IBM i2 Solutions

Turning Big Data into Actionable Intelligence

Cyber Intelligence and Security Solutions

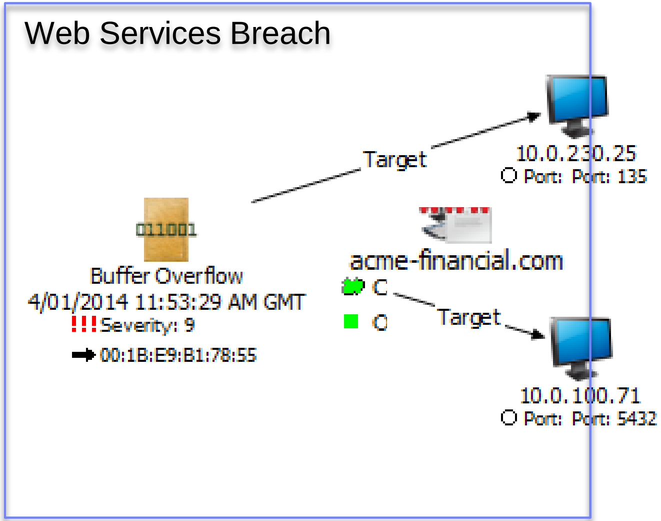
Angus Stewart, IBM

Chris Hawkes, Claviger

i2 and Cyber…

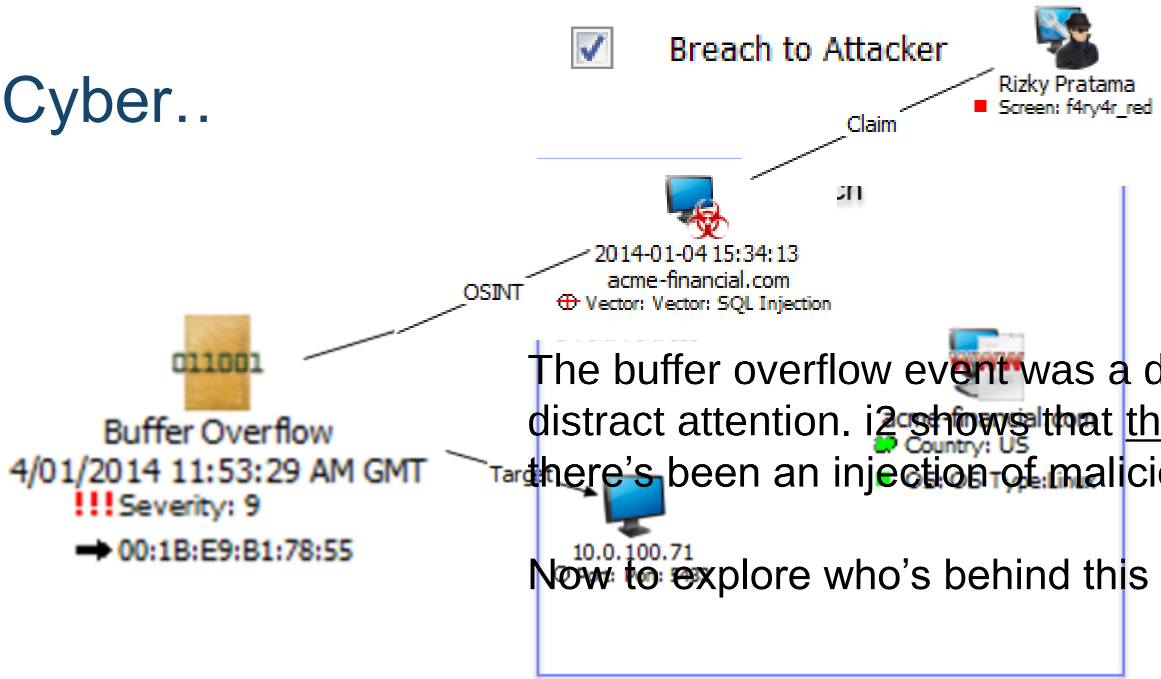
An event signals that an attempt appears to have been made to exploit the IT system.

We need to investigate…



i2 highlights that two servers related to ACME Financial’s website are connected to this potentially malicious event…

i2 and Cyber..



The buffer overflow event was a diversion meant to distract attention. i2 shows that <u>the real story</u> is that there’s been an injection of malicious code.

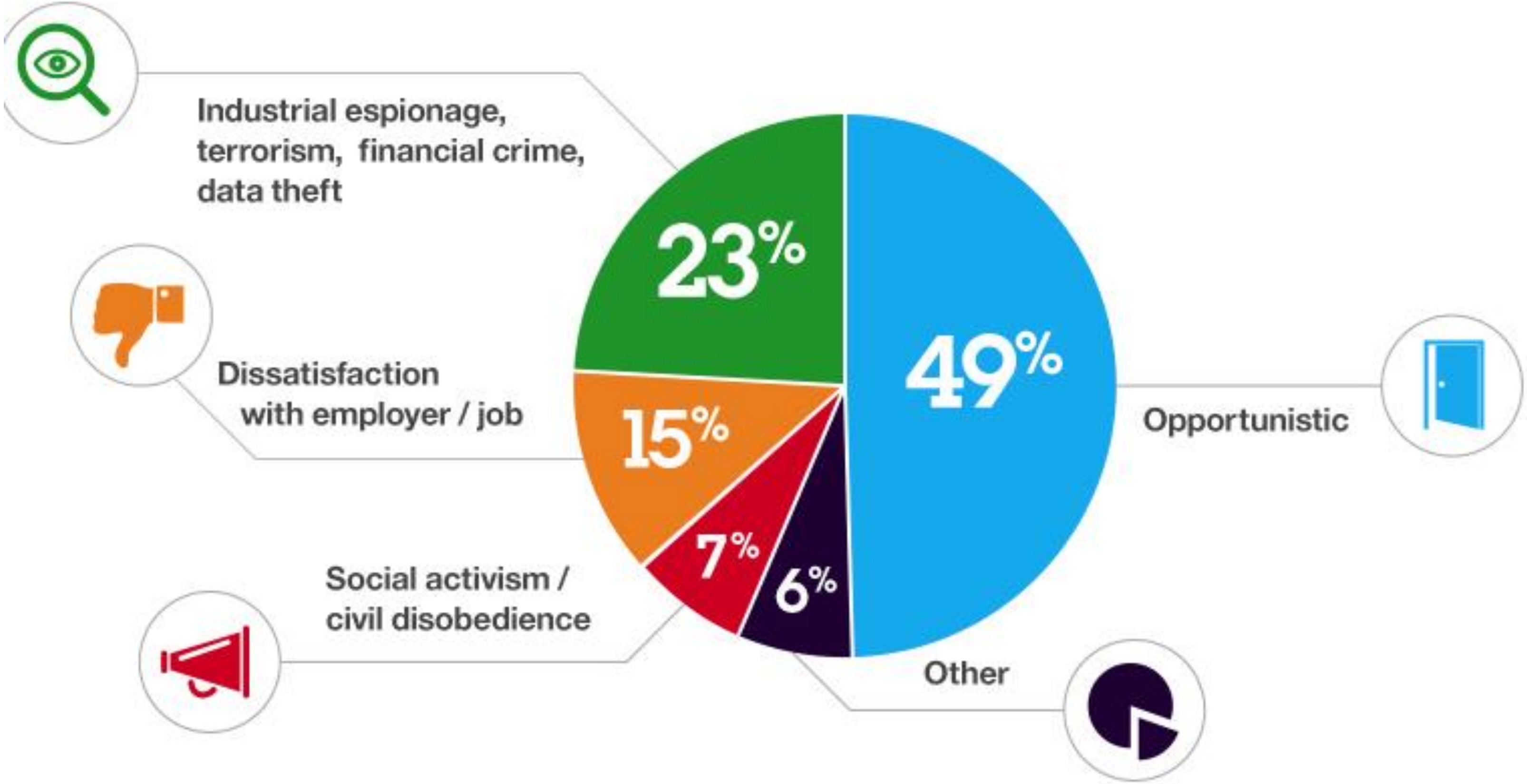
Now to explore who’s behind this attack…

i2 for Cyber…

✓Investigate system vulnerabilities and identify remediation options

✓Combine internal data with external open source intelligence

✓Understand the attacks and the attackers to prevent future attacks, mitigate potential damage and risk…



Source: *IBM Security Services 2013 Cyber Security Intelligence Index*

We are in an era of continuous breaches

Attackers are relentless, victims are targeted, and the damage toll is rising

2011

Operational Sophistication

IBM X-Force® declared

Year of the Security Breach

2012

Near Daily Leaks of Sensitive Data

40% increase

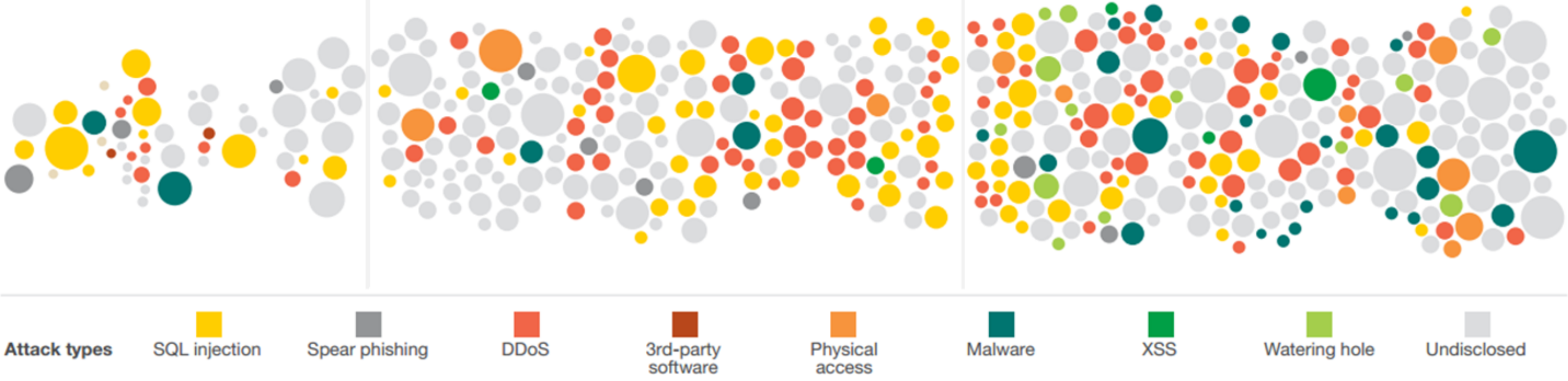
in reported data breaches and incidents

2013

Relentless Use of Multiple Methods

500,000,000+ records

were leaked, while the future shows no sign of change



Source: [IBM X-Force Threat Intelligence Quarterly – 1Q 2014]

Note: Size of circle estimates relative impact of incident in terms of cost to business.

Cost per record* in 2013

IBM

Global average

$145

9%

year-to-year increase

$135

In Australia

Cost per incident* in 2013

Global average

$3.5M

15%

year-to-year increase

$2.6M

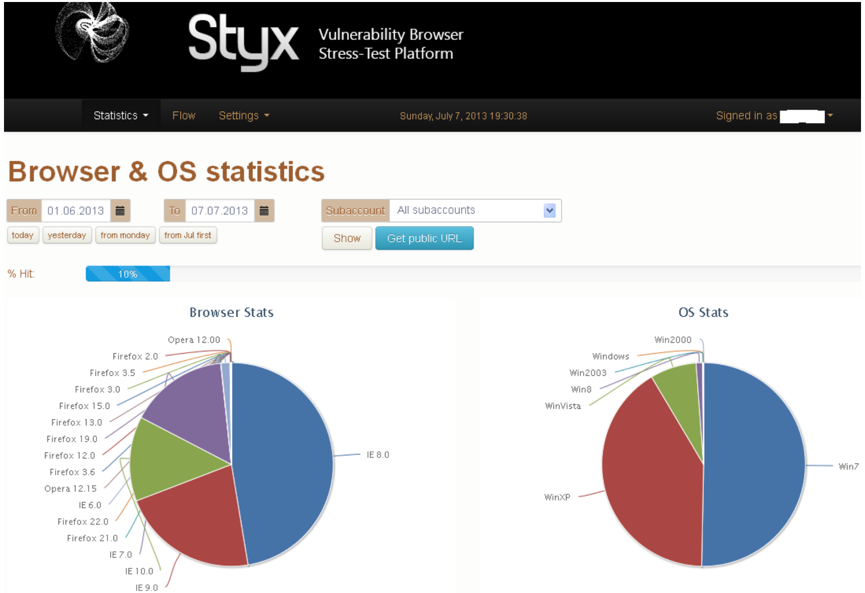
In Australia

*Currencies converted to US dollars

Attackers use exploit kits to deliver payloads

Blackhole Exploit Kit

- Most popular in 2013
- Creator arrested in October



Sunday, July 7, 2013 19:30:38

Signed in as [redacted]

Browser & OS statistics

From 01.06.2013

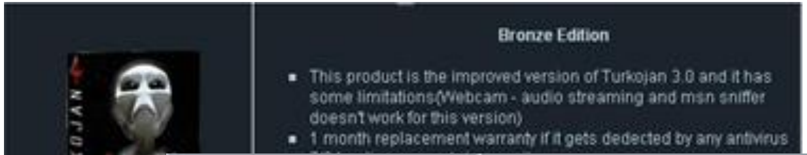
To 07.07.2013

Subaccount: All subaccounts

% Hit: 10%

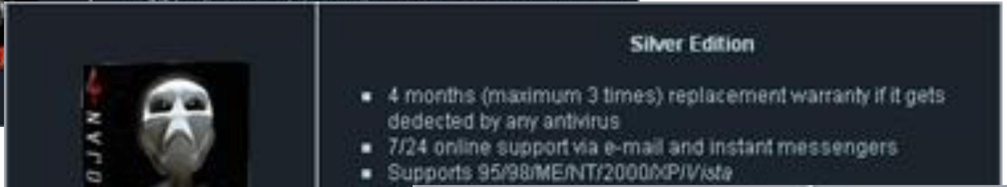
Styx Exploit Kit

- Rising in popularity
- Successful in exploiting IE and Firefox on Windows



Bronze Edition

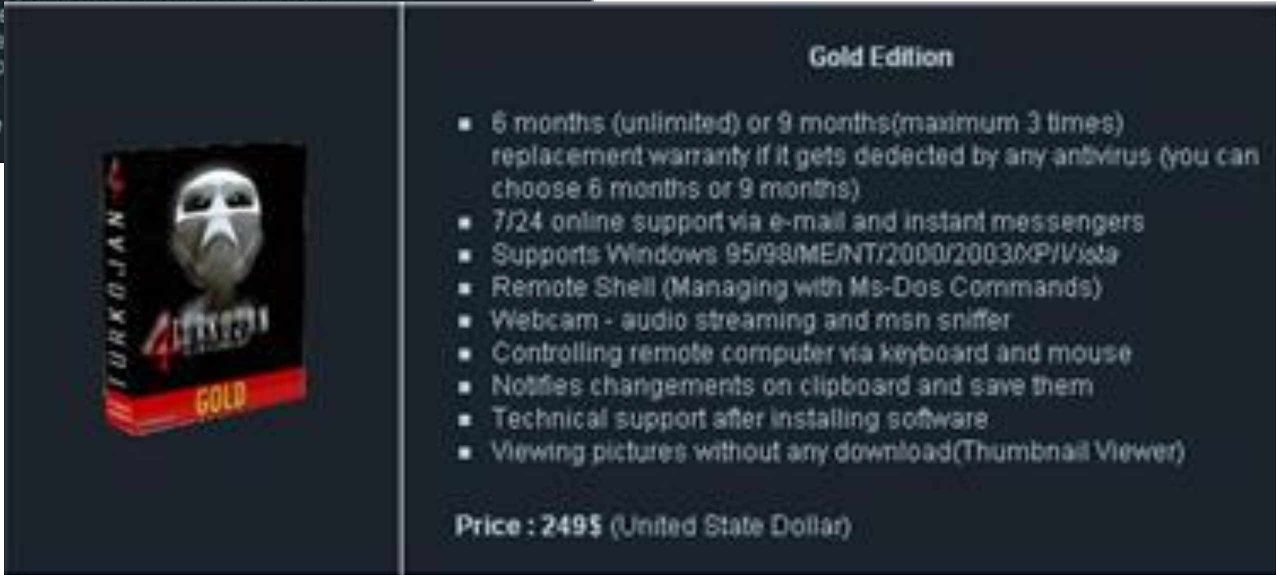
- This product is the improved version of Turkojan 3.0 and it has some limitations(Webcam - audio streaming and msn sniffer doesn't work for this version)
- 1 month replacement warranty if it gets dedected by any antivirus



Silver Edition

- 4 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail and instant messengers
- Supports 95/98/ME/NT/2000/XP/Vista
- We
- Re
- No

Price



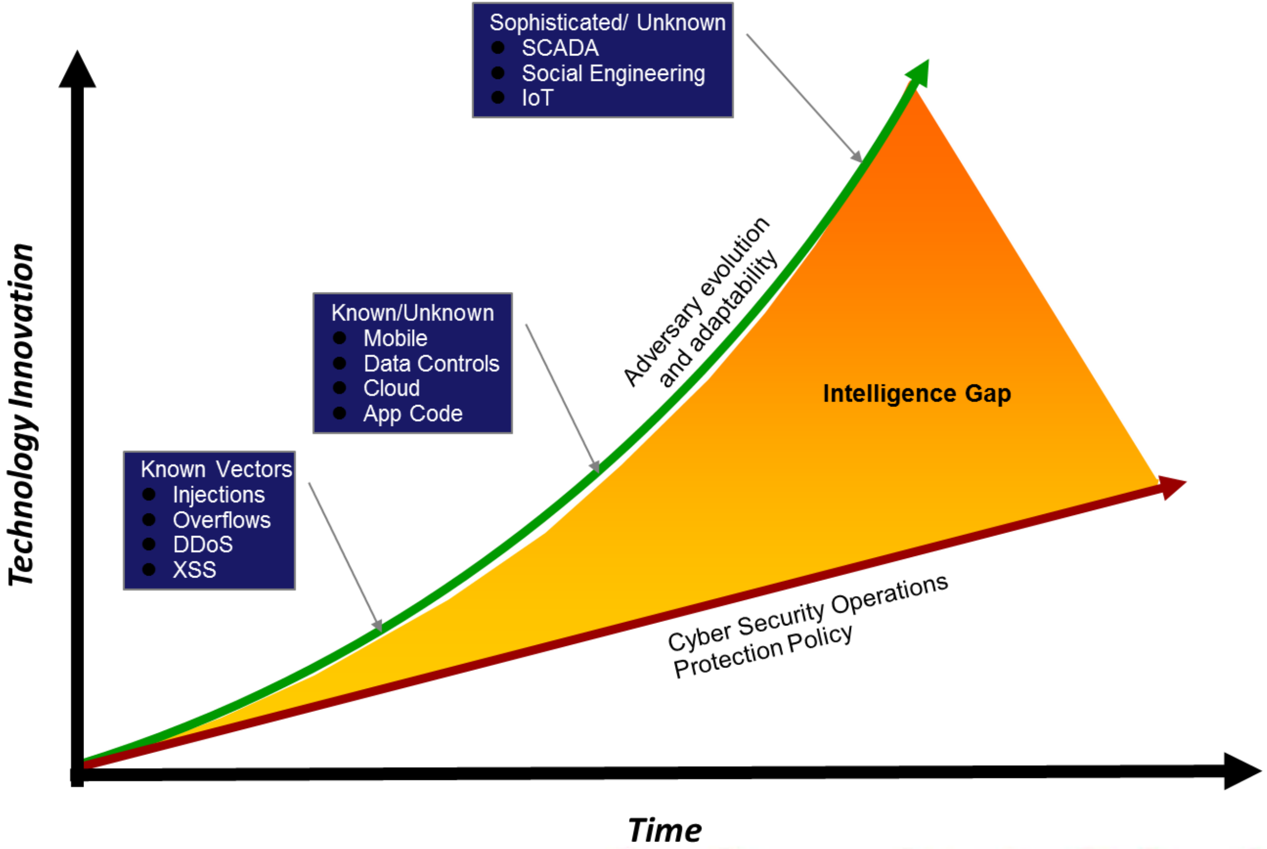
Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers
- Supports Windows 95/98/ME/NT/2000/2003/XP/Vista
- Remote Shell (Managing with Ms-Dos Commands)
- Webcam - audio streaming and msn sniffer
- Controlling remote computer via keyboard and mouse
- Notifies changements on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

Price : 249$ (United State Dollar)

It's just another business model…

The Cyber Intelligence Concept


Technology Innovation
Time
Adversary evolution and adaptability
Intelligence Gap
Cyber Security Operations Protection Policy

Sophisticated/ Unknown

- SCADA
- Social Engineering
- IoT

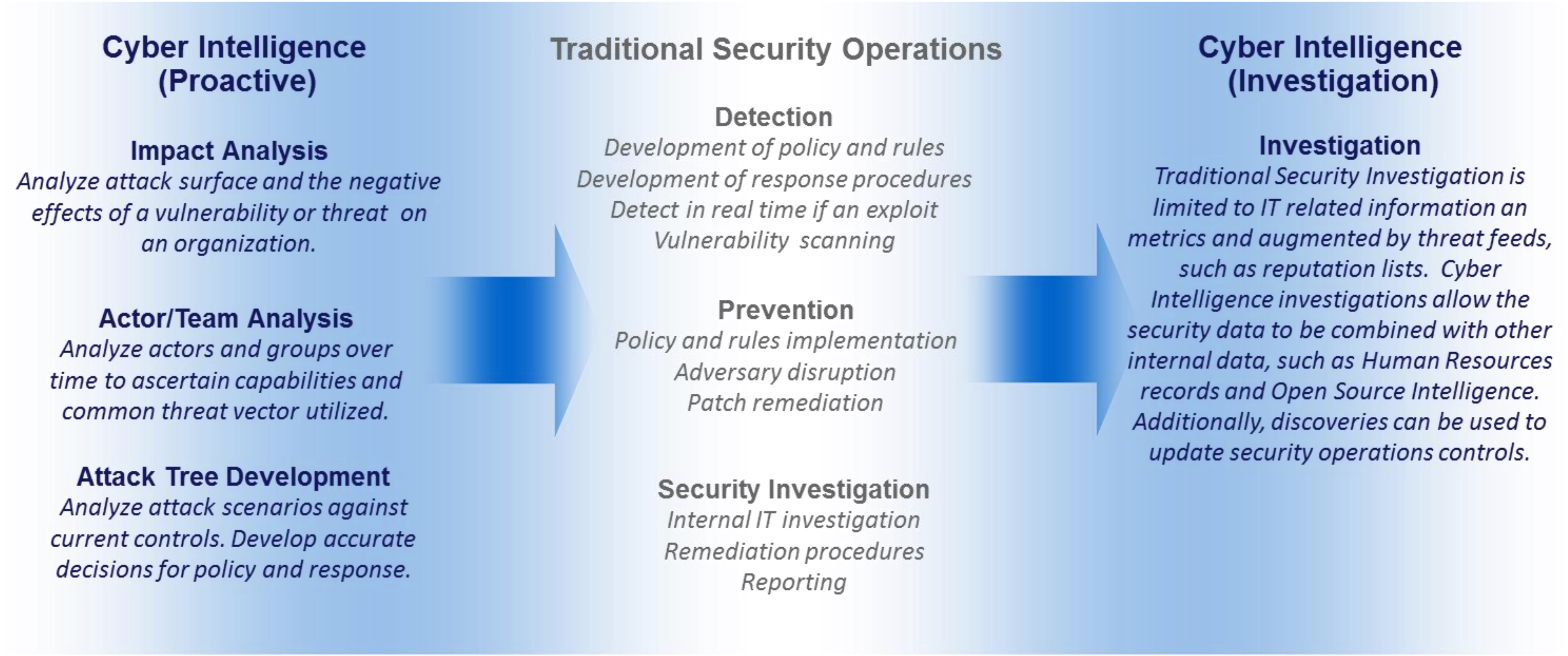
Known/Unknown

- Mobile
- Data Controls
- Cloud
- App Code

Known Vectors

- Injections
- Overflows
- DDoS
- XSS

Proactive Cyber Intelligence



Cyber Intelligence (Proactive)

Impact Analysis

Analyze attack surface and the negative effects of a vulnerability or threat on an organization.

Actor/Team Analysis

Analyze actors and groups over time to ascertain capabilities and common threat vector utilized.

Attack Tree Development

Analyze attack scenarios against current controls. Develop accurate decisions for policy and response.

Traditional Security Operations

Detection

Development of policy and rules
Development of response procedures
Detect in real time if an exploit
Vulnerability scanning

Prevention

Policy and rules implementation
Adversary disruption
Patch remediation

Security Investigation

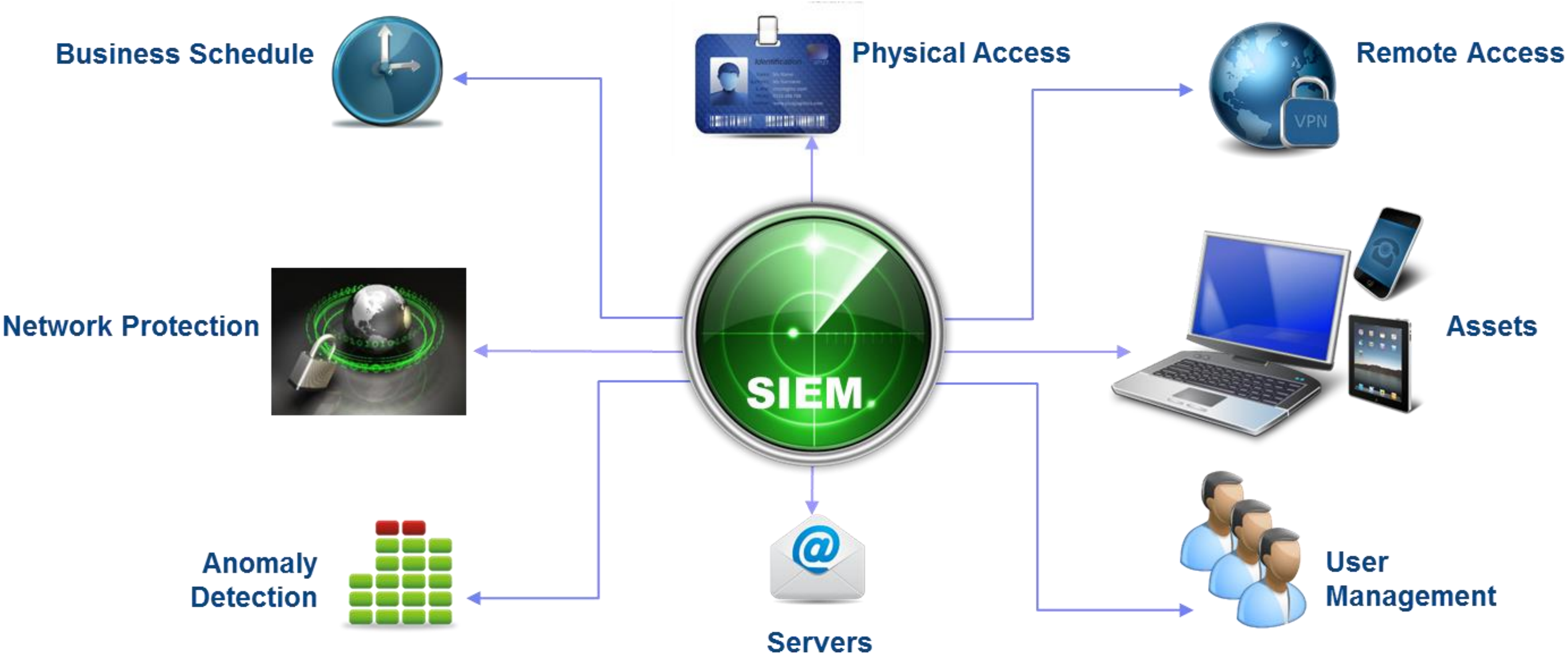
Internal IT investigation
Remediation procedures
Reporting

Cyber Intelligence (Investigation)

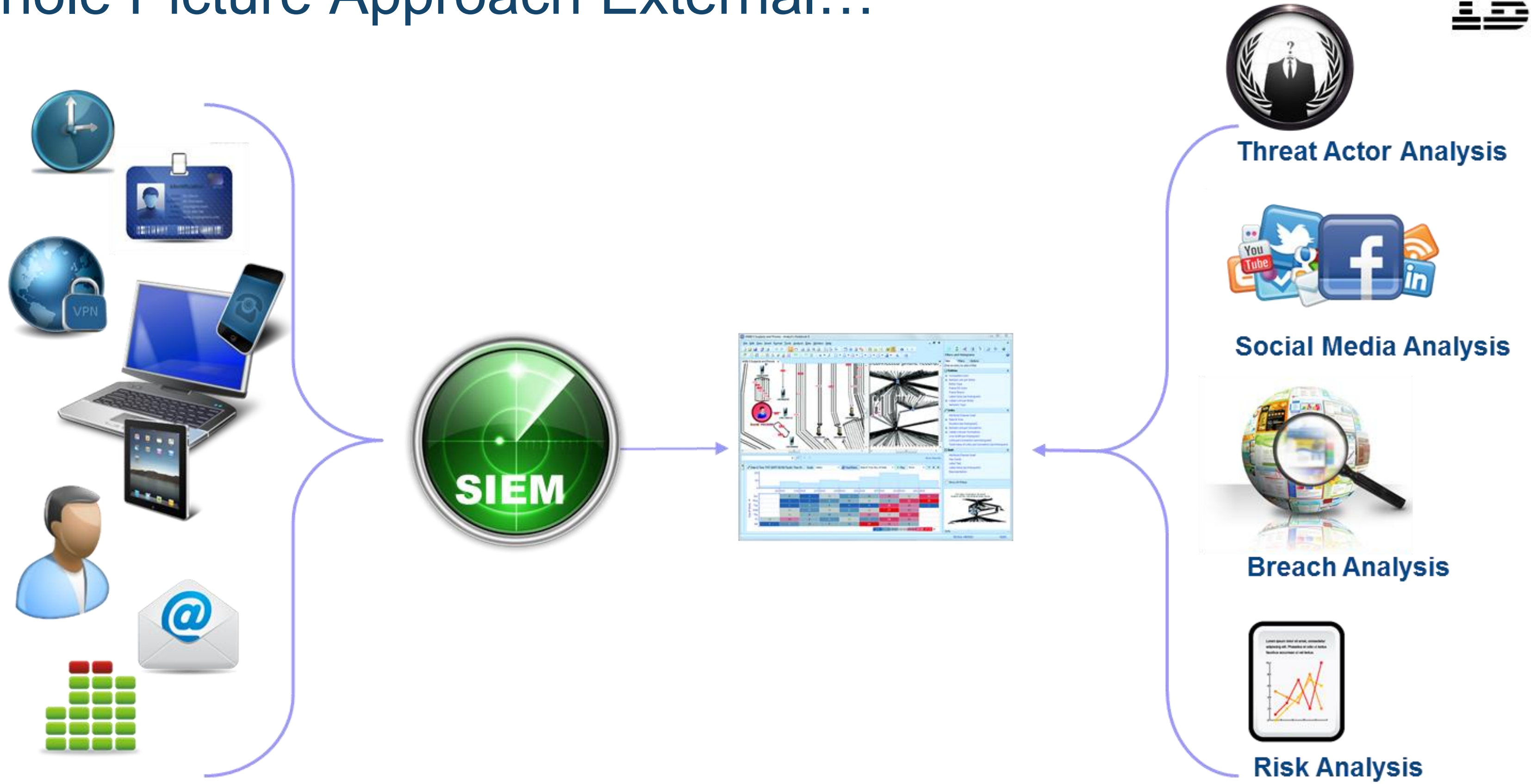
Investigation

Traditional Security Investigation is limited to IT related information an metrics and augmented by threat feeds, such as reputation lists. Cyber Intelligence investigations allow the security data to be combined with other internal data, such as Human Resources records and Open Source Intelligence. Additionally, discoveries can be used to update security operations controls.

Know the Environment. Security layers may already be in place.



Whole Picture Approach External…



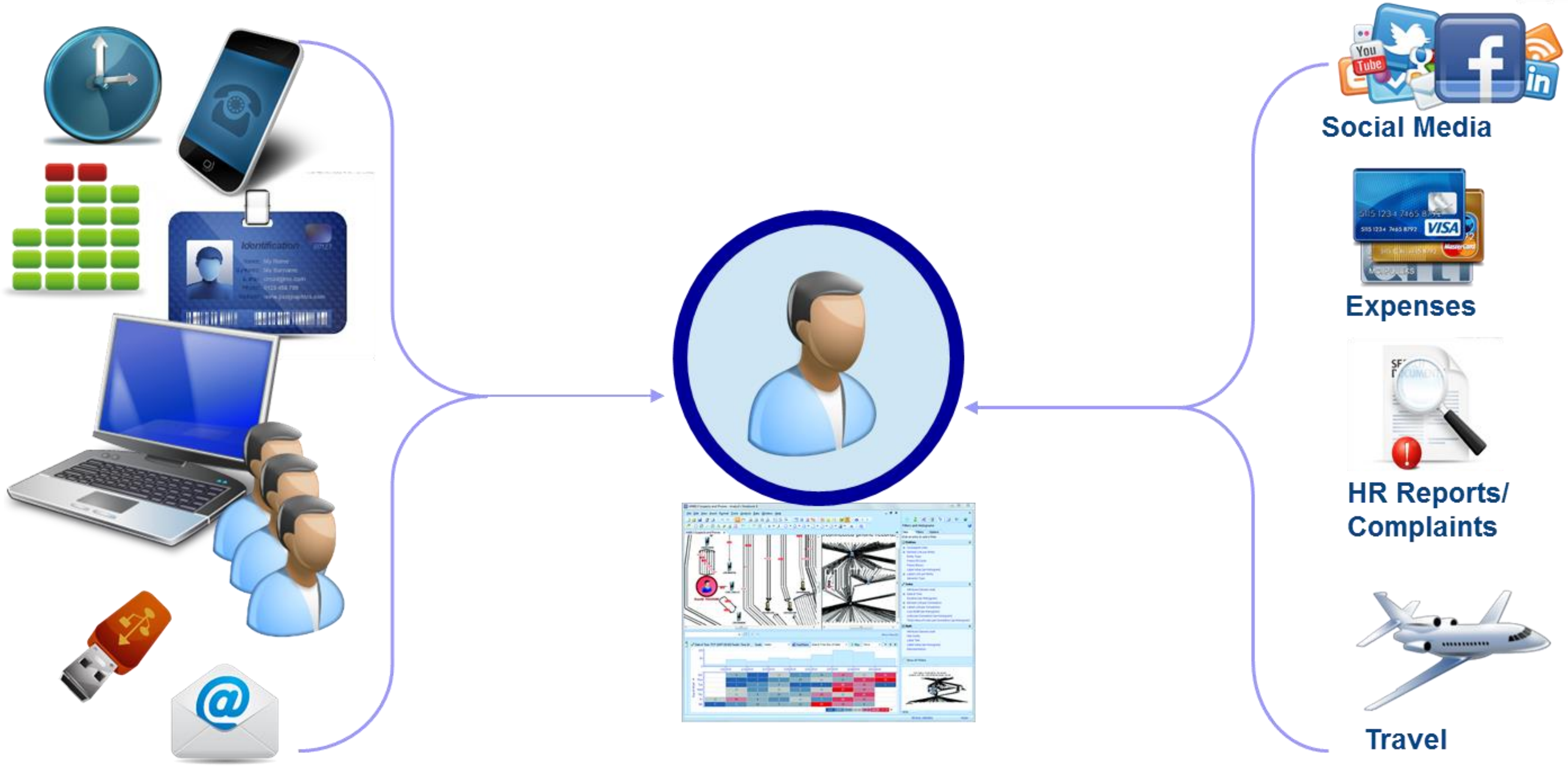
Threat Actor Analysis

Social Media Analysis

Breach Analysis

Risk Analysis

The Whole Picture Approach Internal



Social Media

Expenses

HR Reports/ Complaints

Travel

Key Takeaways

- The Cyber Security market is large and growing at and impressive rate
- Cyber Security is growing towards being proactive, not just defensive
- Organisations need investigative solutions that extend to areas that traditional security and IT security solutions do not

- Cyber Security and Intelligence is an ever-changing environment
- New applications and solutions pose unknown threats
- The malware foot print changes daily
- Threat actors and groups move and change alliances
- Crumbling perimeters pose new protection challenges

Insider Threats

Does your organization have a process in place to learn from incidents and share with others, internally and externally, to prevent the same thing from happening again?

a) Yes
b) No
c) Not sure

Do you feel like you have a complete picture of the cyber threats to your organization? Have you had instances where you felt you could have prevented or disrupted an attack more quickly?

a) Yes
b) No
c) Not sure

Is the organization looking to uncover unknown security threats?

a) Yes
b) No
c) Not sure

Does your organization collect data on adversaries? How do you use that data to understand their relationships, motives, targets and capabilities?

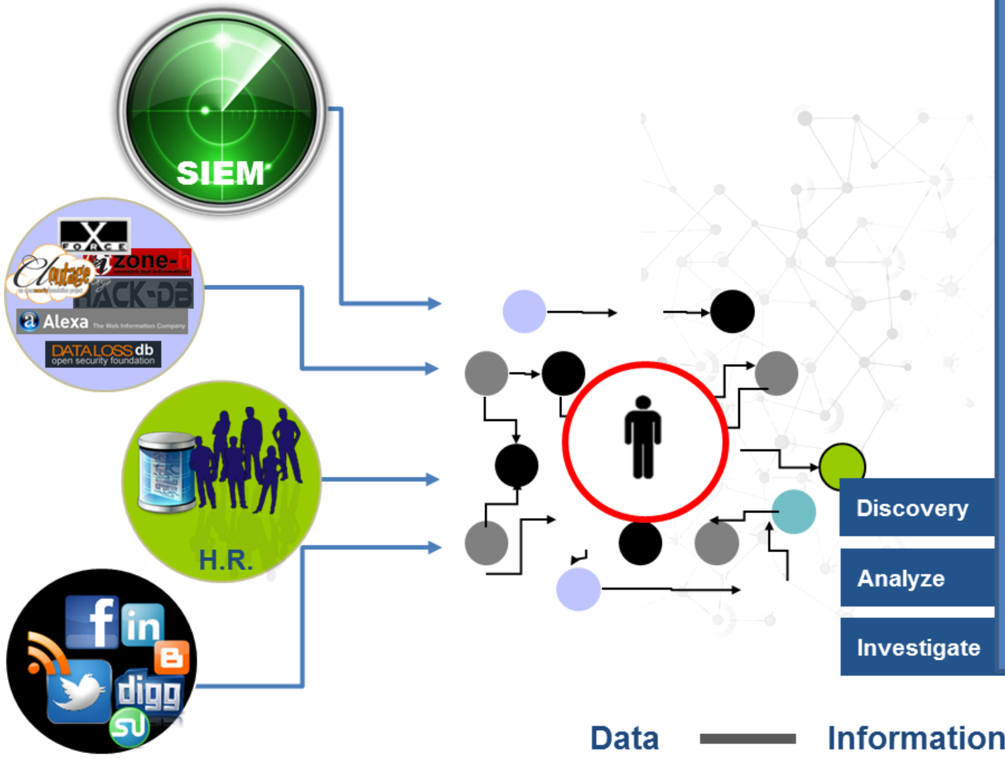
a) Yes
b) No
c) Not sure

How effective have you been in determining your infrastructure weaknesses? Do you run exercises on various types of attacks so you know how to proceed very quickly when you are faced with them?

a) Yes
b) No
c) Not sure

External Threats

Key Takeaways


SIEM
X-FORCE
zone-h
Outage
HACK-DB
Alexa The Web Information Company
DATALOSS db open security foundation
H.R.
digg

Discovery

Analyze

Investigate

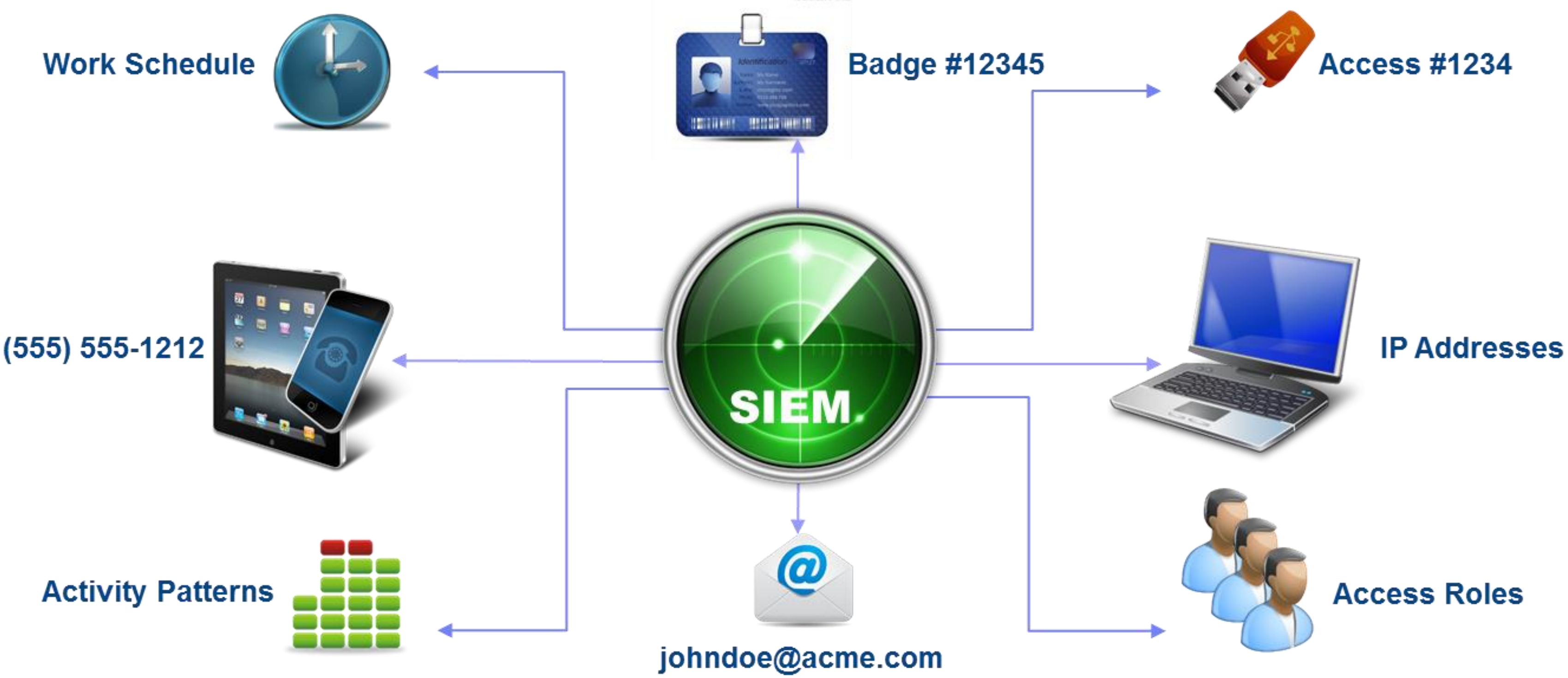
Improved Cyber Threat Analysis

Know **where**, **when**, **why**, **how** and by **whom** your network is being compromised.

- Understand threats and their consequences
- Discover monitoring weaknesses in the infrastructure for policy adjustment
- Develop tactical intelligence for remediation
- Discover anomalies with Data, Network and User information – unacceptable usage
- Create "Kill Chain" intelligence on **what** can occur or has occurred
- Define threat actors (including insiders) and motivation
- Link known associates and groups
- Identify potential digital asset losses, methods, and the exploitation of the asset.

Data — **Information** → **Counter Intelligence**

Know the Insiders. Chances are, they are not sophisticated attackers.


Work Schedule
Badge #12345
Access #1234
(555) 555-1212
SIEM
IP Addresses
Activity Patterns
johndoe@acme.com
Access Roles