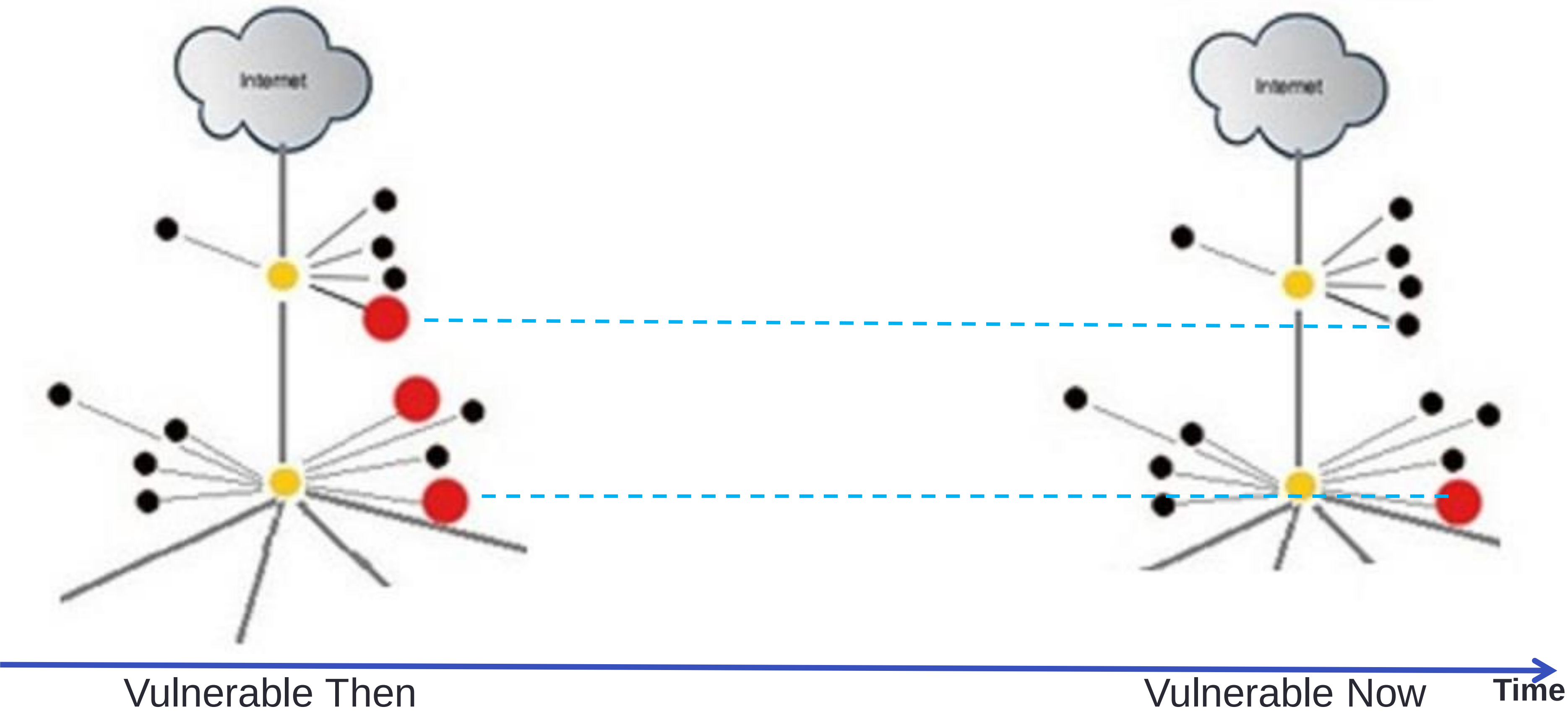


Integrated Security Ecosystem Suspects



Hypothetical Risk Use Case

New Zero Day Impacts Apache version 2.4.0 – 2.4.32 but fixed in 2.4.33



Vulnerable Then

Vulnerable Now

Time

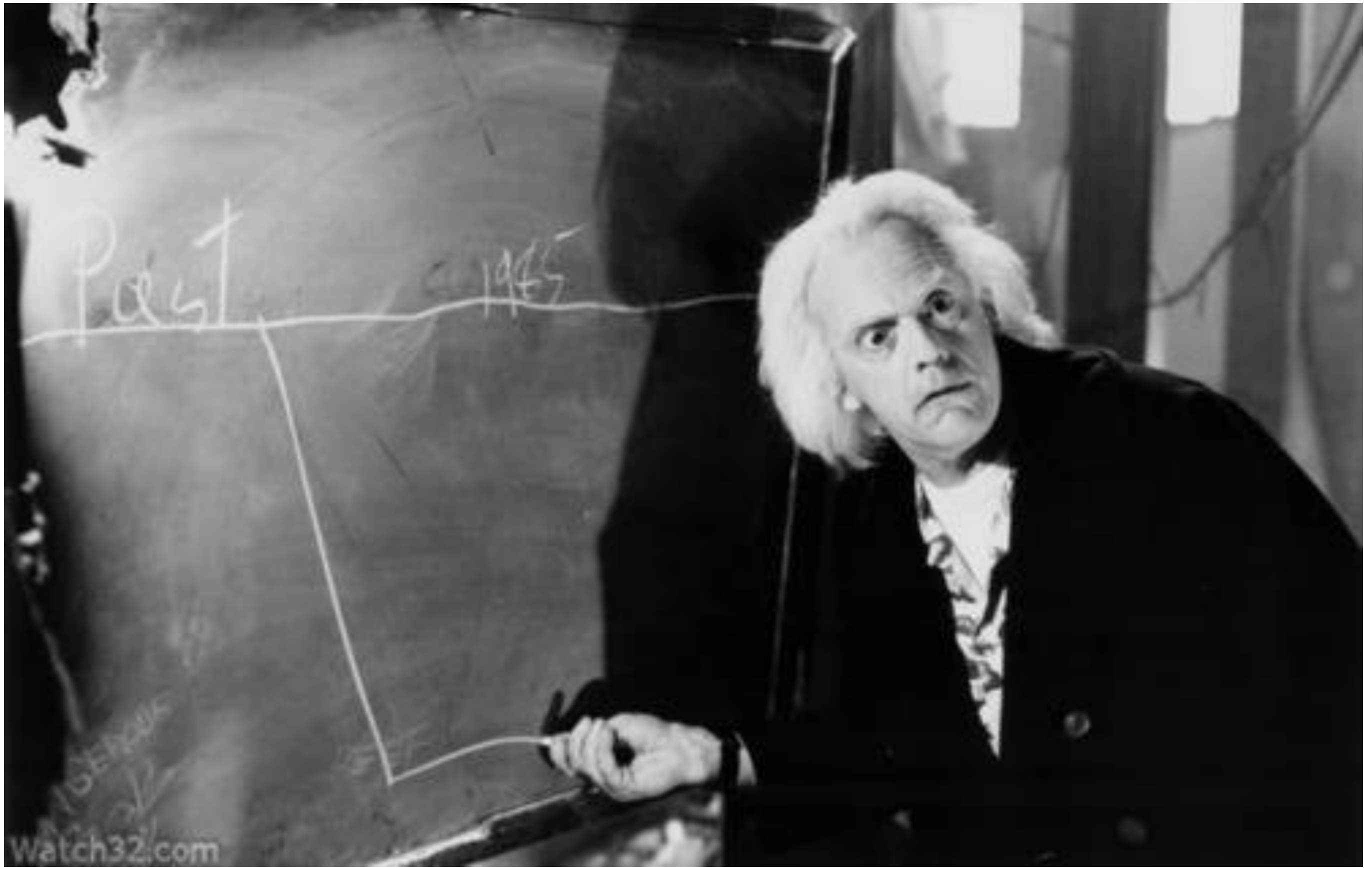
Vulnerability Management Integration with Incident Response

VULNERABILITY MANAGEMENT

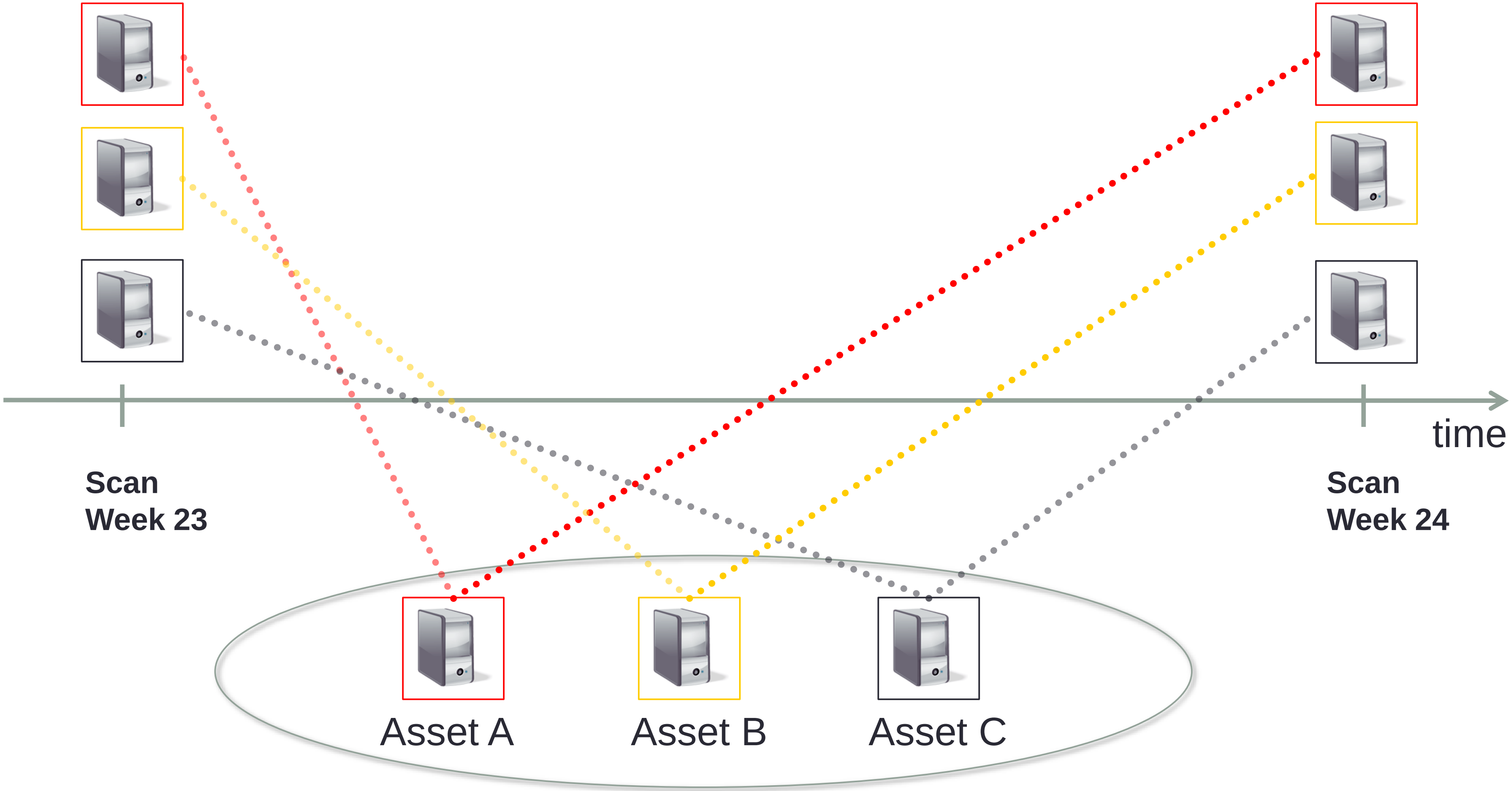
POSSIBLE HOST COMPROMISES

INCIDENT RESPONSE

Let’s Take Step Back (to the Future) And Think About Time

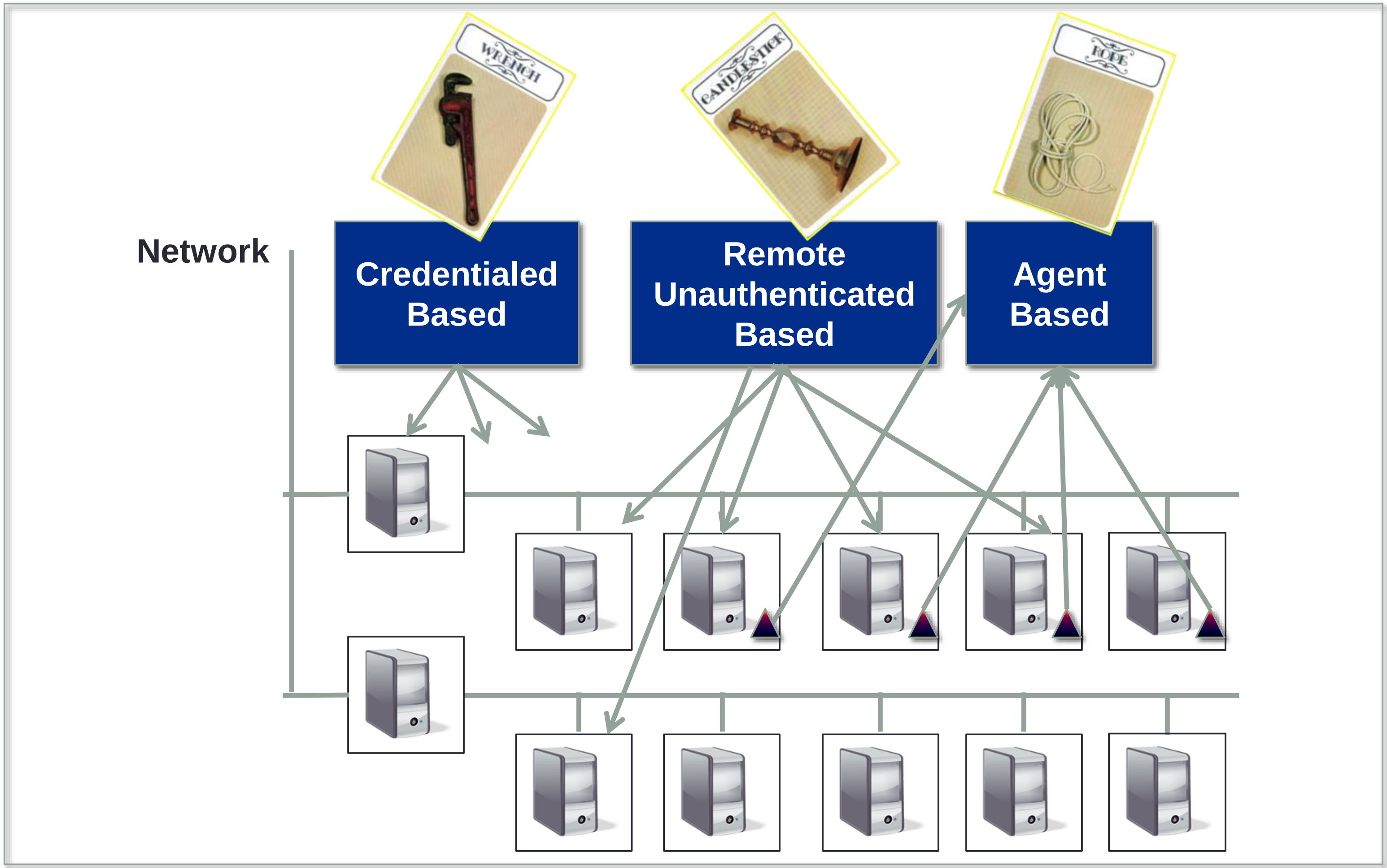


Ms. Scarlett's Weakness
Assessing Hosts Across Time



Real World Network Assets

Vulnerability Scanning Technology



Network

Credentialed Based

Remote Unauthenticated Based

Agent Based

▲ - Local Agents

Circumstantial Evidence

How Vulnerability Management Systems Track Endpoints Across Time

(For Remote Authenticated Scanning)

- Use one or more Network Detectable Characteristic as Match Key:
  - IP Address
  - Various Hostnames (DNS, NETBIOS)
  - MAC Address
  - Host Type
  - Others

Ms. Scarlett's Testimony

Vendor Host Tracking Algorithm Example

- Single Host Tracking Key, Admin User specifies one of:

  1- IP Address (default), or

  2- DNS Hostname, or

  3- NETBIOS Hostname.

Prevalence of Network Churn

DDI Study

- Internal Assessments

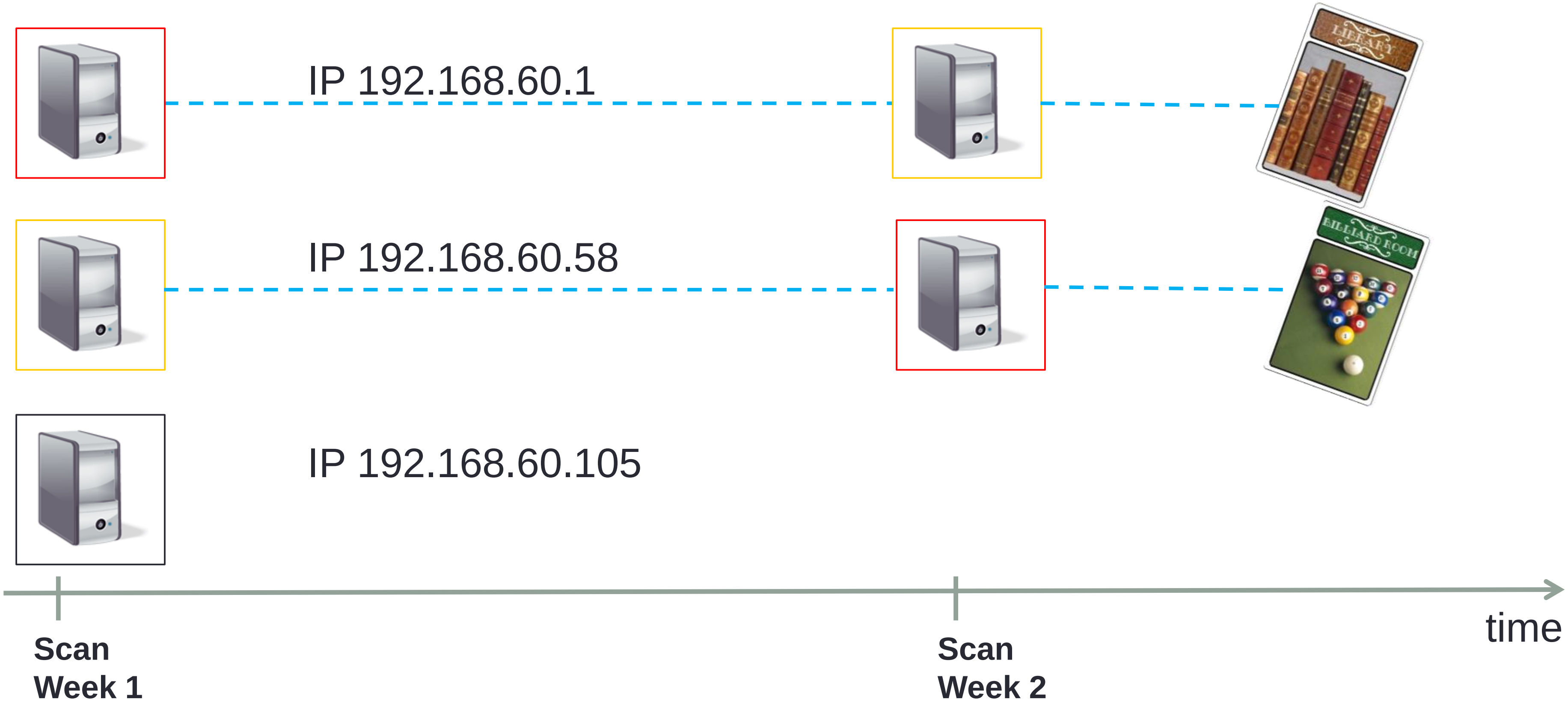
- Across 3 Month Time Period

- **Server Host Characteristic Changes**
  - IP Address Change – 4%
  - DNS Hostname Change – 46%
  - NETBIOS Change – 34%

- **Client Host Characteristic Changes**
  - IP Address Change – 36%
  - DNS Hostname Change – 42%
  - NETBIOS Change – 20%

Study Located Here: https://www.digitaldefense.com/white-papers/doing-the-math-white-paper/

Takeaway
- Endpoints Change Over Time – Significantly!



Who Dunnit Revealed

- Most widely used scanning technology is Remote Unauthenticated Scanning.

- Most VM vendors track point-in time scanned endpoints using limited set of Remotely discovered endpoint characteristics – Ms. Scarlett

- All Remotely Discoverable Characteristics are Subject to Change over time - and Study Finds Change Significant!

- **Real Crime: VM Systems Lack Sufficient Scan-to-Scan Endpoint Correlation Technology**

Result – Often Mistakenly Correlate Endpoints to incorrect Assets over Time.

STUDY
Secret passage to Kitchen
HALL
MISS SCARLET
LOUNGE
Secret passage to Conservatory
PROF. PLUM
LIBRARY
COL. MUSTARD
DINING ROOM
BILLIARD ROOM
MRS. PEACOCK
CONSERVATORY
Secret passage to Lounge
BALL ROOM
KITCHEN
Secret passage to Study
MR.
MRS.
DOOR
MISS SCARLET
CANDLESTICK
LIBRARY
BILLIARD ROOM
BALLROOM
case file
CONFIDENTIAL
00045
Suspect
Room
Weapon

Consequences

2 types

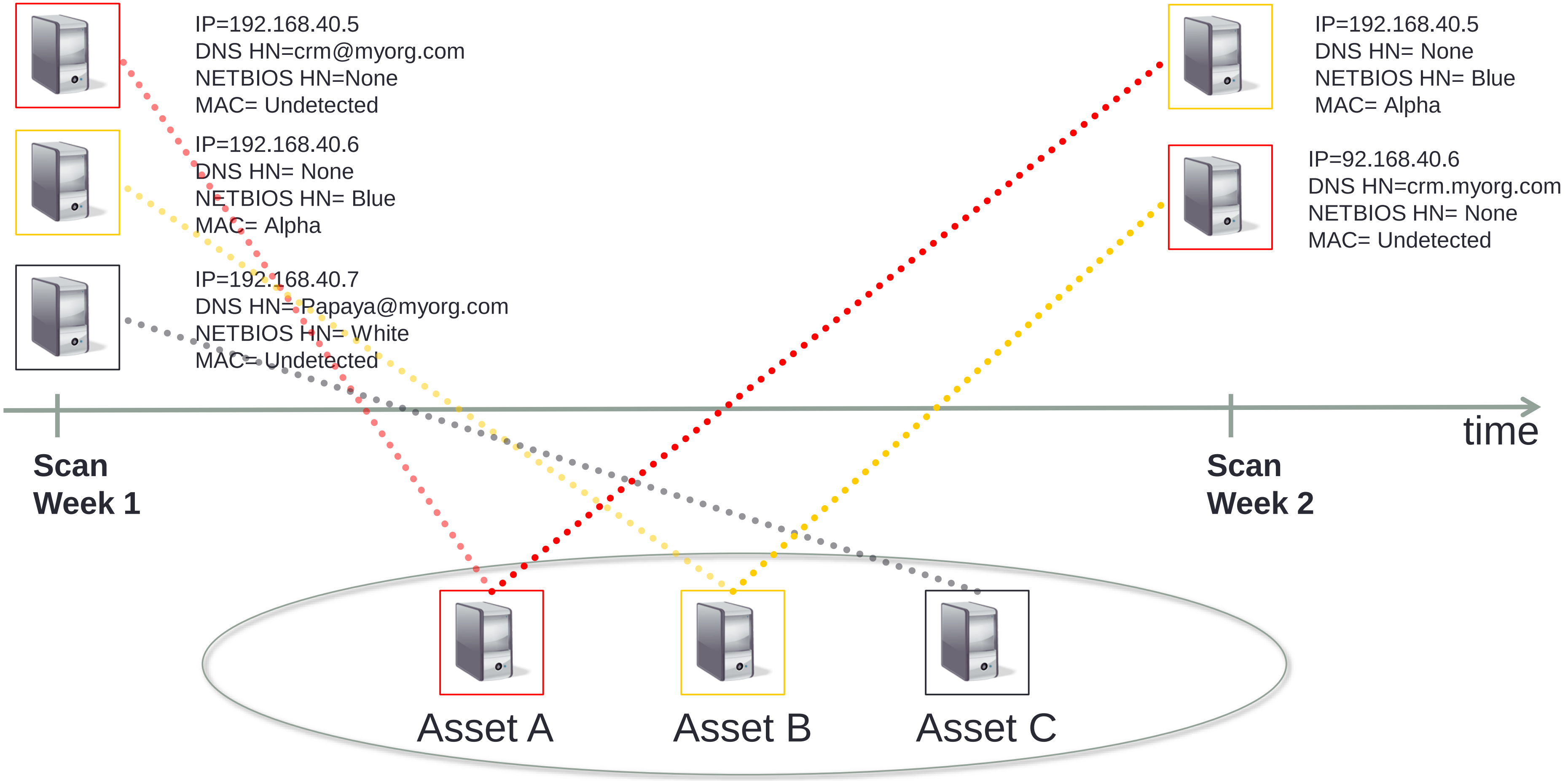
1- Asset Duplication

2- Asset Mismatch

Let’s Examine These…

Consequence of Flaw

Configurable Single Tracking Key – Asset Mismatch



IP=192.168.40.5
DNS HN=crm@myorg.com
NETBIOS HN=None
MAC= Undetected

IP=192.168.40.6
DNS HN= None
NETBIOS HN= Blue
MAC= Alpha

IP=192.168.40.7
DNS HN= Papaya@myorg.com
NETBIOS HN= White
MAC= Undetected

IP=192.168.40.5
DNS HN= None
NETBIOS HN= Blue
MAC= Alpha

IP=92.168.40.6
DNS HN=crm.myorg.com
NETBIOS HN= None
MAC= Undetected

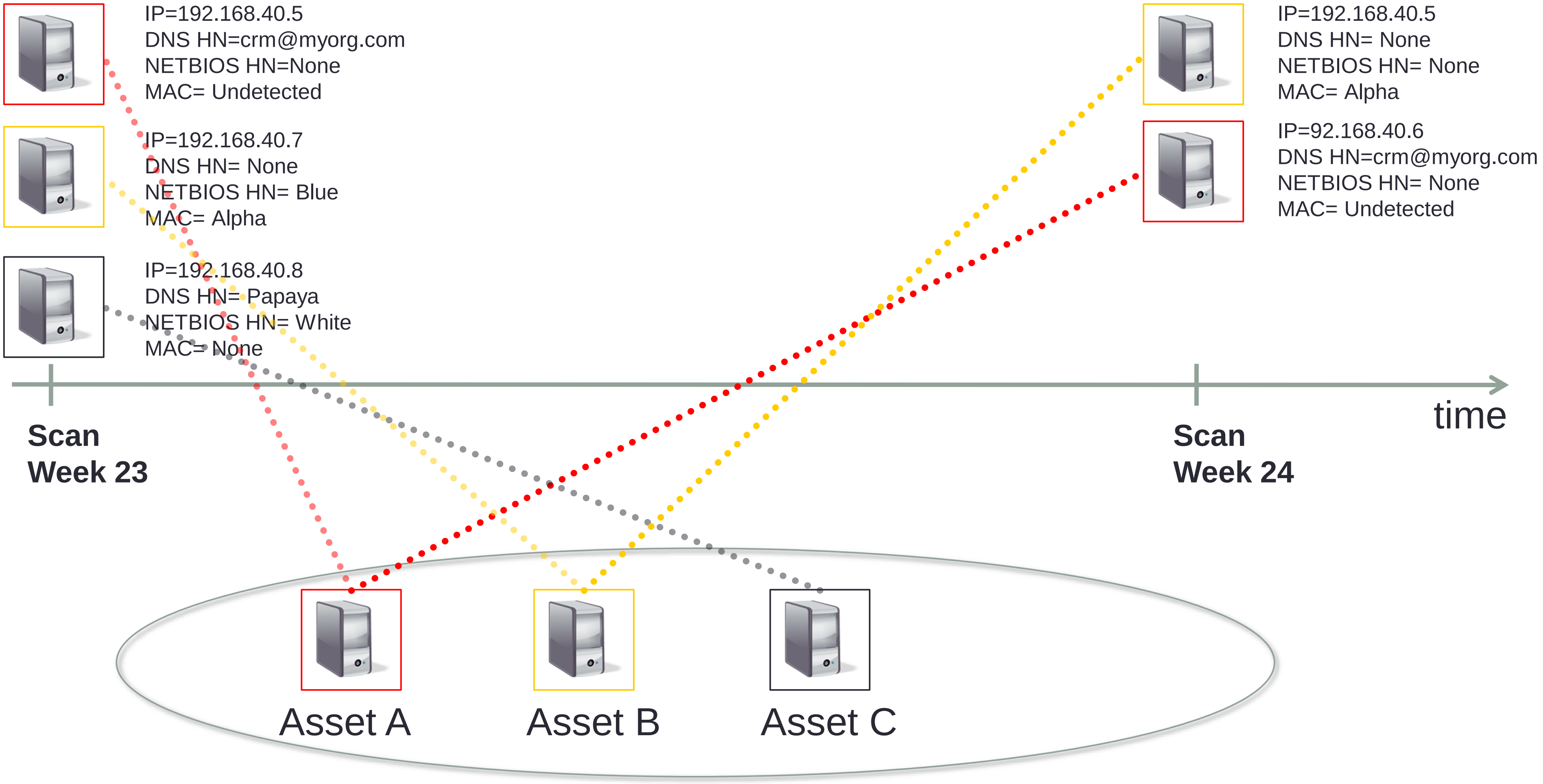
Real World Network Assets

Victims & Impacts

- Endpoint and Vulnerability Information Inaccurate over time - resulting in “chasing ghosts.”
- Mismatched scanned endpoints to assets result in
  - Vulnerabilities Declared Fixed when Still Present
  - Vulnerabilities Declared New when Already Present
- Integrated Security Tools Relying on Faulty Data – Numerous Security Use Cases Negatively Impacted.
- Information Security Generals taking decisions based on miscalibrated Security Risk Gauge.

Don’t Rely on Circumstantial Evidence Correlate on All Findings Like Fingerprints

Ideal Scan-to-Scan Host Correlation



IP=192.168.40.5
DNS HN=crm@myorg.com
NETBIOS HN=None
MAC= Undetected

IP=192.168.40.7
DNS HN= None
NETBIOS HN= Blue
MAC= Alpha

IP=192.168.40.8
DNS HN= Papaya
NETBIOS HN= White
MAC= None

IP=192.168.40.5
DNS HN= None
NETBIOS HN= None
MAC= Alpha

IP=92.168.40.6
DNS HN=crm@myorg.com
NETBIOS HN= None
MAC= Undetected

Real World Network Assets

Murder Mystery: Solved

- Security Ecosystem Use Cases often Rely on Historical security information.

- Network endpoints change characteristics due to normal IT administration, but they are still the same endpoints.

- Most VM solutions good with 1 point in time assessment, weak with correlating different point in time assessments

- Use your own Endpoint Correlation Technology or select a vulnerability management solution with advanced scan to scan correlation capabilities.

QUESTIONS?

Gordon MacKay

Email: gordon.mackay@digitaldefense.com

Twitter: @gord_mackay

DIGITAL DEFENSE® INCORPORATED