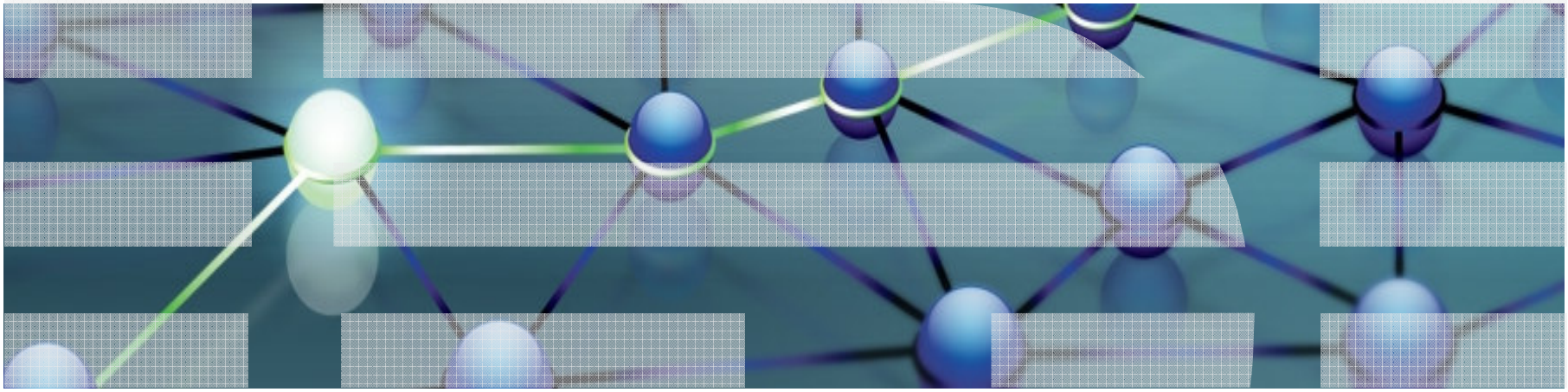
IBM Security Services Cyber Security Intelligence Index

Analysis of cyber security attack and incident data from IBM's worldwide security operations



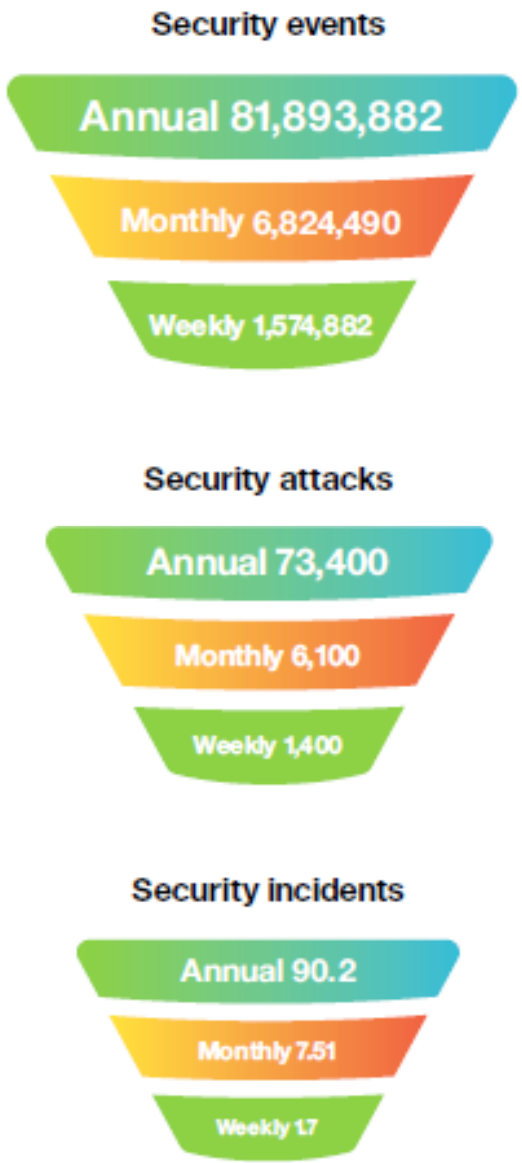


Figure 1. Security intelligence makes it possible to reduce the millions of security events detected annually in any one of our clients' systems to an average of 73,400 attacks—and under 100 incidents—in a single organization over the course of a year .

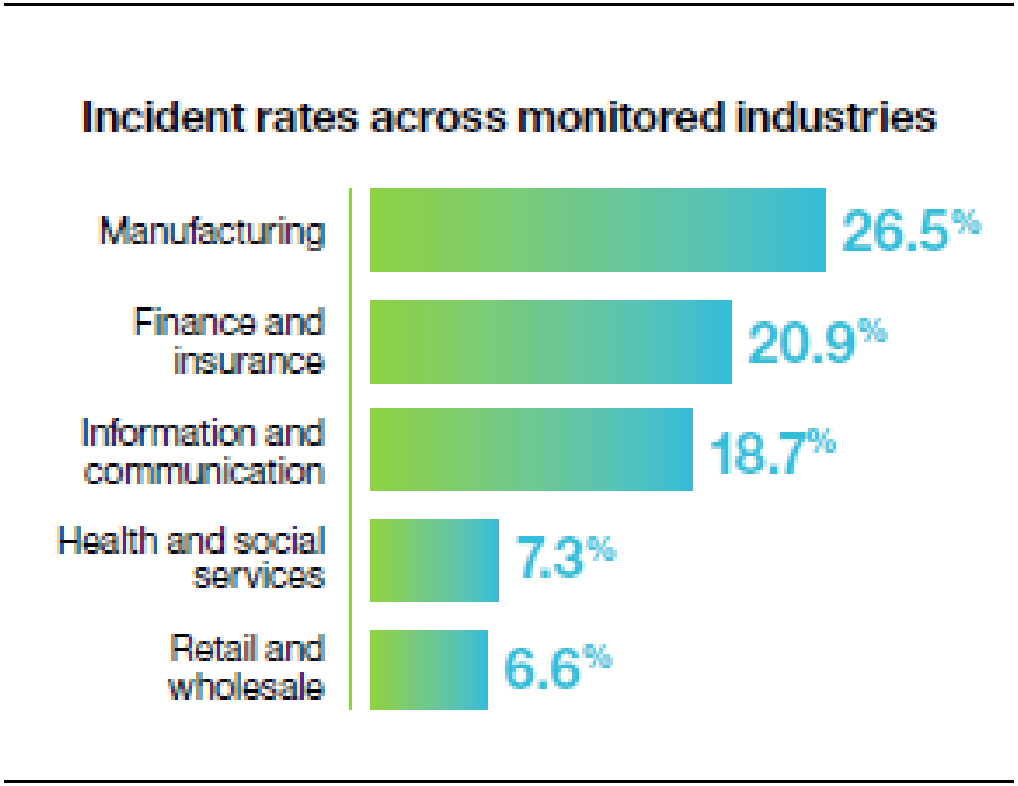


Figure 2. The manufacturing and finance and insurance industries tend to offer attackers the most significant potential payoff.

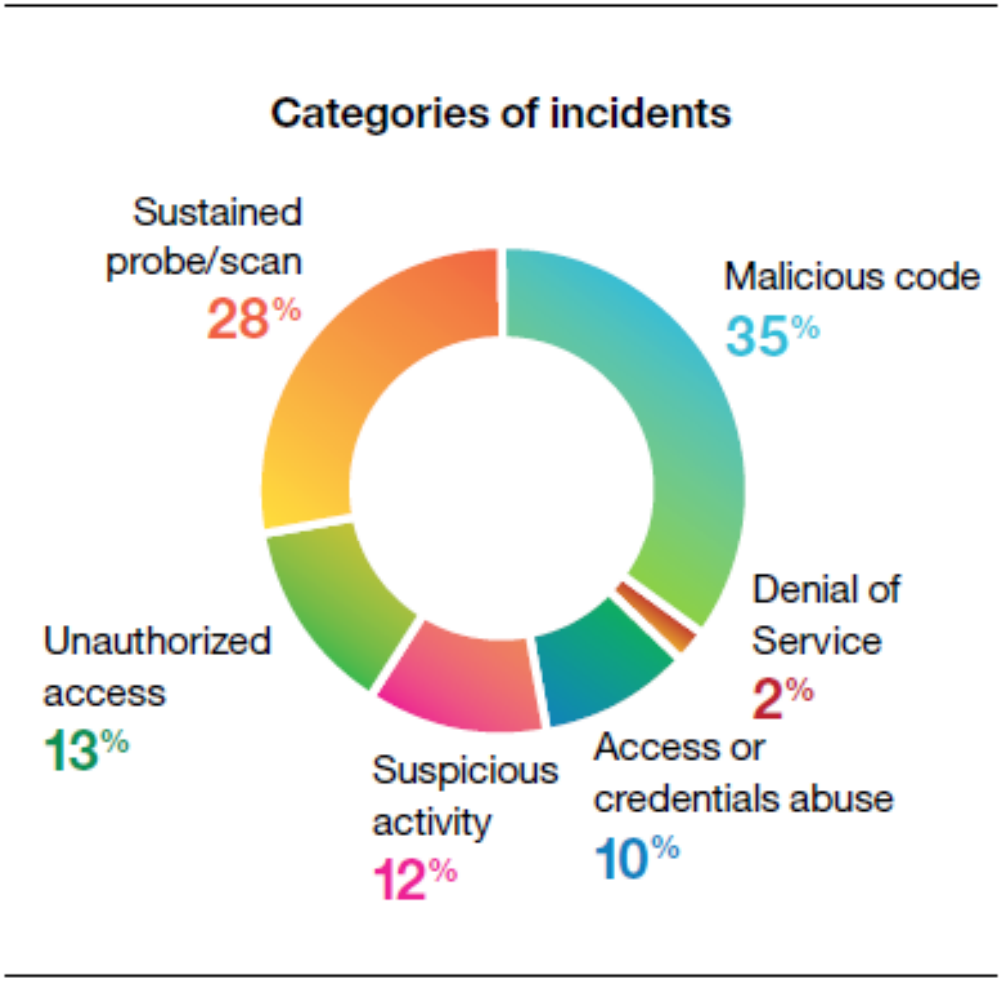


Figure 3. Malicious code and sustained probes or scans top the list of incident categories impacting every industry covered in this report.

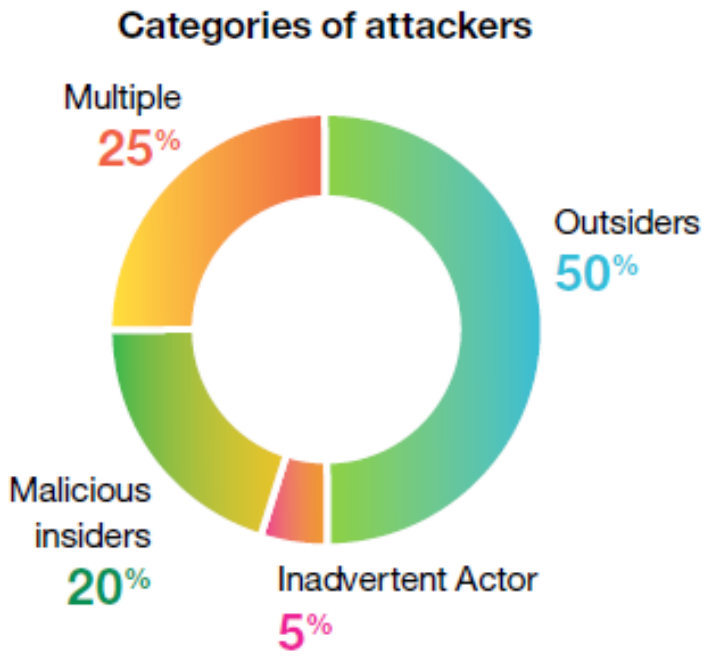


Figure 4. Half of all attacks are most likely to be instigated by outsiders.

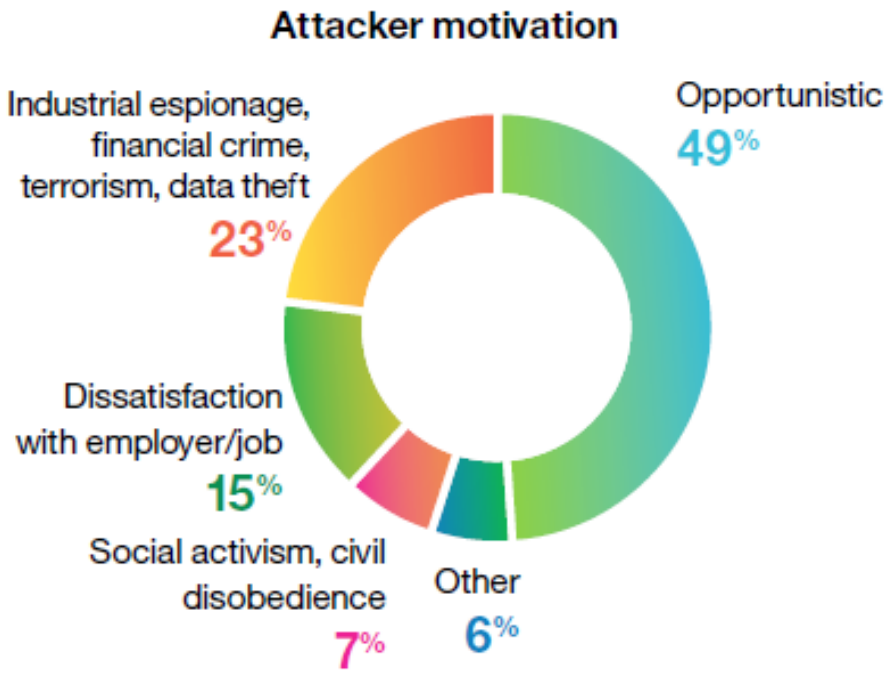


Figure 5. Opportunity served as the prime motivator for nearly half of the attackers we identified and investigated.

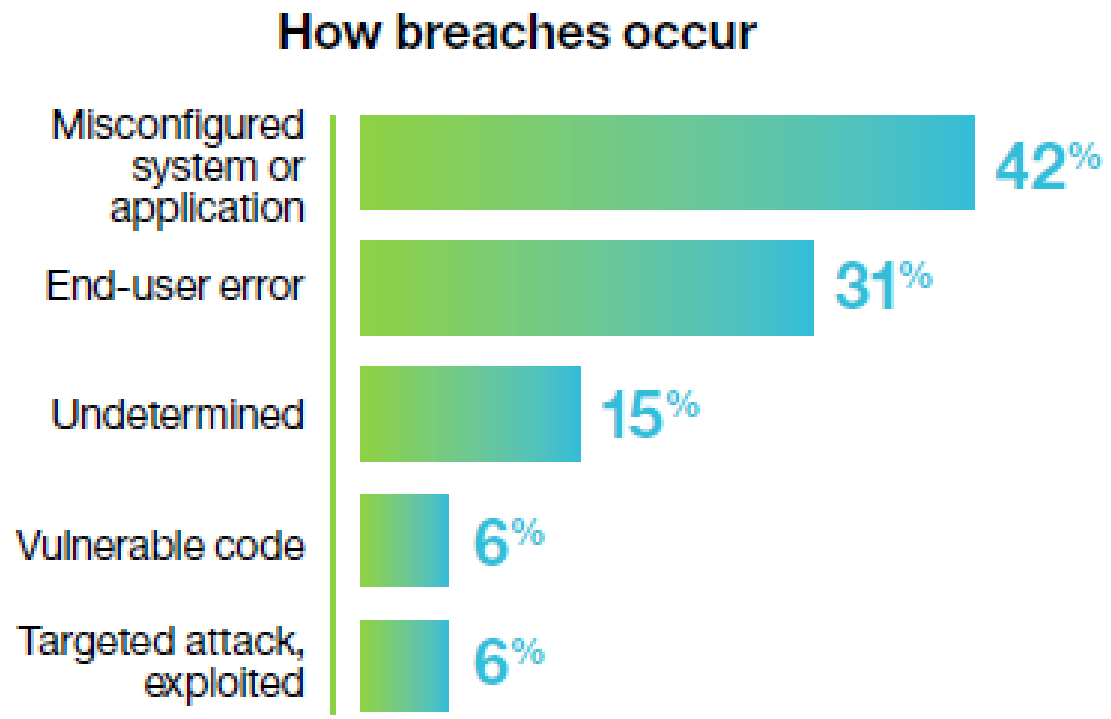


Figure 6. Although preventable errors are often to blame for security incidents, it was impossible to identify the culprit in nearly 20 percent of the cases we examined.

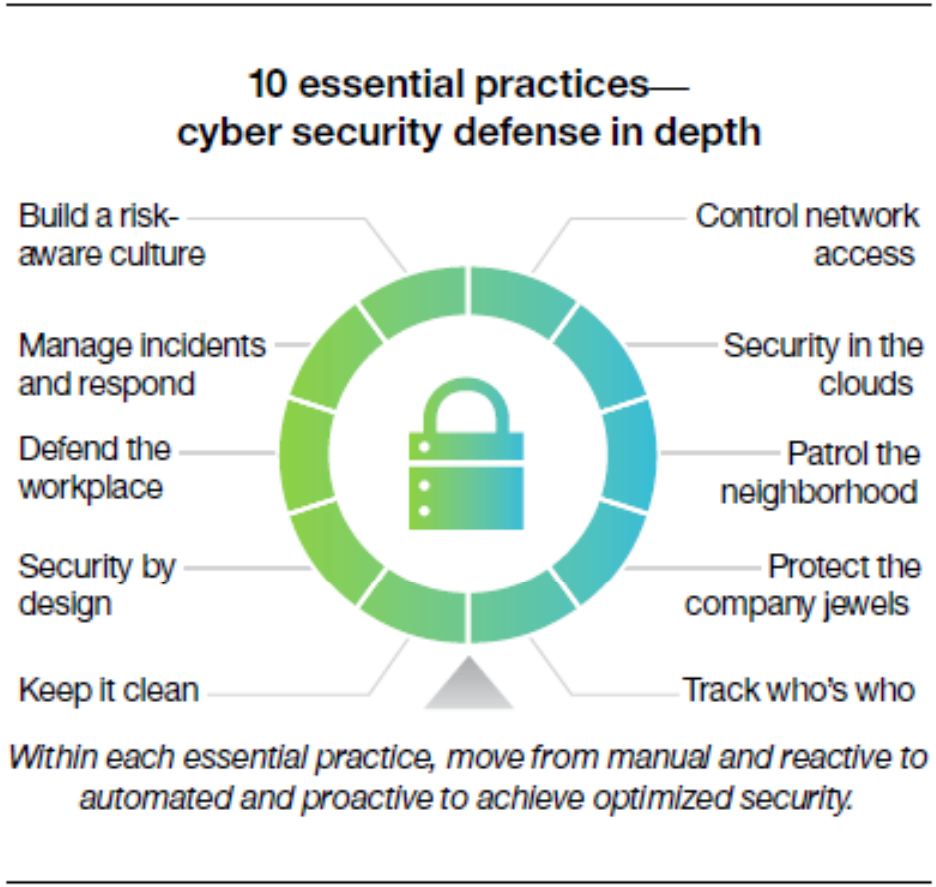
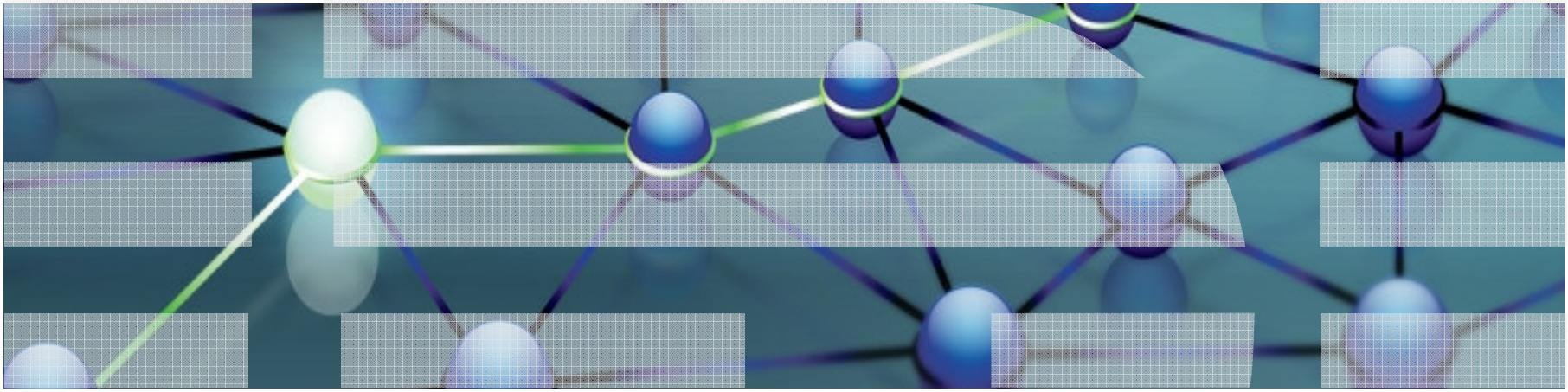
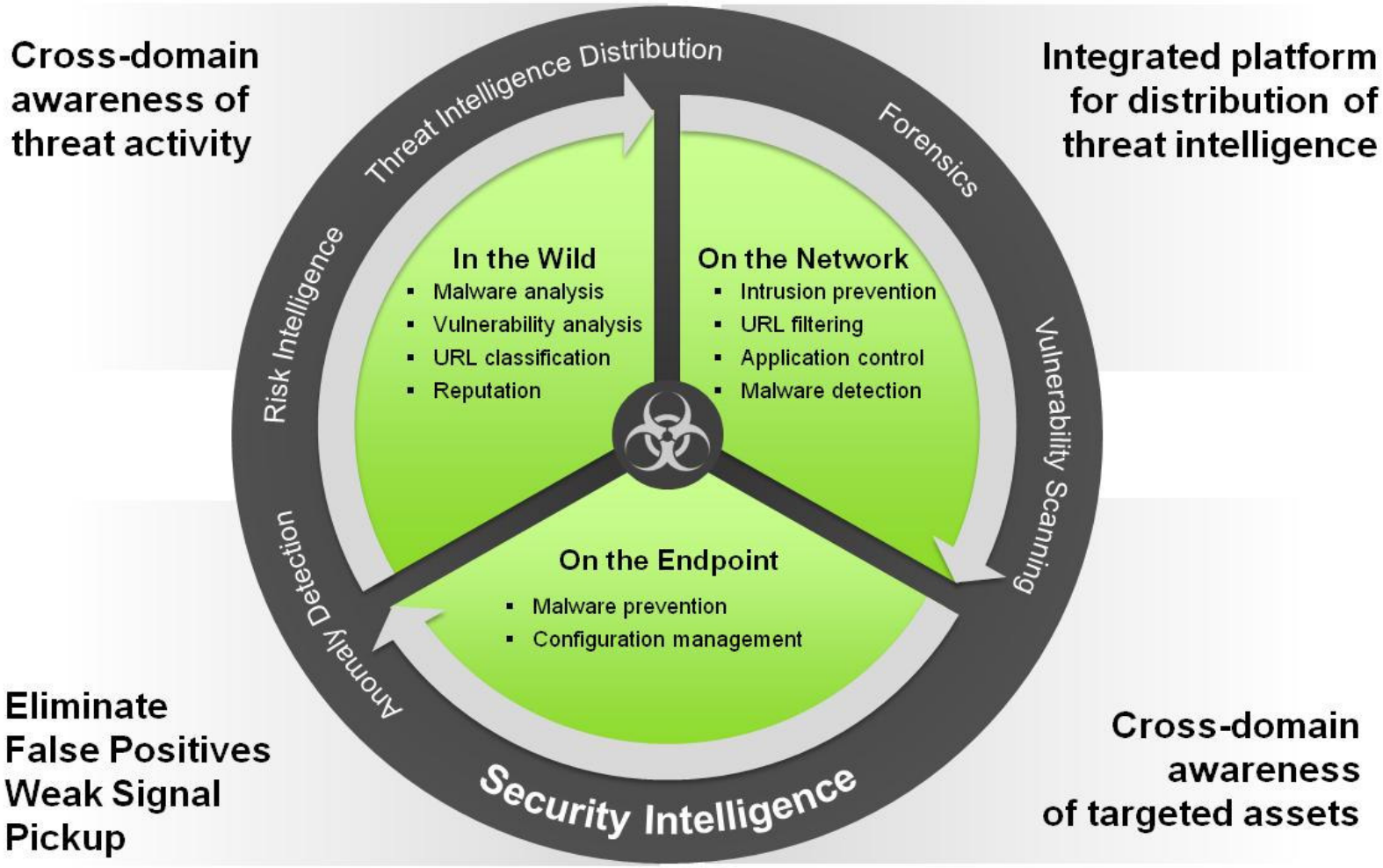


Figure 7. Ten essential practices: A successful security program strikes a balance that allows for flexibility and innovation while maintaining consistent safeguards that are understood and practiced throughout the organization.

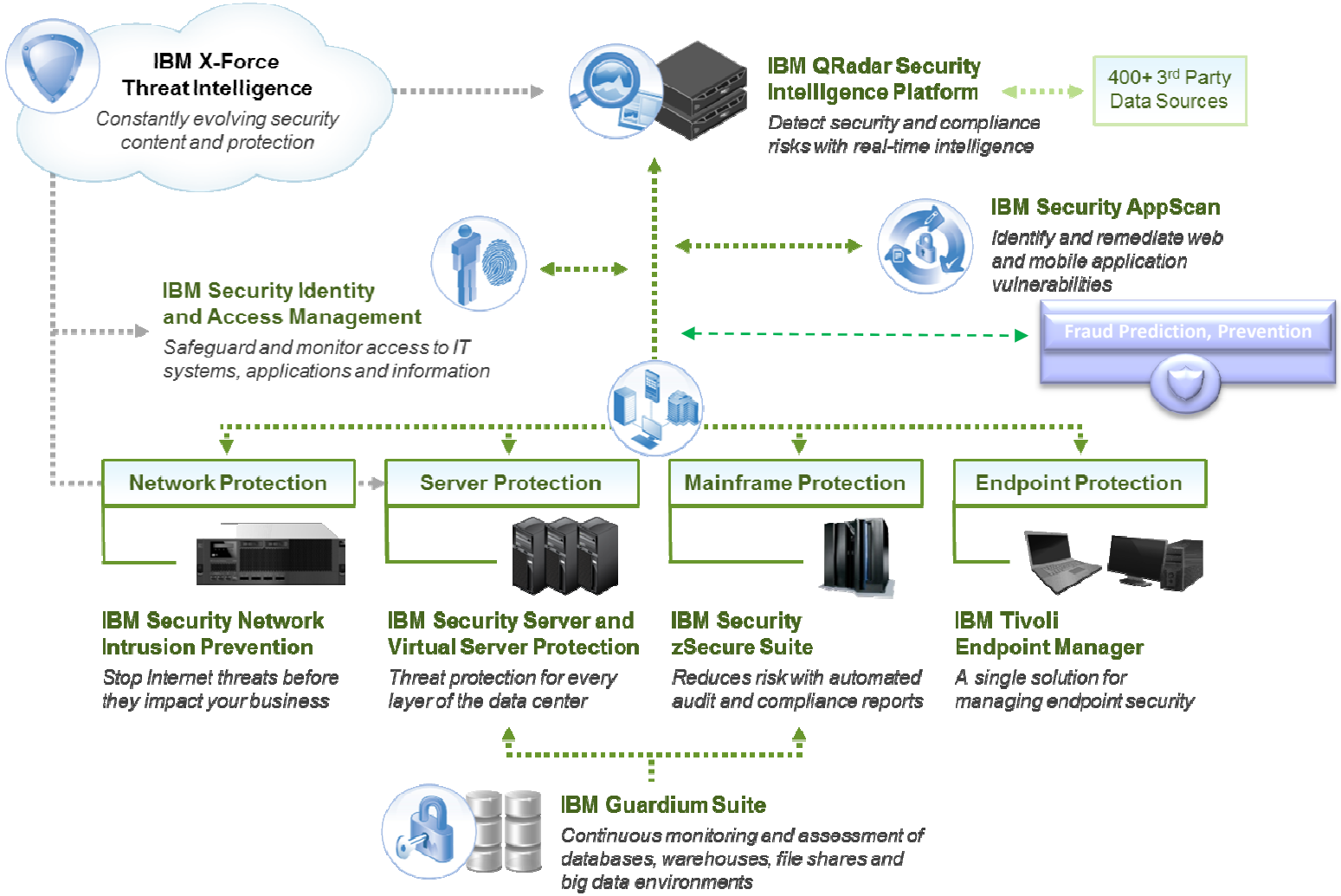
Counter
Advanced Persistent Threat
with
IBM Advanced Persistent Intelligence



IBM's Vision for Integrated Advanced Threat Protection



In-The-Wild Protection: X-Force Intelligence



Attackers are using sophisticated techniques to bypass defenses

Off-the-Shelf tools and techniques

Sophisticated

- Indiscriminate
- Lack sophisticated technical skills
- Use tool chest of exploit and malware kits
- Botnet builders
- Financially motivated malware activity
- Spam and DoS

- Cyberwar

Broad

- Financially motivated targeted hacks
- DDoS attacks
- LulzSec and Anonymous (hacktivists)

- Advanced Persistent Threat
- Organized, state sponsored teams
- Discovering new zero-day vulns
- Unprecedented attack techniques

Targeted

"Advanced Persistent Threat" is the approach often used by State-Sponsored Entities

Source: IBM X-Force Research and Development

What's different about Advanced Persistent Threats?

Advanced

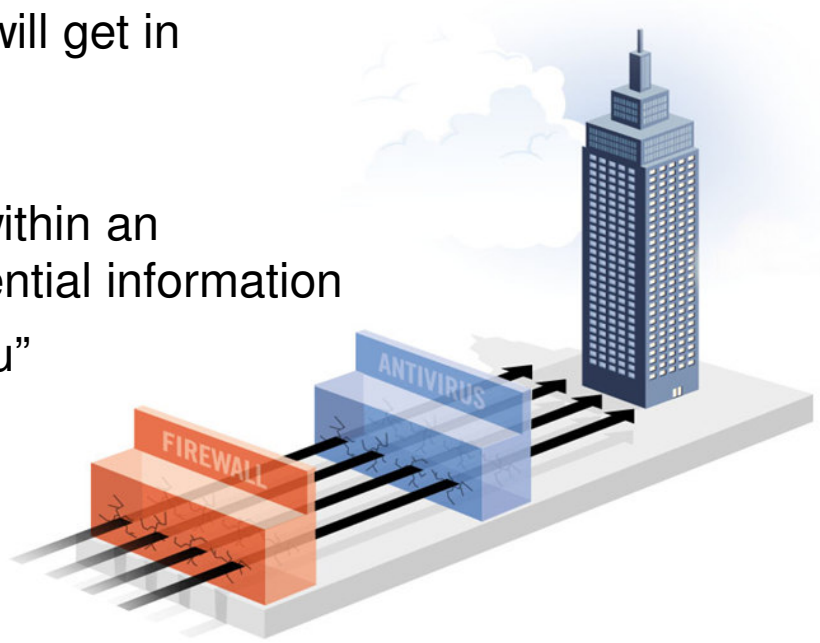
- Exploiting unreported (zero-day) vulnerabilities
- Advanced, custom malware is not detected by antivirus products
- Coordinated, well researched attacks using multiple vectors

Persistent

- Attacks last for months or years (average: 1 year; longest: 4.8 years)[1]
- Attackers are dedicated to the target – they will get in

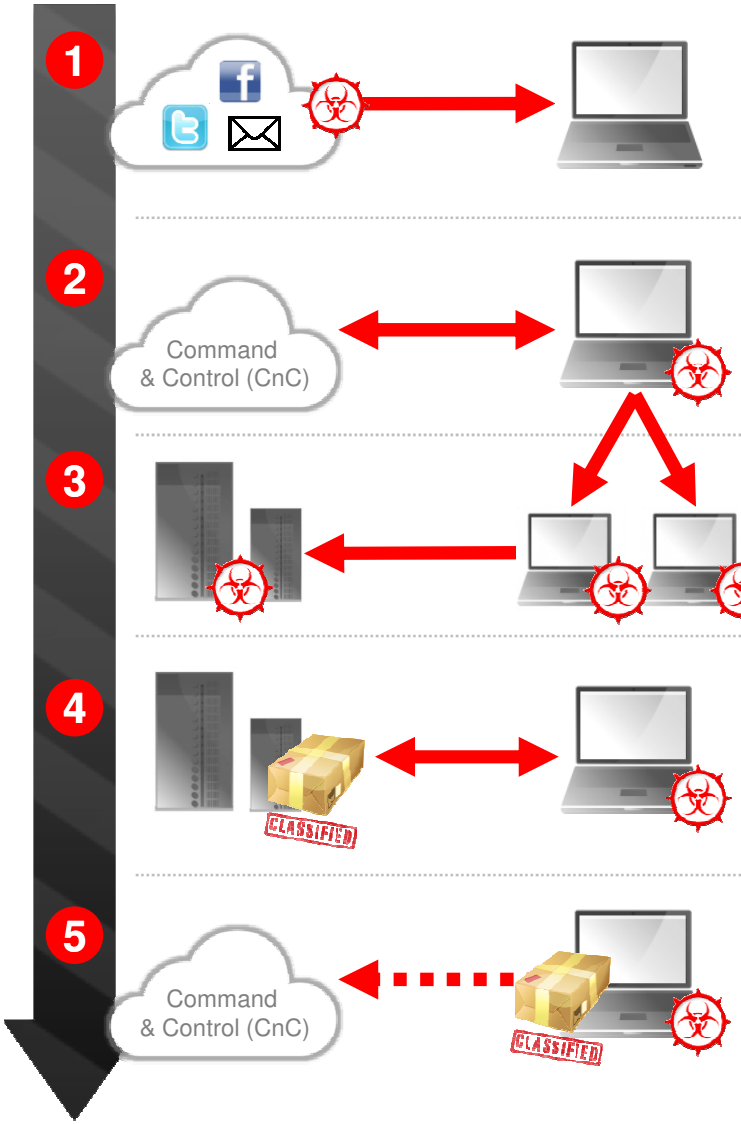
Threat

- Targeted at specific individuals and groups within an organization; aimed at compromising confidential information
- Not random attacks – they are "out to get you"



1) Source: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Attackers follow a 5-Stage attack chain



Break-in

Spear phishing and remote exploits to gain access

Latch-on

Malware and backdoors installed to establish a foothold

Expand

Reconnaissance and lateral movement to increase access and maintain a presence

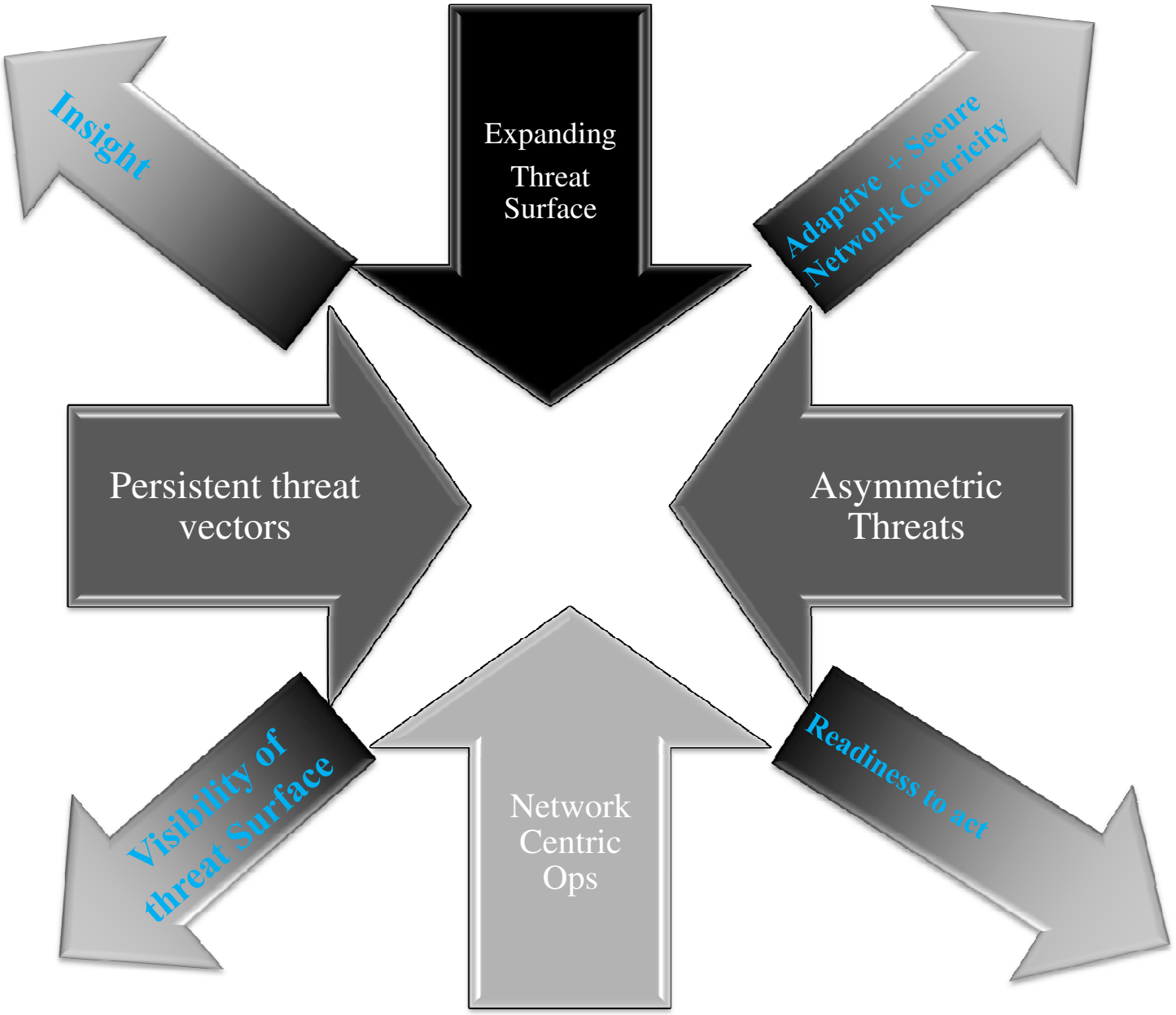
Gather

Acquisition and aggregation of confidential data

Exfiltrate

Data exfiltration to external networks

The Challenges & the Imperatives



What X-Force Intelligence means to the threat

URGENT: Need your assistance immediately!

From: James Fowler, CFO [james.fowler.acmeco@yahoo.com]

To: Lori Jones, Bill Smith, Philip White

Sent: Tuesday, 10 August 2013, 7:00 am

Team,

I just got off the phone with our auditors, and we have discovered a huge problem with this year's financial reports. The board is counting on us to get this addressed immediately!

Please click here for the details.

I'll be setting up a conference call to discuss within the hour, so please look at this right away.

James Fowler
Chef Financial Officer
AcmeCo
24 West 23rd Street, New York, NY
+1.212.555.1212

X-Force reputation data categorizes:

Phishing sites
Malware sites
Botnet command & control
Anonymous proxies
Uncategorized sites

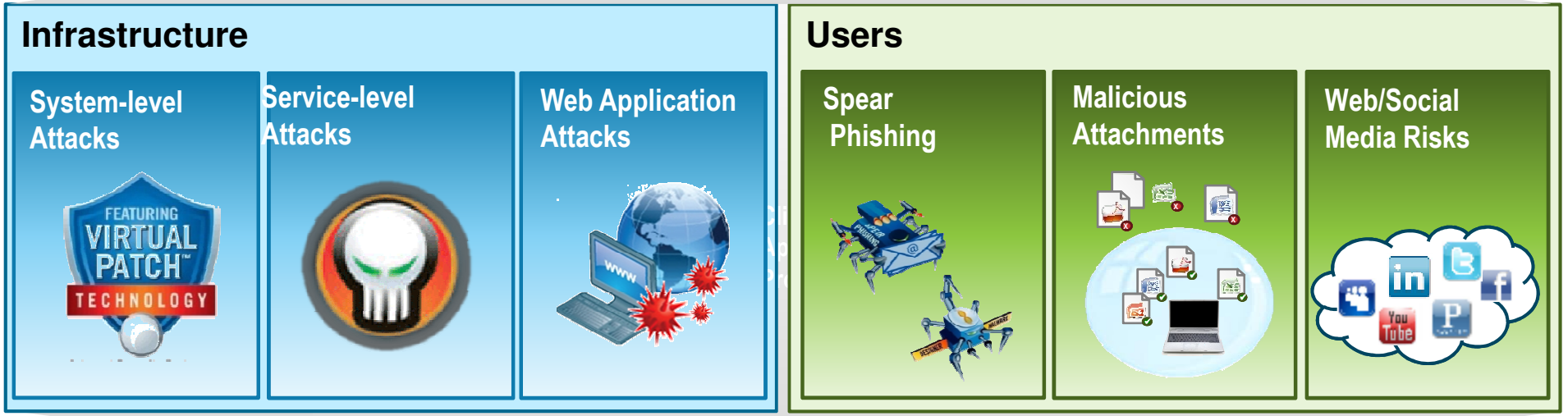
NETWORK PROTECTION

Network Protection:
The XGS 5100 Next-Generation IPS

ADVANCED THREAT PROTECTION	COMPREHENSIVE VISIBILITY & CONTROL	SEAMLESS DEPLOYMENT & INTEGRATION
Proven protection from sophisticated and constantly evolving threats, powered by X-Force®	Helps discover and block existing infections and rogue applications while enforcing access policies	Adaptive deployment and superior integration with the full line of IBM security solutions

Advanced Threat Protection

The XGS 5100 helps protect against a full spectrum of targeted attacks, even in SSL-encrypted connections



Extensible, Ahead-of-the-Threat Protection

backed by the power of IBM X-Force® to help protect against mutating threats

Comprehensive Visibility & Control

Context-aware access control policies block pre-existing infections, rogue applications, and policy violations

Deep Packet Inspection fully classifies network traffic, regardless of address, port , protocol, application, application action or security event

Complete Identity Awareness associates valuable users and groups with their network activity, application usage and application actions

Access Control Policies block pre-existing compromises and rogue applications as well as enforce corporate usage policies

400+
Protocols and File Formats Analyzed

2,000+
Applications and Actions Identified

20 Billion+
URLs classified in 70 Categories

What Network Protection means to the threat

URGENT: Need your assistance immediately!

From: James Fowler, CFO [james.fowler.acmeco@yahoo.com]

To: Lori Jones, Bill Smith, Philip White

Sent: Tuesday, 10 August 2013, 7:00 am

Team,

I just got off the phone with our auditors, and we have discovered a huge problem with this year's financial reports. The board is counting on us to get this addressed immediately!

Please click here for the details.

I'll be setting up a conference call to discuss within the hour, so please look at this right away.

James Fowler
Chef Financial Officer
AcmeCo
24 West 23rd Street, New York, NY
+1.212.555.1212

Blocks malicious links
Leveraging X-Force Intelligence

Blocks malicious attachments
Utilizing advanced heuristics

Disrupts command and control
To disable existing infections

ENDPOINT PROTECTION

Trusteer Apex: Three Security Layers

Stop exploitation of user application vulnerabilities

Prevent drive-by downloads

Block malware communication

Prevent information theft

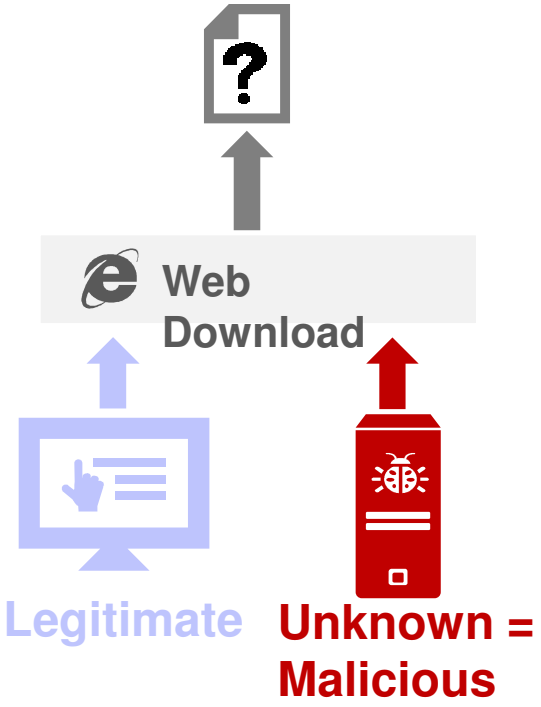
Block key-loggers

Prevent submission on phishing sites

Prevent reuse on public consumer sites

Exploit Prevention: Automatically prevent application exploitation

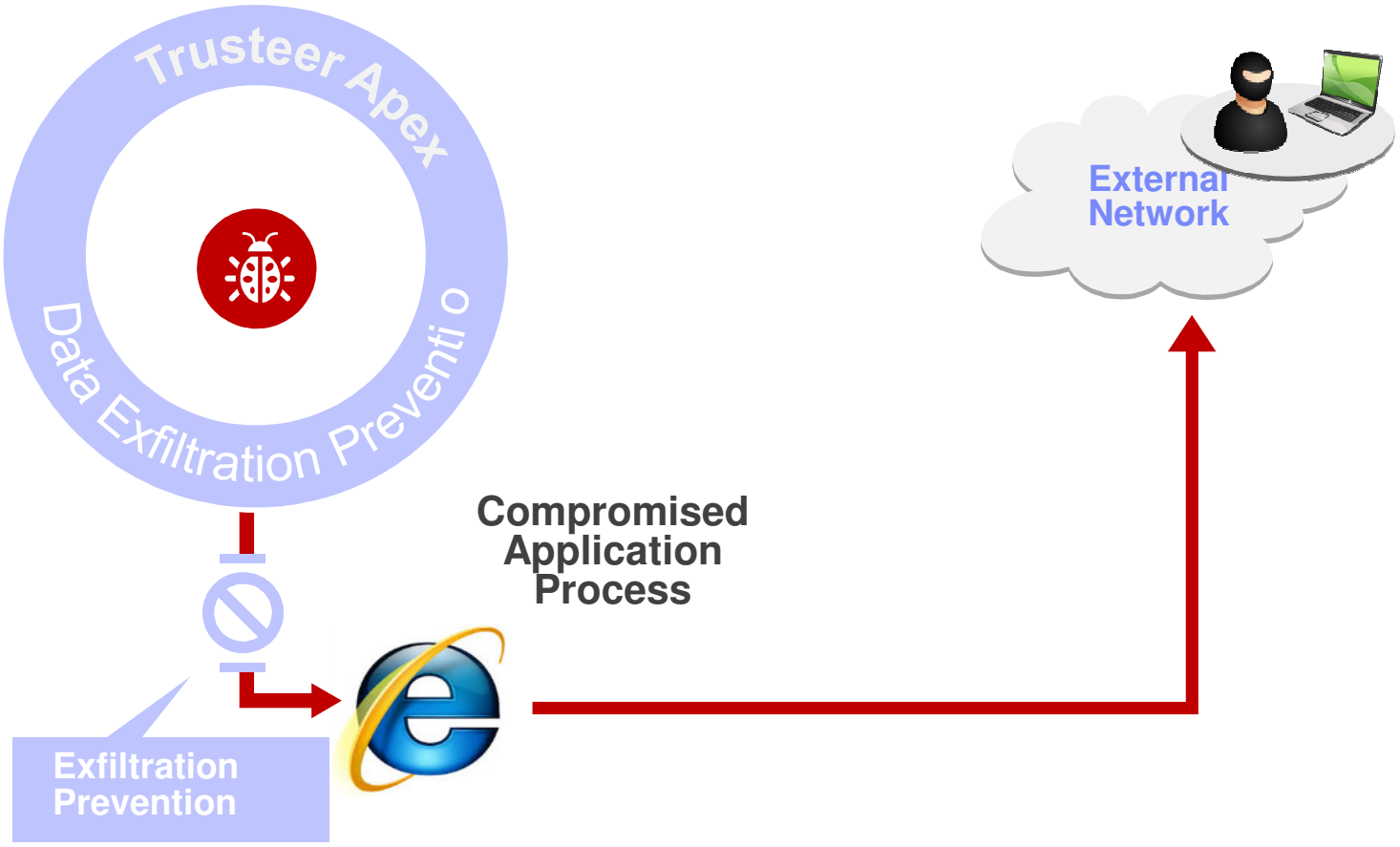
What is the application doing?	**Action:** a file is written to the file system and executed
Why is it doing it?	**State:** user initiated download OR **UNKNOWN**



If action and state are not pre-approved:

action is stopped, infection prevented

Stop Malware Communication by Preventing Application Compromise



What Endpoint Protection means to the threat

URGENT: Need your assistance immediately!

From: James Fowler, CFO [james.fowler.acmeco@yahoo.com]

To: Lori Jones, Bill Smith, Philip White

Sent: Tuesday, 10 August 2013, 7:00 am

Team,

I just got off the phone with our auditors, and we have discovered a huge problem with this year's financial reports. The board is counting on us to get this addressed immediately!

Please click here for the details.

I'll be setting up a conference call to discuss within the hour, so please look at this right away.

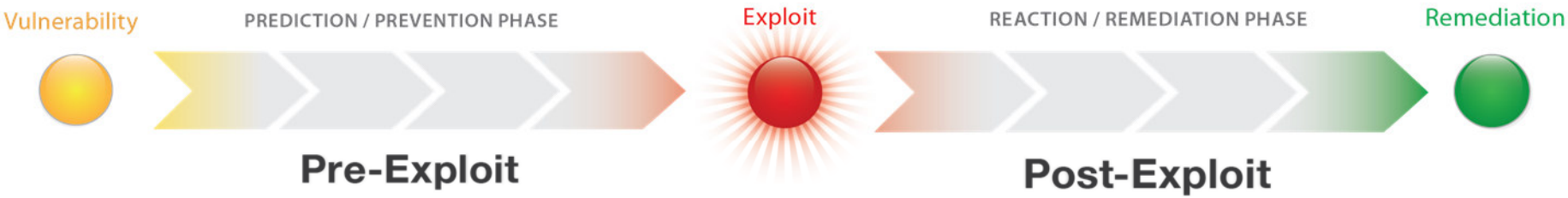
James Fowler
Chef Financial Officer
AcmeCo
24 West 23rd Street, New York, NY
+1.212.555.1212

Blocks Malware Infection and Data Exfiltration
using advanced techniques refined from years of preventing fraud for the world's top financial institutions

Security Intelligence

PUTTING IT ALL TOGETHER

Solutions for the full Security Intelligence timeline



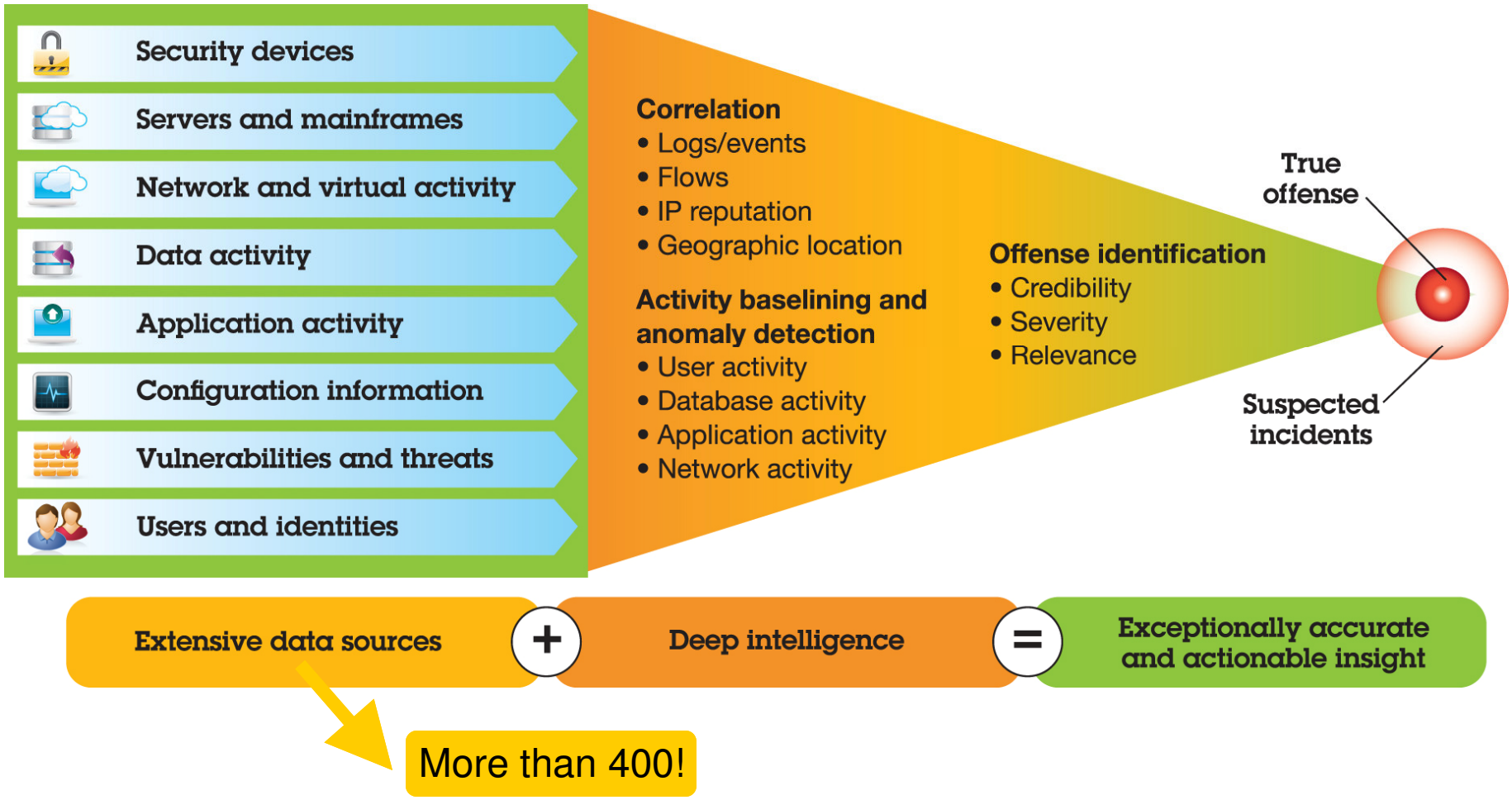
Prediction & Prevention

Risk Management. Vulnerability Management.
Configuration and Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management.
Reporting and Scorecards.

Reaction & Remediation

Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Leak Prevention.
Security Information and Event Management.
Log Management. Incident Response.

Taking Data from a Wide Spectrum of Feeds



IBM X-Force® Threat Information Center

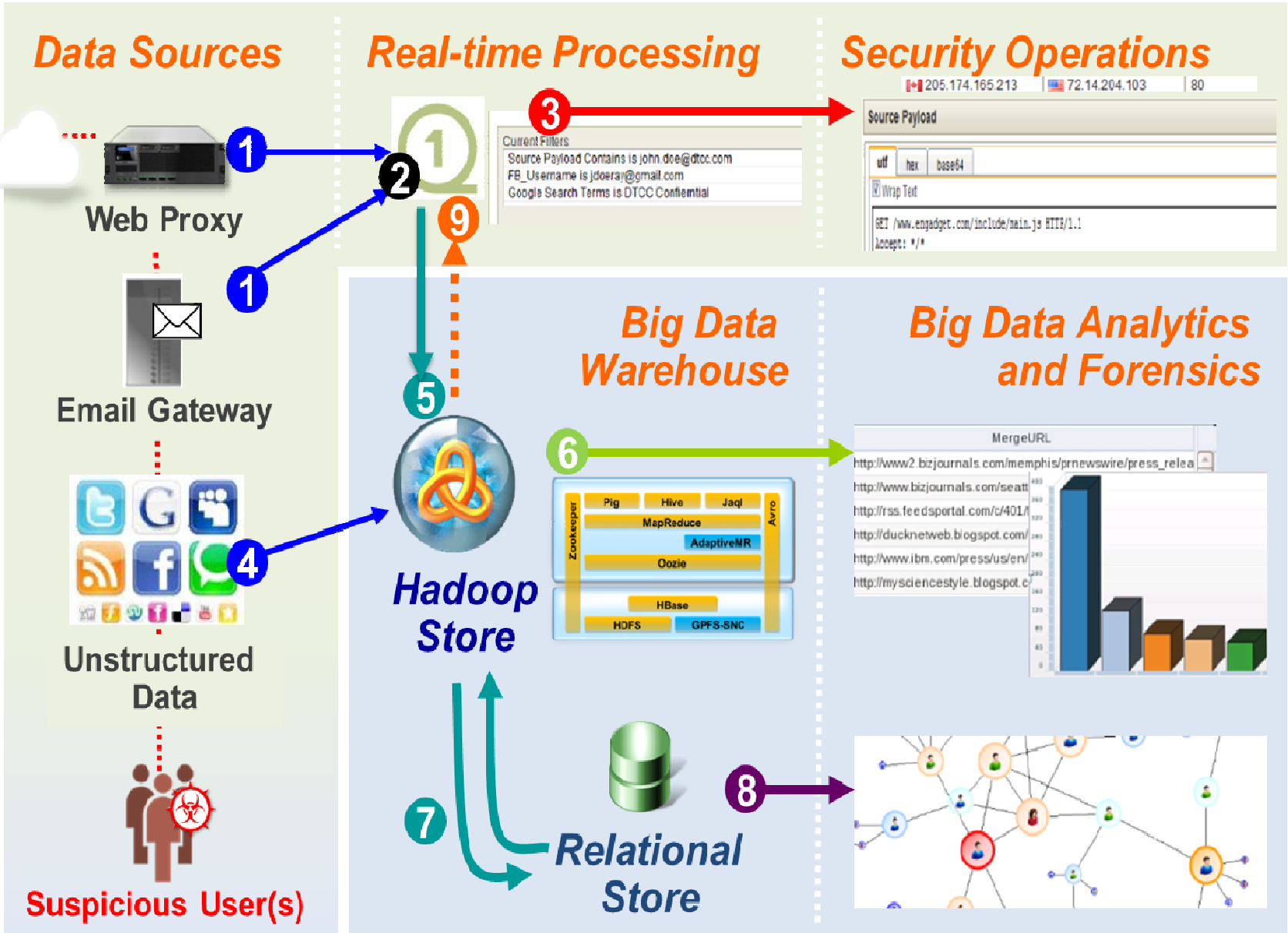
Real-time Security Overview w/ IP Reputation Correlation

Identity and User Context

Real-time Network Visualization and Application Statistics from Flow Data

Inbound Security Events

360 Degree Threat Intelligence



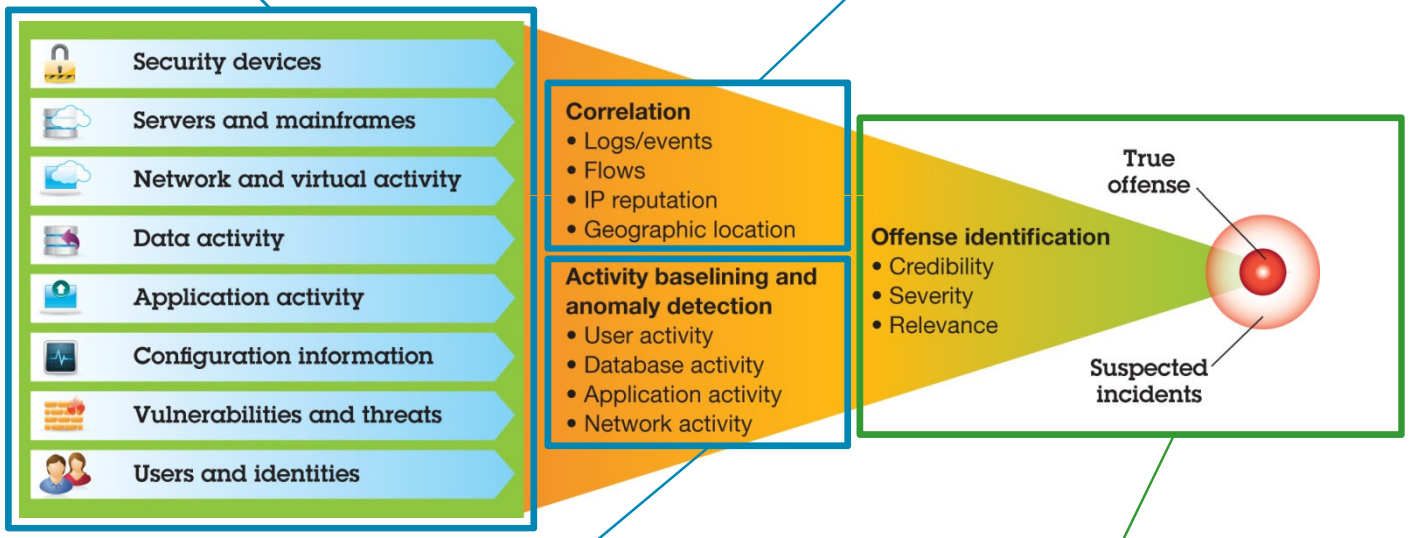
Leverage advanced analytics across all stages of the attack

Monitor everything

Logs, network traffic, user activity

Correlate intelligently

Connect the dots of disparate activity



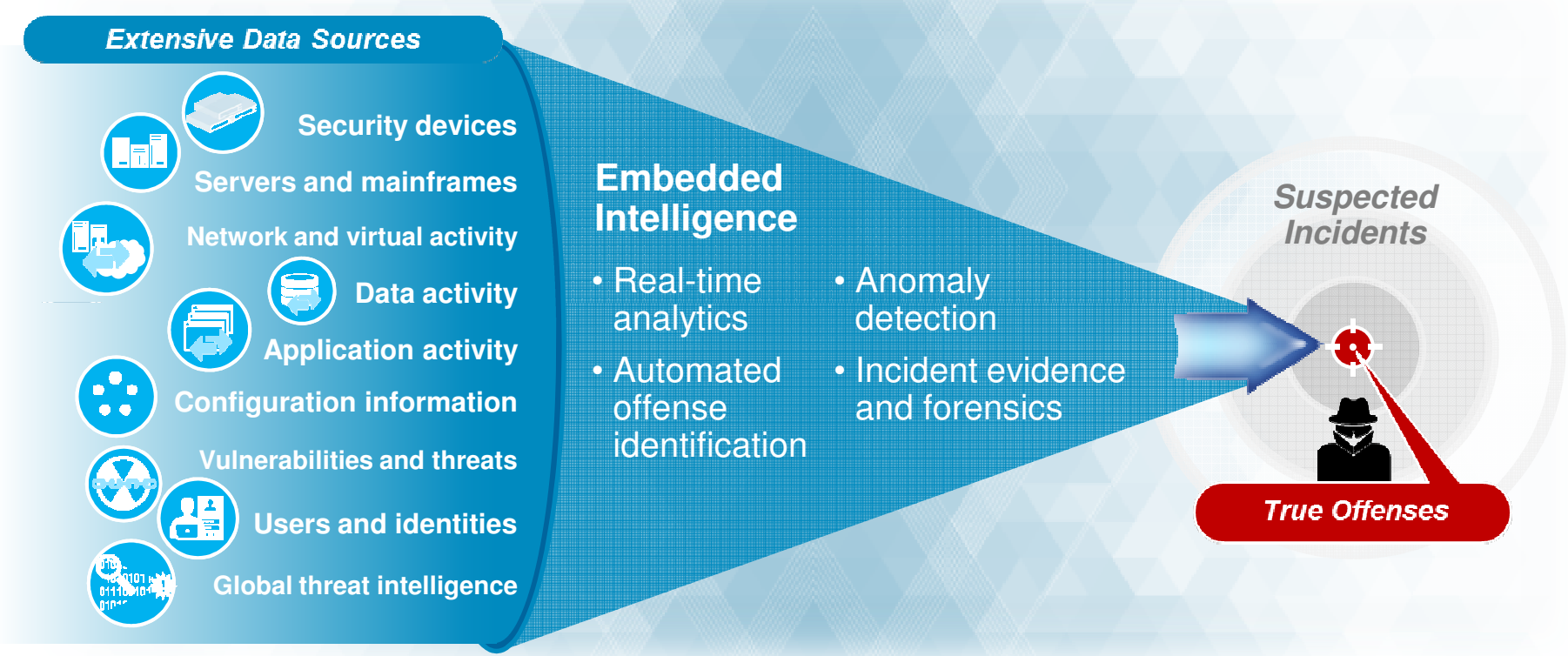
Detect anomalies

Unusual yet hidden behavior

Prioritize for action

Attack high-priority incidents

Use intelligence and anomaly detection across every domain



Gain insights to prioritize what is most critical

2 Billion logs and events per day

25 high priority offenses

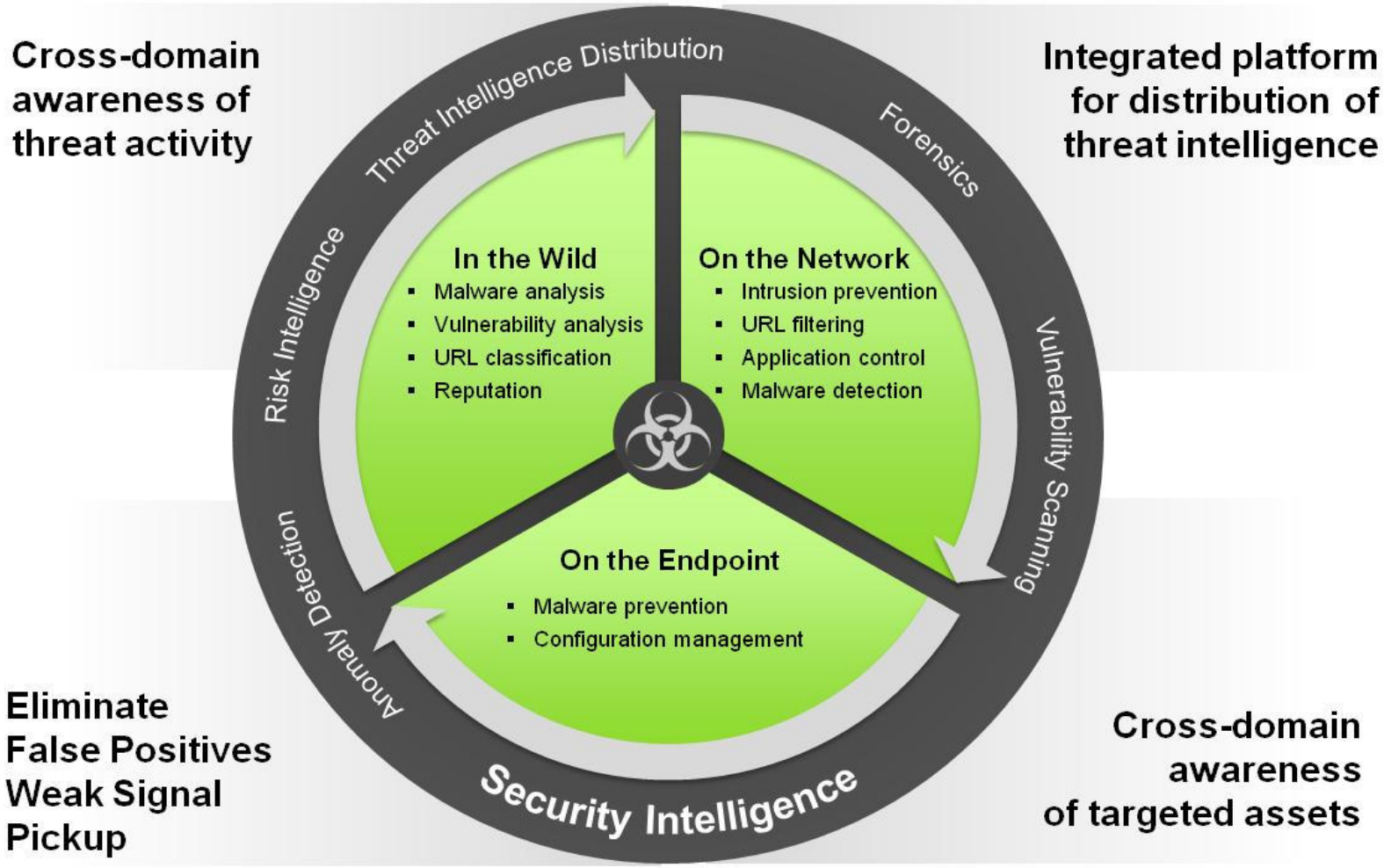
QRadar Security Intelligence Platform

Source: IBM client example

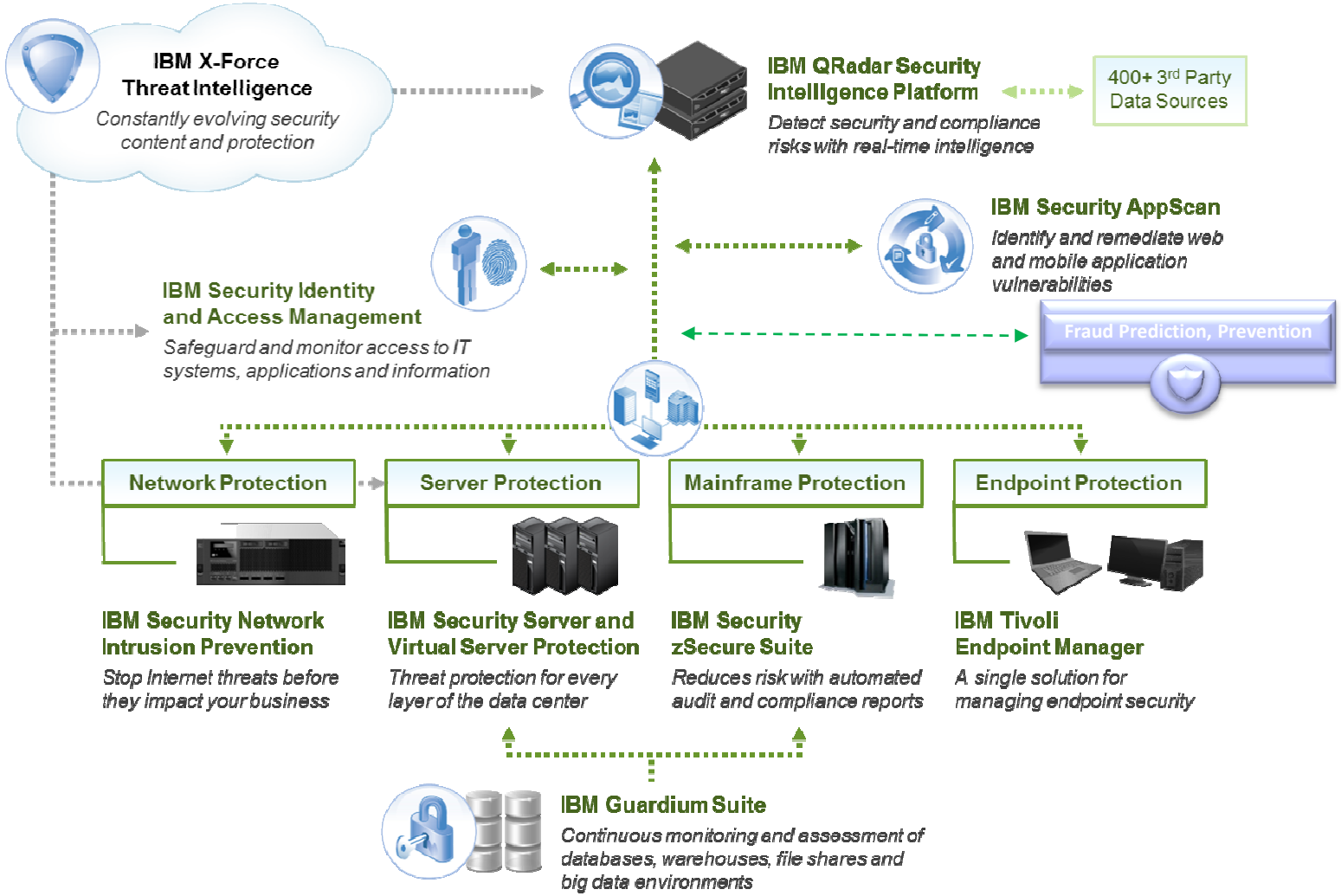
Thank You !

Krishnan Jagannathan
+65 9010 7275 krishnan@sg.ibm.com
Business Advisor, Institute of Advanced Security

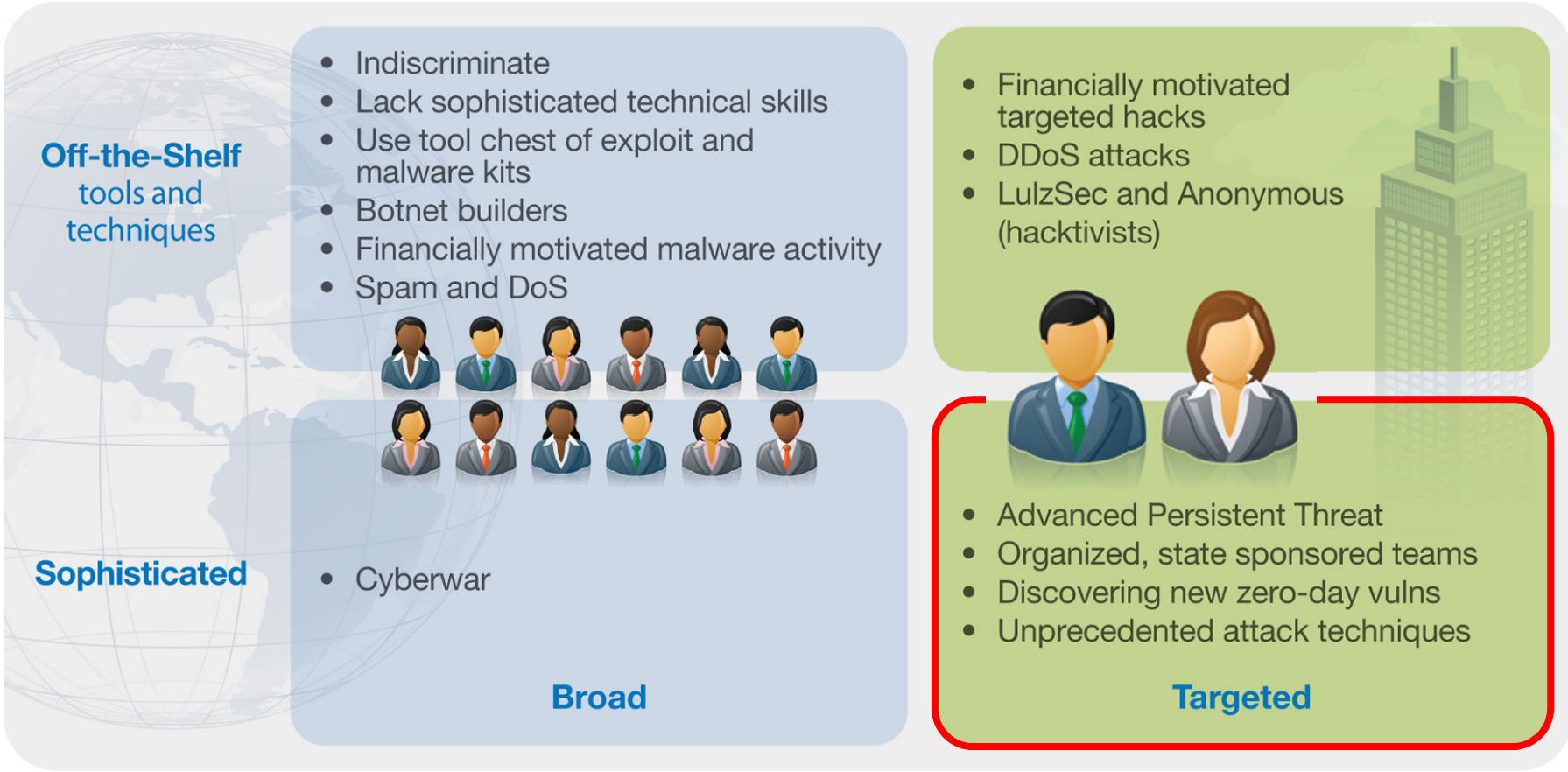
IBM's Vision for Integrated Advanced Threat Protection



In-The-Wild Protection: X-Force Intelligence



Attackers are using sophisticated techniques to bypass defenses



"Advanced Persistent Threat" is the approach often used by State-Sponsored Entities

Source: IBM X-Force Research and Development

What's different about Advanced Persistent Threats?

Advanced

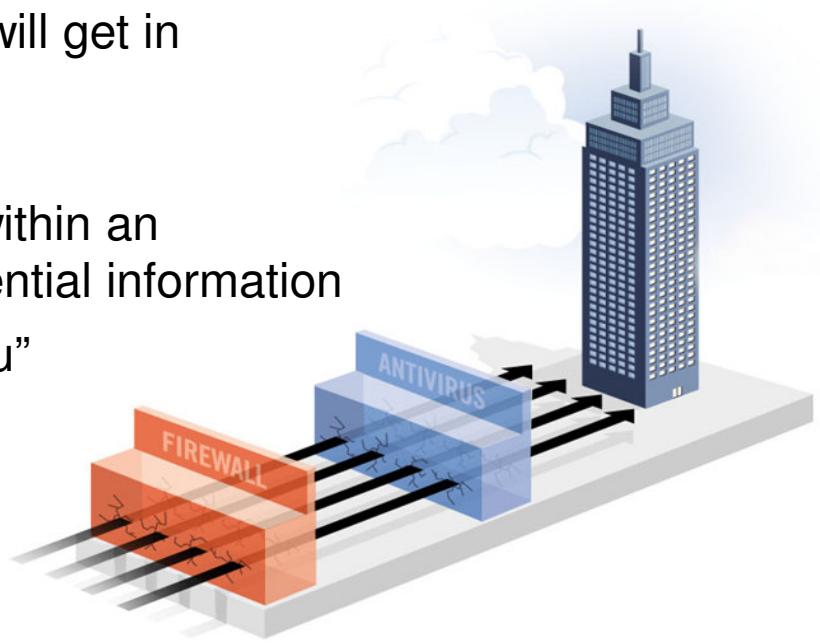
- Exploiting unreported (zero-day) vulnerabilities
- Advanced, custom malware is not detected by antivirus products
- Coordinated, well researched attacks using multiple vectors

Persistent

- Attacks last for months or years (average: 1 year; longest: 4.8 years)[1]
- Attackers are dedicated to the target – they will get in

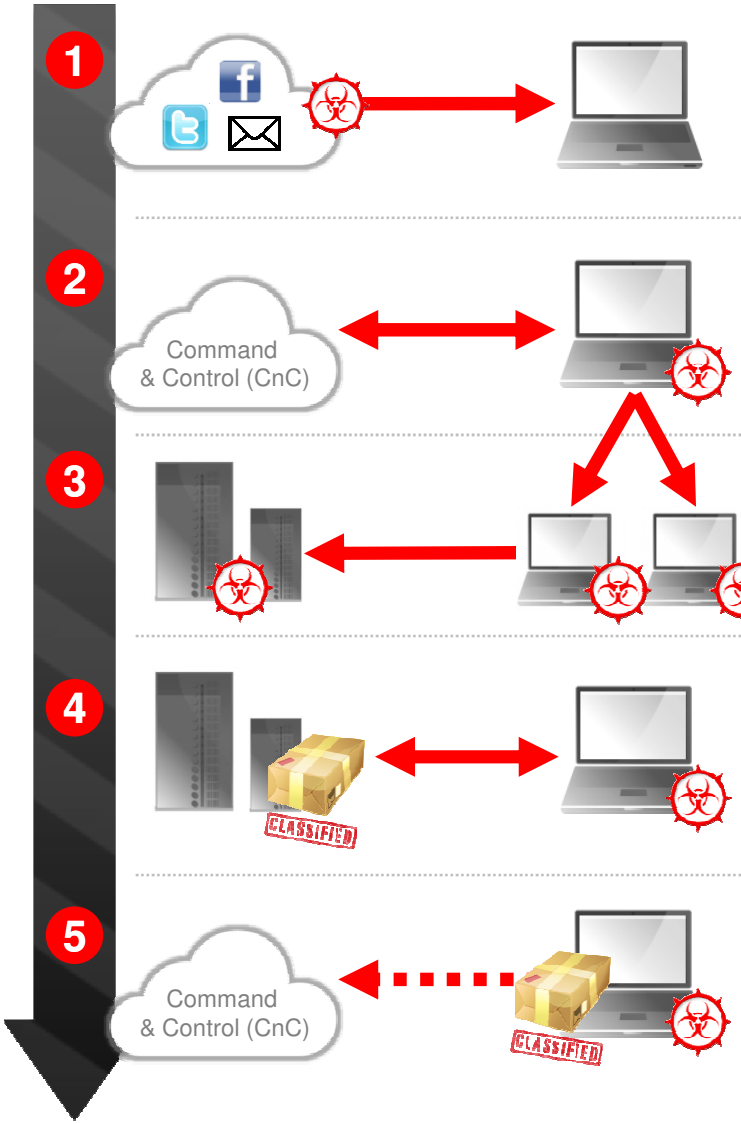
Threat

- Targeted at specific individuals and groups within an organization; aimed at compromising confidential information
- Not random attacks – they are "out to get you"



1) Source: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Attackers follow a 5-Stage attack chain



Break-in

Spear phishing and remote exploits to gain access

Latch-on

Malware and backdoors installed to establish a foothold

Expand

Reconnaissance and lateral movement to increase access and maintain a presence

Gather

Acquisition and aggregation of confidential data

Exfiltrate

Data exfiltration to external networks

Stage 1: Break-in

1 Break-in
2 Latch-on
3 Expand
4 Gather
5 Exfiltrate

Your Challenge

- Employees are always vulnerable to well-executed phishing attempts
- Even patched machines can be compromised by “zero-day attacks” that leverage previously unknown vulnerabilities
- Antivirus has proven to be largely ineffective against zero-day malware

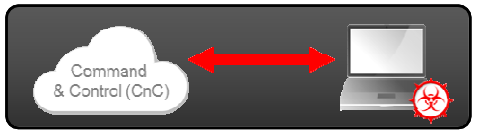
How IBM Can Help

- **IBM Security Network IPS** and **IBM Security Network Protection** help block zero-day exploits using advanced behavioral analysis, and block phishing and malware sites using a database of 13 billion URLs
- **IBM Endpoint Manager** helps limit attack surface by auditing and enforcing compliance with patch and configuration policies

Other Considerations

- Ask your endpoint protection vendor what they provide for advanced detection, and how they detect indicators of compromise
- Consider using a specialized malware detection solution

Stage 2: Latch-on



1 Break-in

2 Latch-on

3 Expand

4 Gather

5 Exfiltrate

Your Challenge

- Once the attacker has breached your perimeter, they need to establish a communication channel back to “home” and create redundant ways to access your network

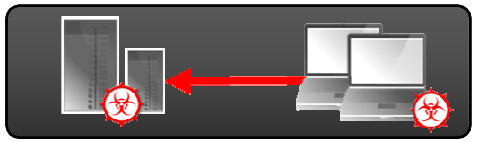
How IBM Can Help

- **IBM Security QRadar** continuously monitors the network and helps identify anomalous activity in terms of location, applications accessed, and more; logs network activity for future forensic investigations, to help determine extent of breach
- **IBM Security Network IPS** uses advanced behavioral analysis to detect subtle communications with malicious destinations

Other Considerations

- Ask your endpoint protection vendor what they are providing for advanced detection, including detecting indicators of compromise

Stage 3: Expand



1 Break-in
2 Latch-on
3 Expand
4 Gather
5 Exfiltrate

Your Challenge

- APTs usually don't infect the host containing target data; thus the attacker needs to find the target data and gain access to it
- They will perform reconnaissance to understand the network and identify high-value assets

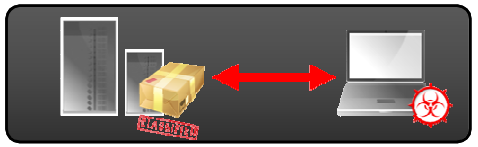
How IBM Can Help

- **IBM Security Privileged Identity Manager** helps lock down user accounts with access to high-value systems and data
- **IBM Security QRadar** uses out-of-the-box analytics to look for suspicious probing across the network – by correlating activity at big data scale
- **IBM Security AppScan** helps reduce the attack surface of enterprise applications by identifying and prioritizing application vulnerabilities

Other Considerations

- Proactively manage your access policies, grant the minimum rights required, and frequently review user access rights

Stage 4: Gather



1 Break-in
2 Latch-on
3 Expand
4 Gather
5 Exfiltrate

Your Challenge

- Once the attacker has compromised your users & gained access to sensitive data repositories, they explore what is available and begin copying target data

How IBM Can Help

- **IBM InfoSphere Guardium** continuously monitors databases and data warehouses to identify suspicious access and protect sensitive data
- **IBM Security Network IPS** helps block malicious behavior within (and beyond) the network
- **IBM Security Network Protection** controls application access at a granular user and application level
- **IBM Security Privileged Identity Manager** helps enforce access policies

Other Considerations

- Place extra controls and focus around your critical assets and data
- Encrypt & protect data in proportion to its value to you and attackers
- Implement an effective DLP (data loss prevention) strategy

Stage 5: Exfiltrate

1 Break-in
2 Latch-on
3 Expand
4 Gather
5 Exfiltrate

Your Challenge

- There are nearly unlimited ways to get acquired data off your network

How IBM Can Help

- **IBM X-Force Threat Intelligence** identifies malicious sites, to help block communications
- **IBM Security QRadar** uses X-Force data to detect traffic to suspect sites; performs activity baselining to help detect anomalous user behavior based on type of activity, volume of data transfers, time of day, location, etc.
- **IBM Security Network IPS** helps stop encrypted traffic associated with suspicious entities, and sensitive data transmission (eg, credit card numbers)
- **IBM Security Network Protection** tracks and controls application usage in all directions to enforce policies and help prevent data loss

Other Considerations

- Push your Endpoint Protection, Network DLP and Network Security vendors to enhance their detection and blocking of suspicious data transmission

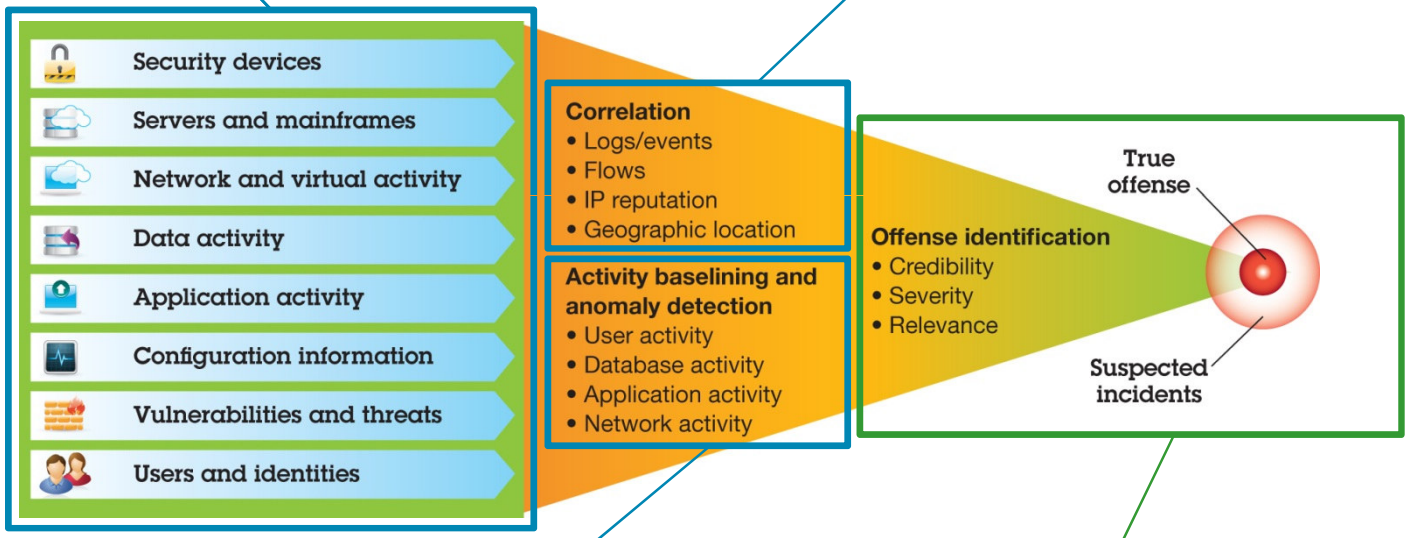
Leverage advanced analytics across all stages of the attack

Monitor everything

Logs, network traffic, user activity

Correlate intelligently

Connect the dots of disparate activity



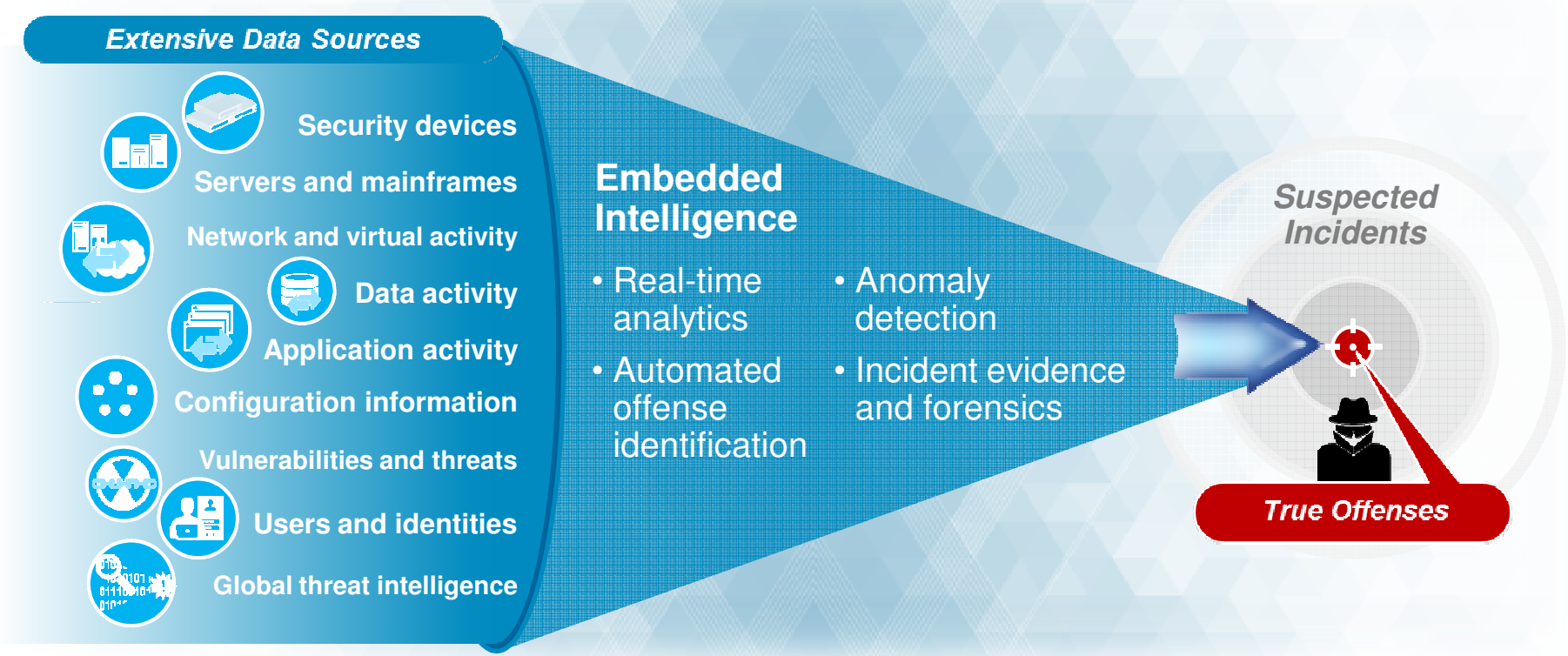
Detect anomalies

Unusual yet hidden behavior

Prioritize for action

Attack high-priority incidents

Use intelligence and anomaly detection across every domain



Gain insights to prioritize what is most critical

2 Billion logs and events per day

25 high priority offenses

QRadar Security Intelligence Platform

Source: IBM client example