Agenda

- **10:40 - 11:20 Before the attack: defend under the assumption of compromise**
  Micheal Hamelin, Lead X-Force Security Architect

- **11:20 - 11:45 During an attack: Intelligent detection and optimized response**

  Vijay Dheap, IBM Master Inventor

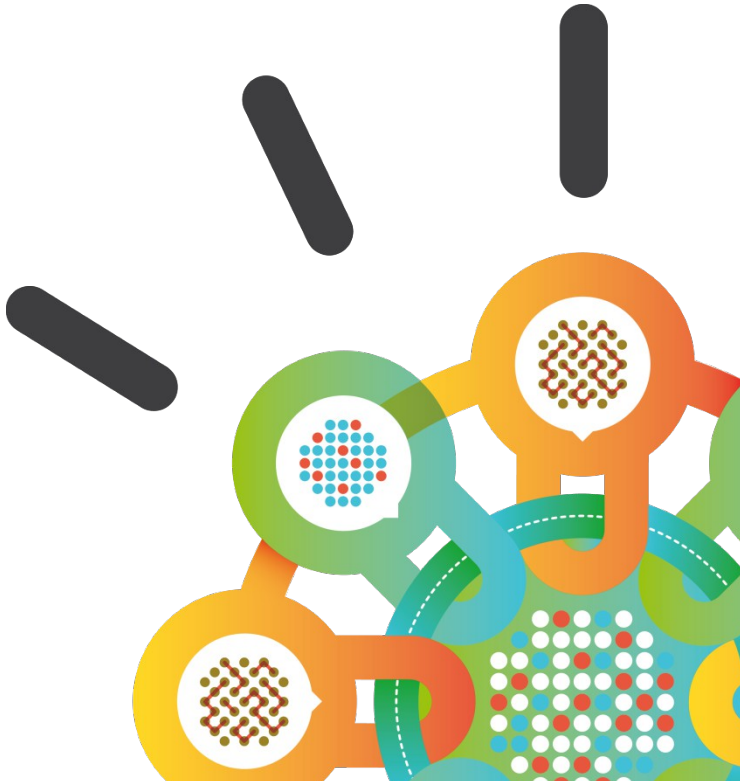
- **11:45 - 12:15 Demo**
  Vaughan Harper, Security Specialist

- **12:15 Closing remarks**

Security Intelligence.
Think Integrated.

Focused Defense Under the Assumption of Compromise

- Michael P. Hamelin
  Lead X-Force Security Architect
- IBM Security Systems



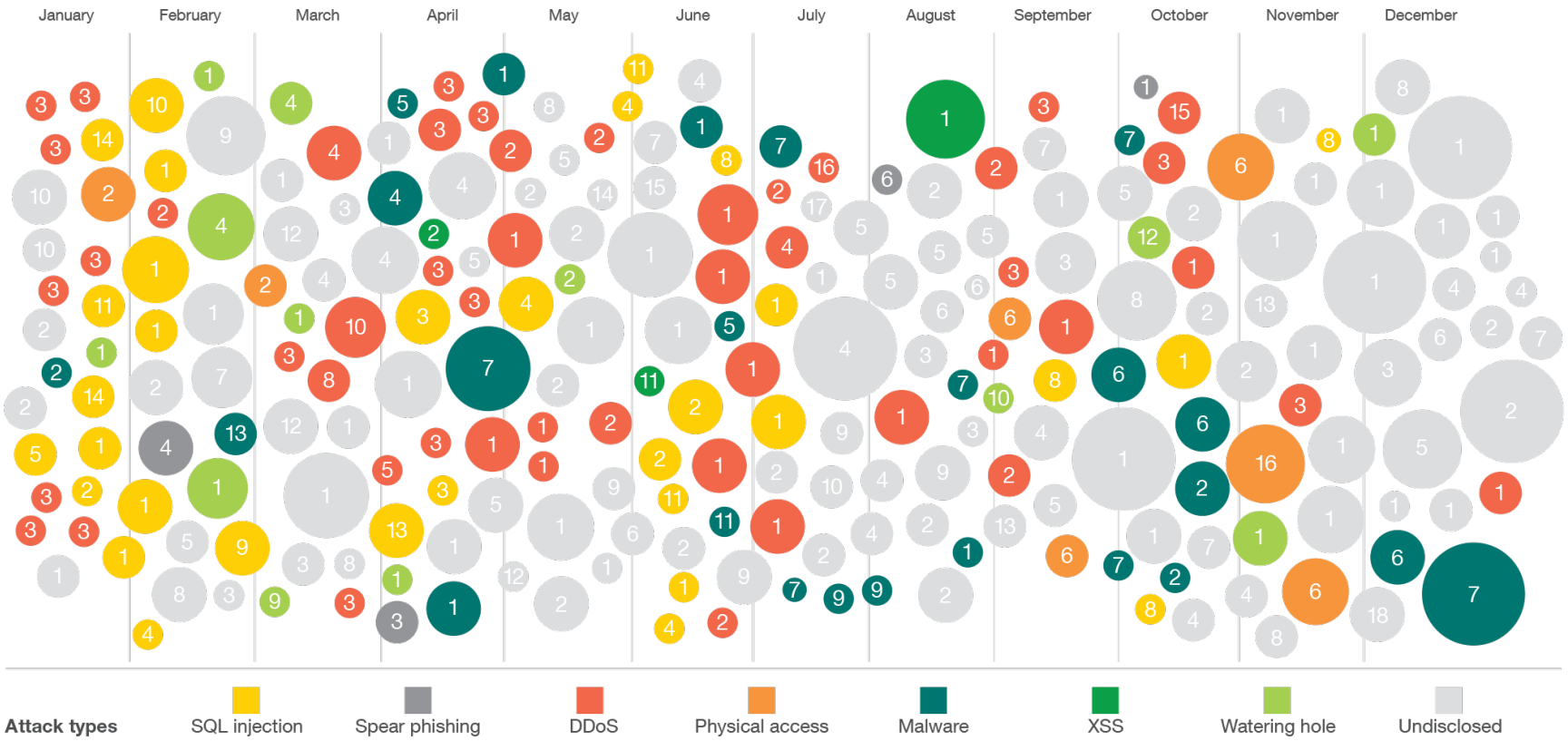
Agenda

- The Perimeter is Gone: Assuming Compromise
- Shrinking the Attack Surface: Vulnerability Management
- Intrusion Prevention and the First Line of Defense
- Deeper Protection: Breaking the Attack Chain
- Questions and Answers

Despite Extensive Effort and Investment…

Sampling of 2013 security incidents by attack type, time and impact

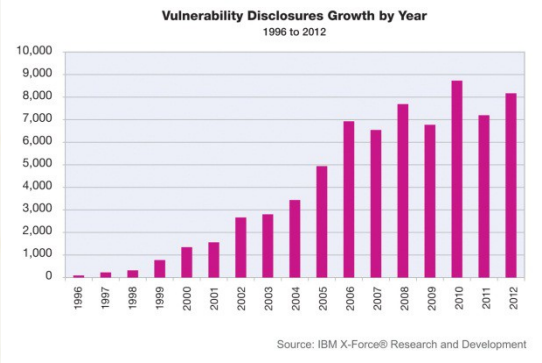
conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses



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

Increasing Attack Surface and Threat Sophistication

Increasing Number of Vulnerabilities



- Vulnerabilities increasing
- Overall attack surface is growing
- Patches cannot be instantly implemented or don't exist

0-Day Attacks and Constantly Mutating Threats

- Attacks constantly mutating to evade signatures
- Increasing number of 0-day exploits

Multi-facted Threats and APTs

- Well coordinated attacks by well coordinated teams
- Attackers exploiting users to gain access
- Traditional security tools unable to detect or assess the extent of the breach

The Expansion of Targeted Attacks

Off-the-Shelf tools and techniques

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

Sophisticated

- 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

Source: IBM X-Force® Research and Development

What's Needed in 2014?

- **Current challenges**
  - Traditional tools and approaches are failing to do sophisticated attackers and threats
  - Security tools and technologies continue to be in siloes and poorly integrated
  - Unable to understand security posture and respond to security incidents rapidly

- **3 critical things to do in 2014**
  - Minimize attack surface as much as possible
  - Stop attacks in real-time including 0-days and advanced malware
  - Disrupt the lifecycle of the attack even if initially compromised

Threats Need to be Addressed Before, During and Post-Exploit

What are the external and internal threats?

Are we configured to protect against these threats?

What is happening right now?

What was the impact?

Vulnerability

Pre-Exploit

Exploit

Post-Exploit

Remediation

PREDICTION / PREVENTION PHASE

- Gain visibility over the organization's security posture and identity security gaps
- Detect deviations from the norm that indicate early warnings of APTs
- Prioritize vulnerabilities to optimize remediation processes and close critical exposures before exploit

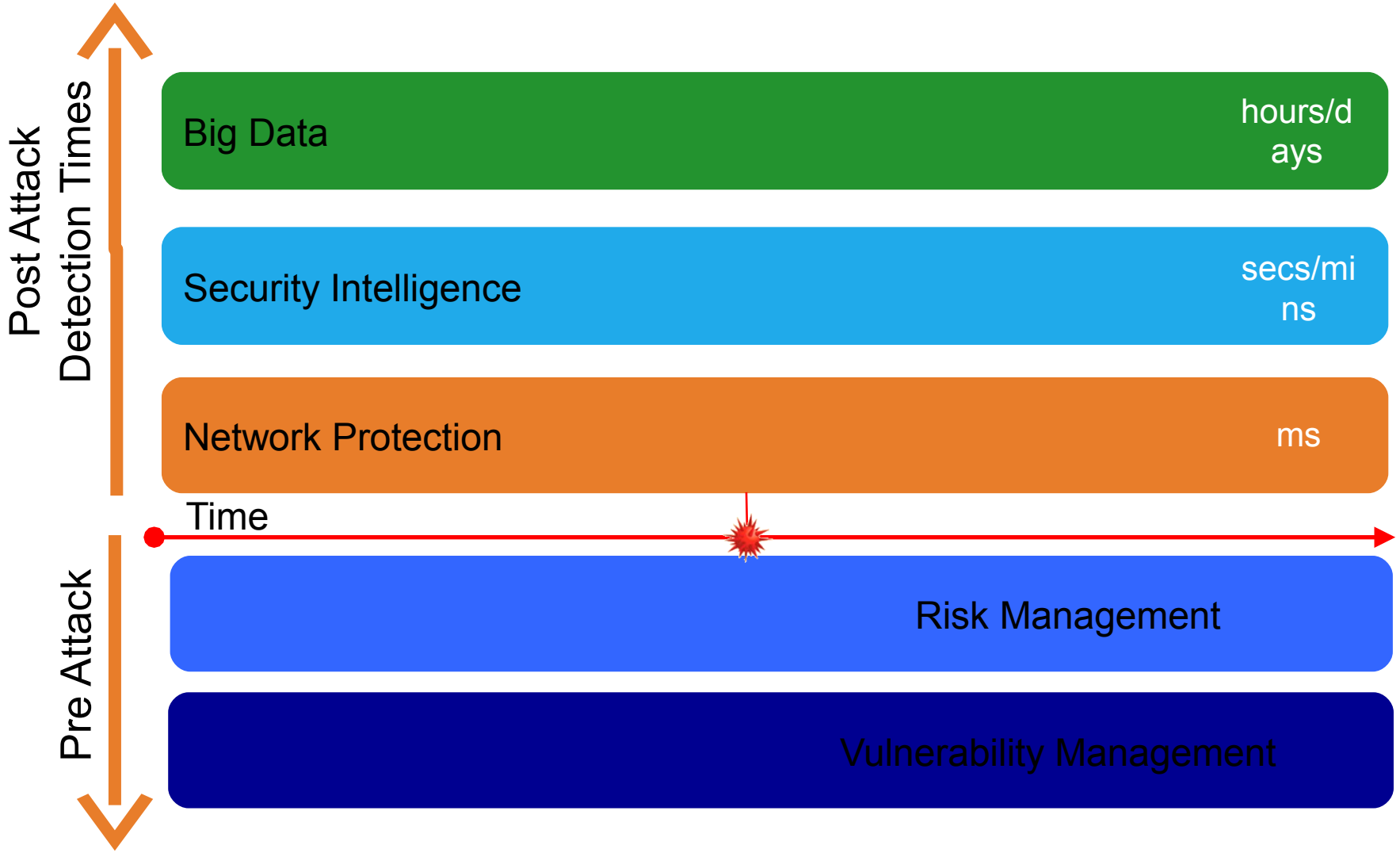
REACTION / REMEDIATION PHASE

- Automatically detect threats with prioritized workflow to quickly analyze impact
- Gather full situational awareness through advanced security analytics
- Leverage results to drive proactive remediation

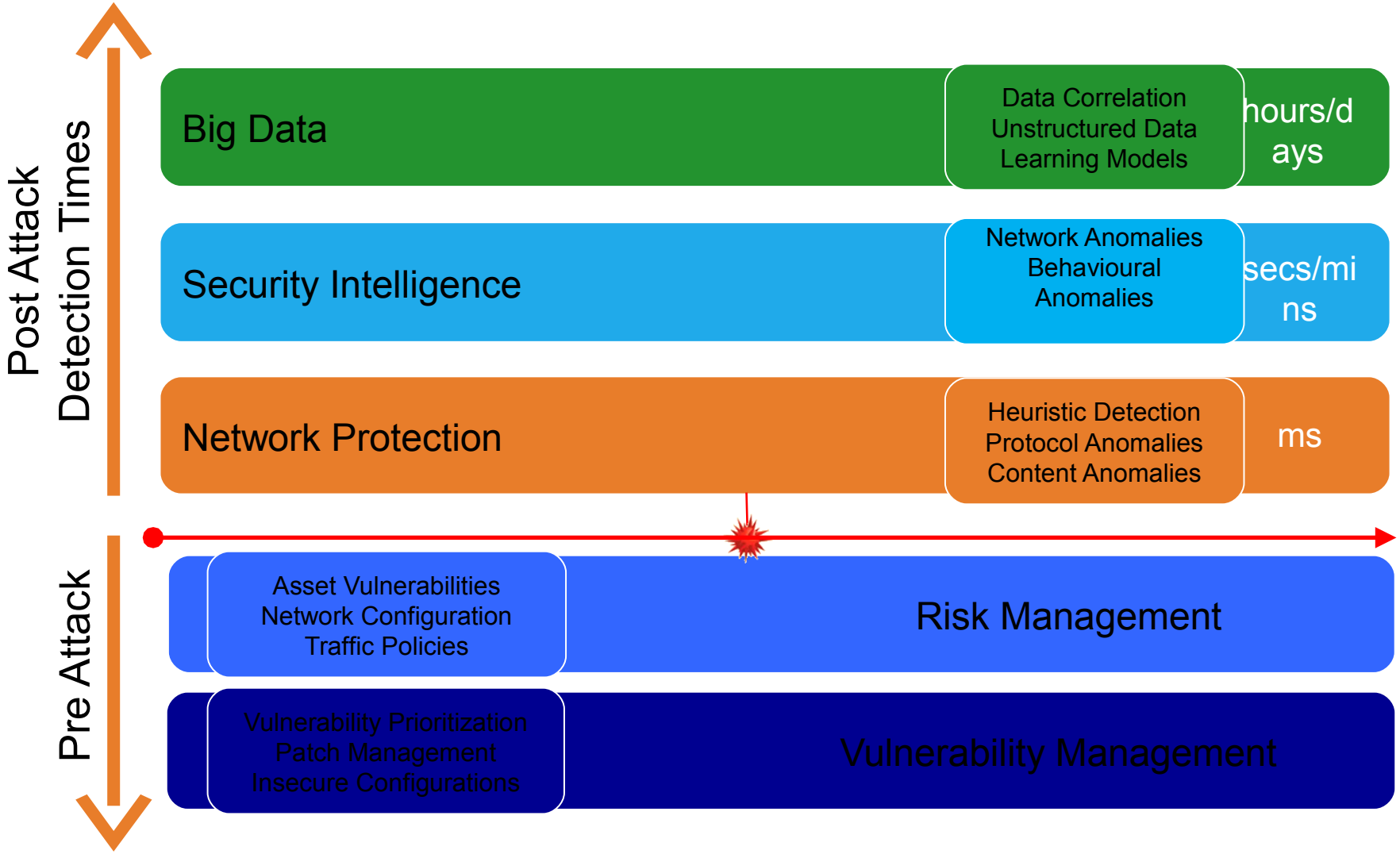
Security Intelligence

The actionable information derived from the analysis of security-relevant data available to an organization

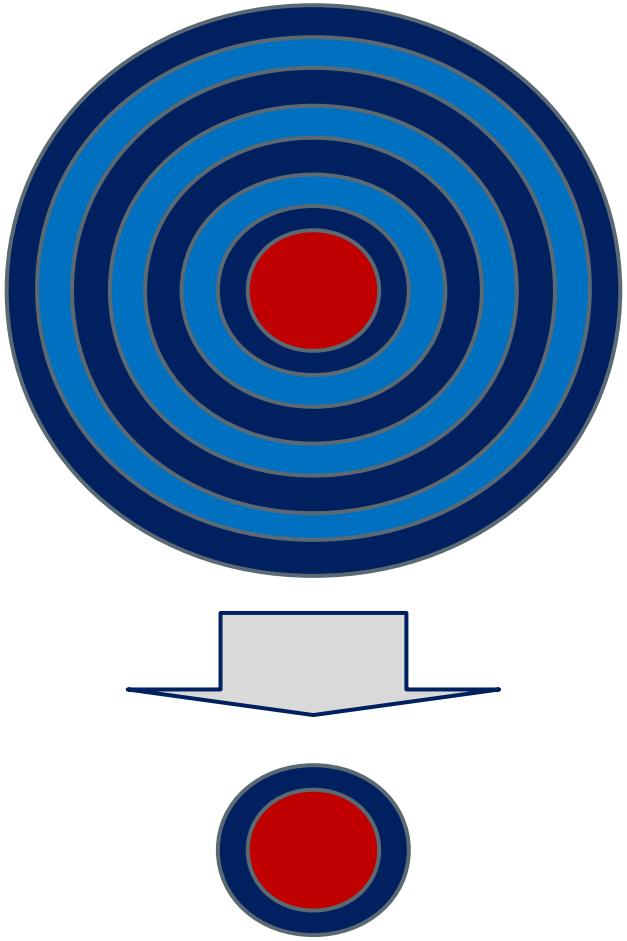
The Need for Detection and Prevention Across the Exploit Lifecycle



The Need for Detection and Prevention Across the Exploit Lifecycle



Pre-Exploit Vulnerability Management to Shrink the Attack Surface



From thousands of vulnerabilities and possible attack vectors…

To a handful of vulnerabilities and possible attack vectors

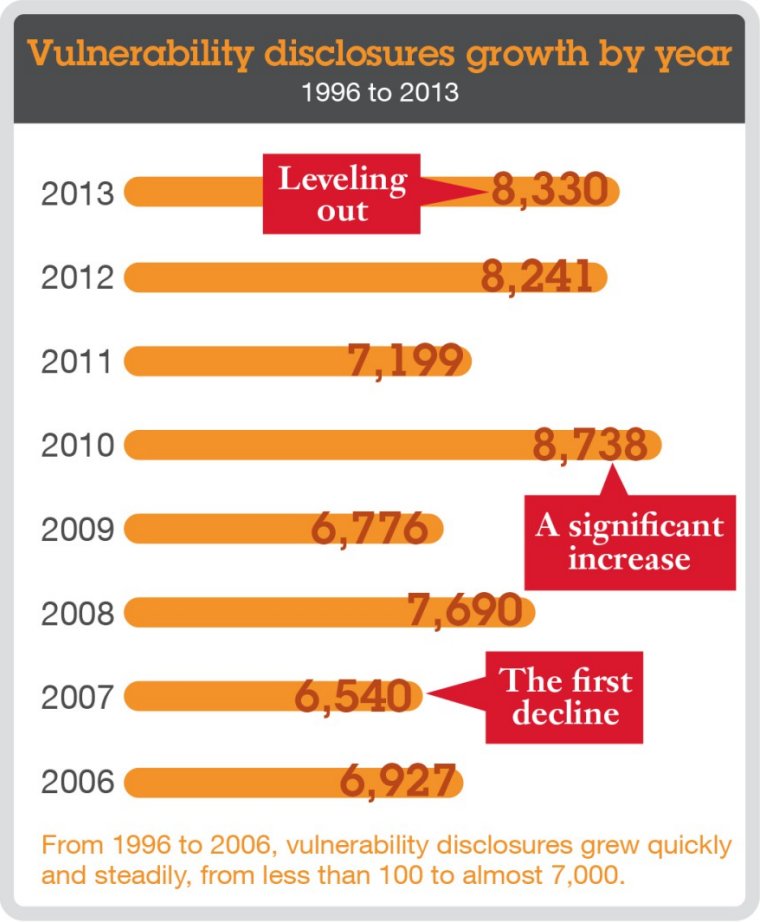


Figure 8. Vulnerability disclosures growth by year, 1996 to 2013

Source: IBM X-Force® Research and Development

AppScan: Focusing on Web App Vulnerabilities Through Automated Scanning

Application Security Management

- Inventory assets
- Assess business impact
- Prioritize vulnerabilities
- Measure status & progress
- Determine compliance

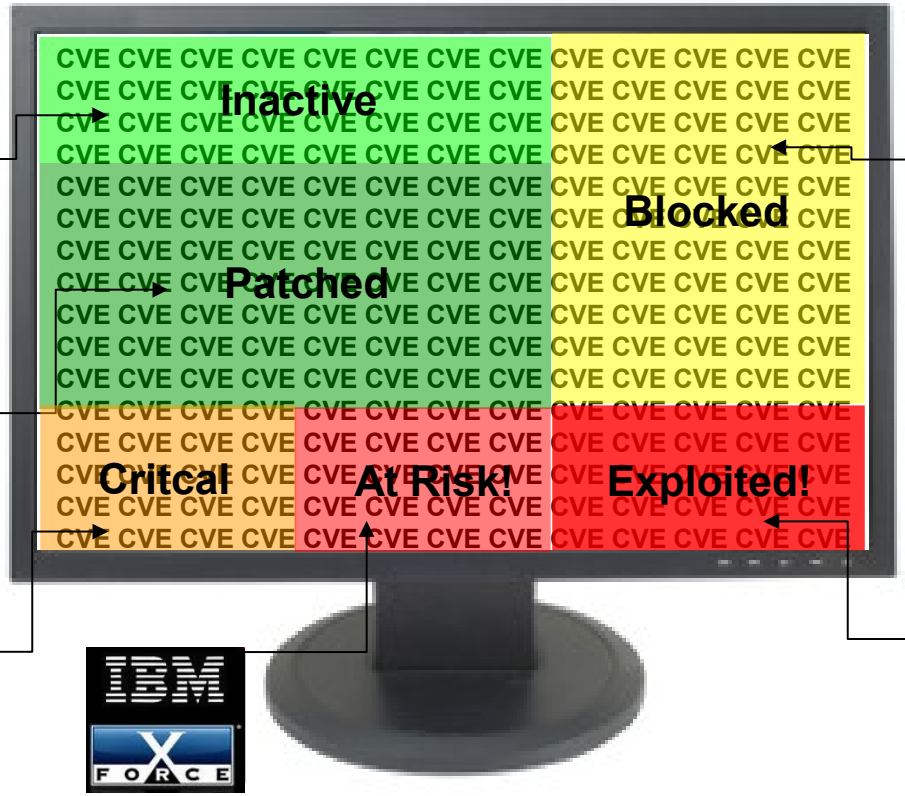
- Dynamic Analysis
- Static Analysis
- Interactive Analysis
- Mobile Application Analysis

QRadar Vulnerability Manager to Bring it All Together

Inactive: Flow analysis senses application activity for prioritization of vulnerabilities

Patched: Endpoint management identifies which vulnerabilities will be patched

Critical: Vulnerability knowledge base, remediation flow and risk management policies inform about business critical vulnerabilities



At Risk: X-Force Threat and SIEM security incident data, coupled with visibility to network flows, help identify which assets are communicating with potential threats

Blocked: Risk Management supports identification of vulnerabilities that are blocked by firewalls and IPSs

Exploited: SIEM correlation and IPS data help vulnerability management reveal which vulnerabilities have been exploited

One Quarter of All Vulnerabilities Still Lack a Vendor Patch

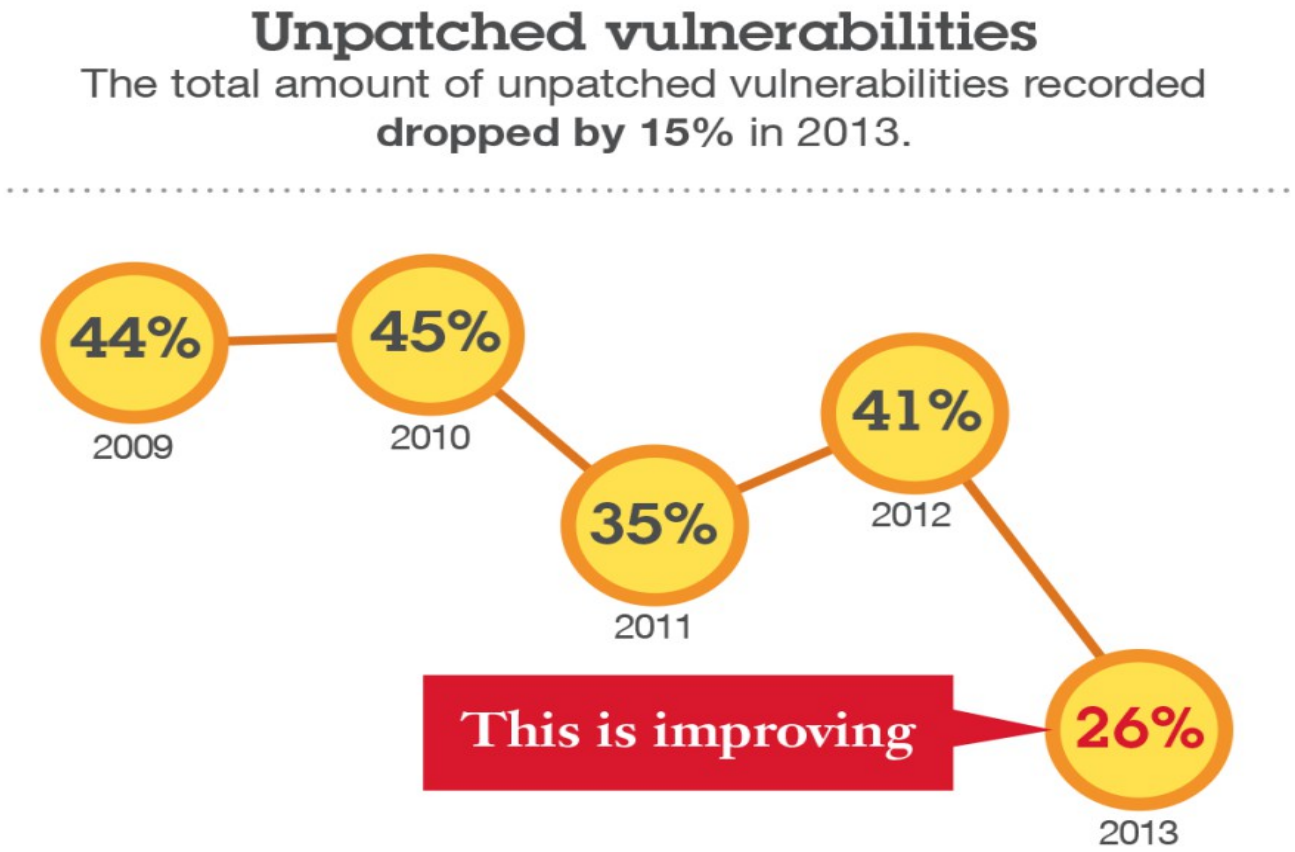
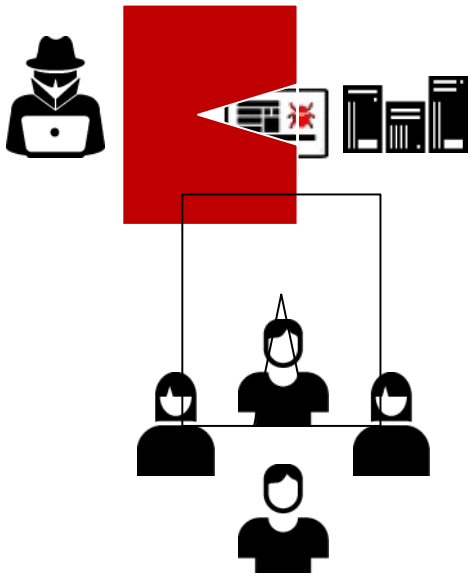


Figure 10. Vendor patch rates of publicly disclosed vulnerabilities, 2009 to 2013

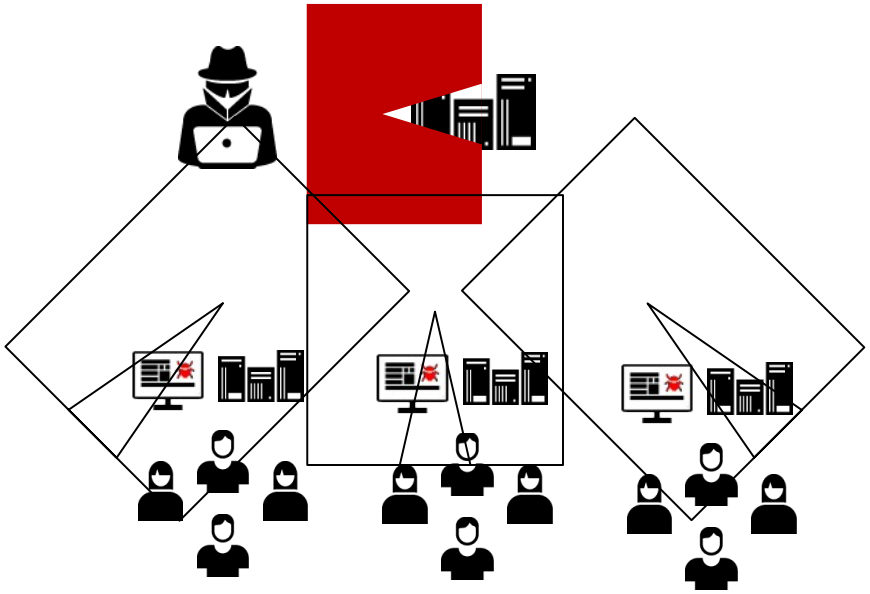
Source: IBM X-Force® Research and Development

Attackers are Finding New Ways to Target Users



Watering Hole

- Attacker injects malware on special interest website
- Vulnerable niche users exploited



Malvertising

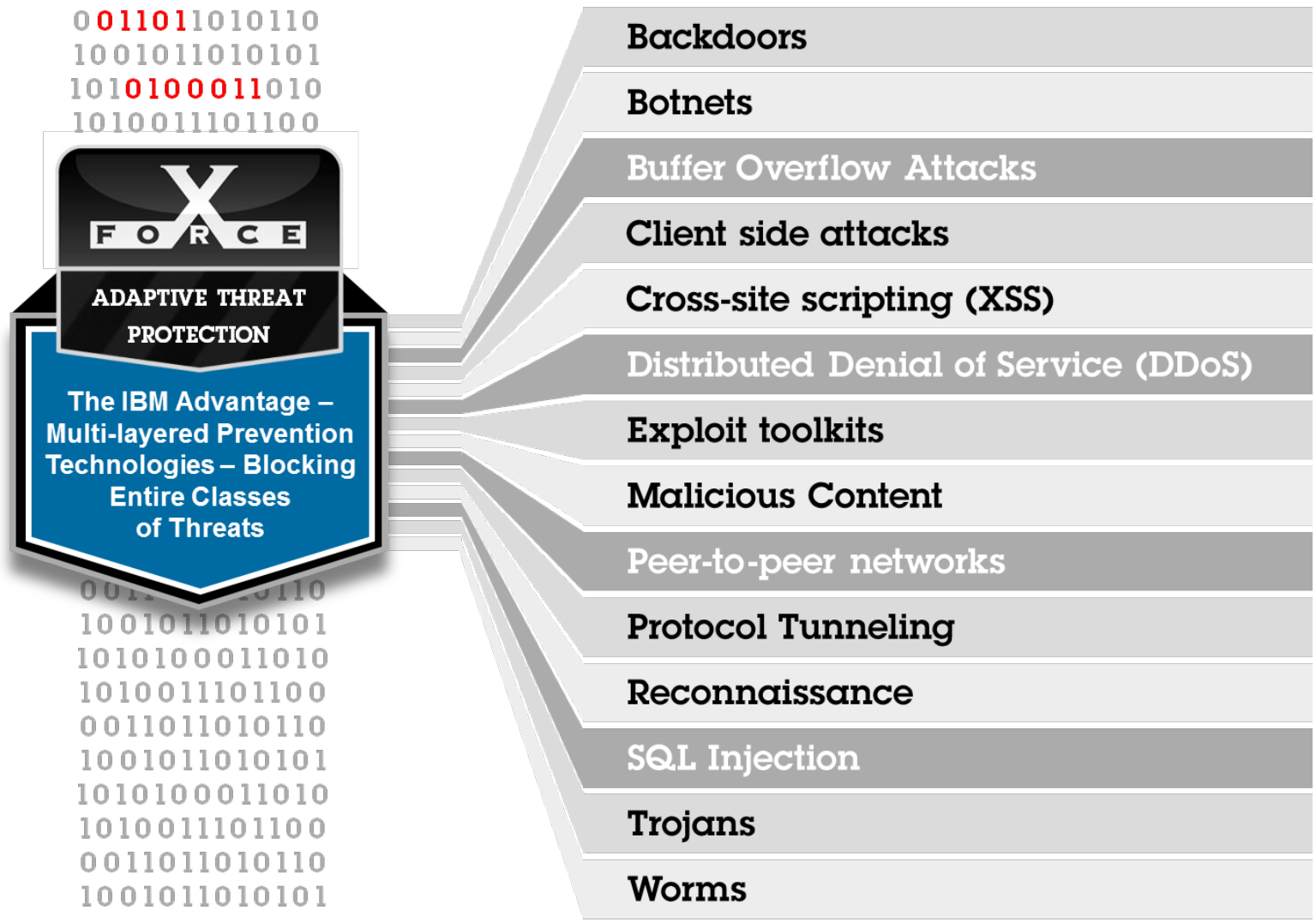
- Attacker injects malware on ad network
- Malicious ad embedded on legitimate websites
- Vulnerable users exploited

IBM Security Network Protection

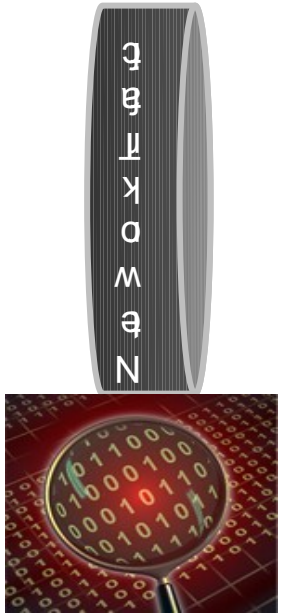
Block mutated threats, prevent malware infections at the point of exploit

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

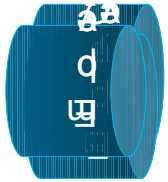
Blocking Emerging Threats in Real-time – Powered by X-Force



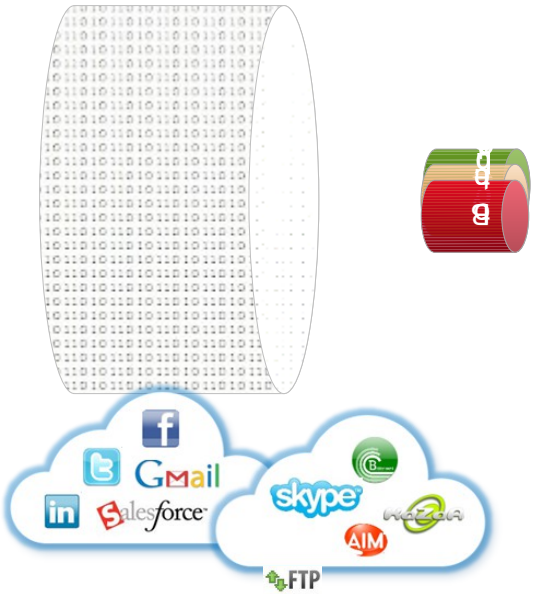
Network Visibility: Understanding What's Happening on the Network



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

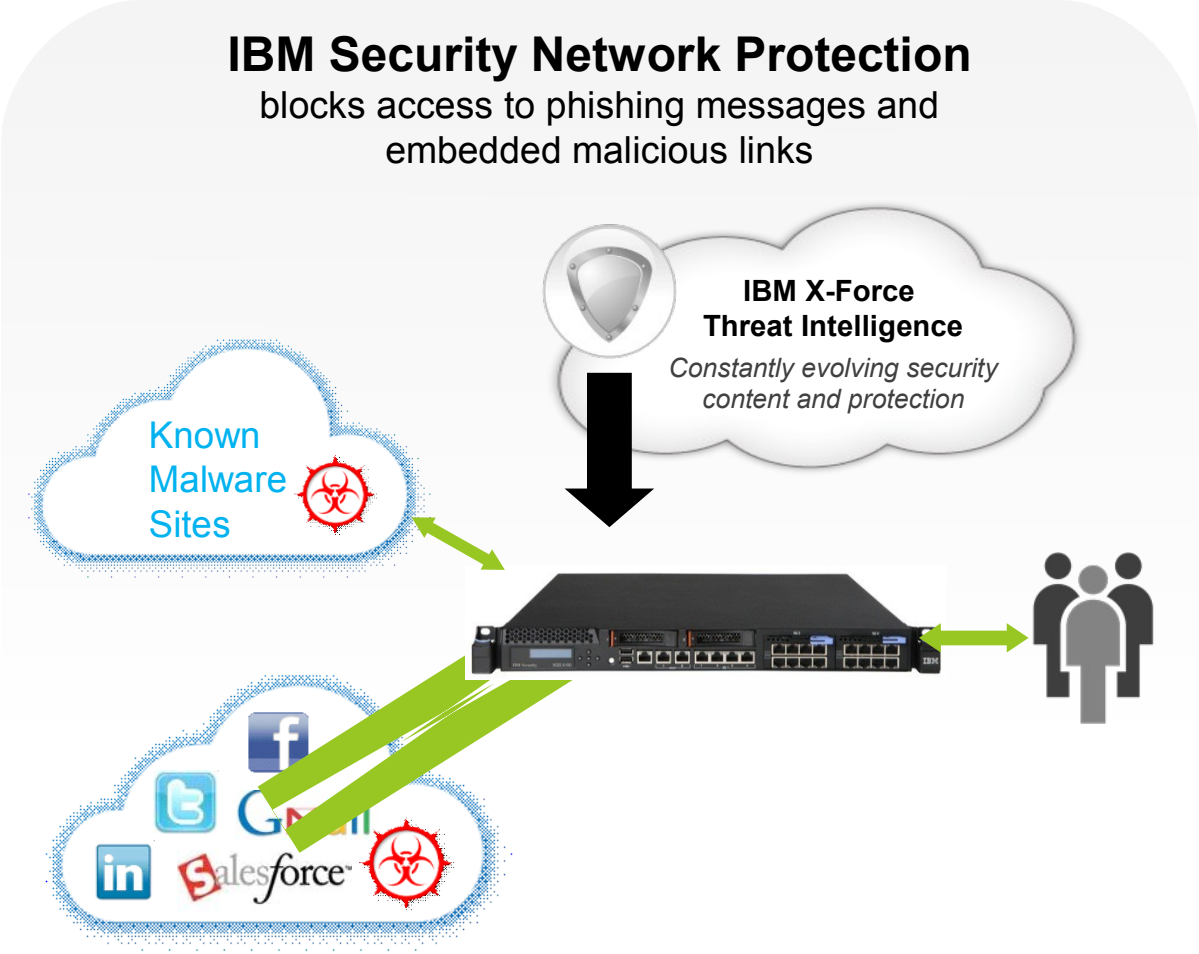


Access Control Policies block pre-existing compromises and rogue applications as well as enforce corporate usage policies

400+	2,000+	20 Billion+
Protocols and File Formats Analyzed	Applications and Actions Identified	URLs classified in 70 Categories

Applying Visibility and Control to Break the Attack Chain

A look at social media and spear phishing



How XGS Can Help

- Ability to granularly control which social media sites are accessed from the network
- Dynamic blocking of users attempting to access known malware sites
- Dual-layer approach to phishing by limiting the access to phishing messages, as well as blocking access to malicious links
- Also able to block command and control traffic from existing infections

Trusteer Apex: Preventing Malware on the Endpoint

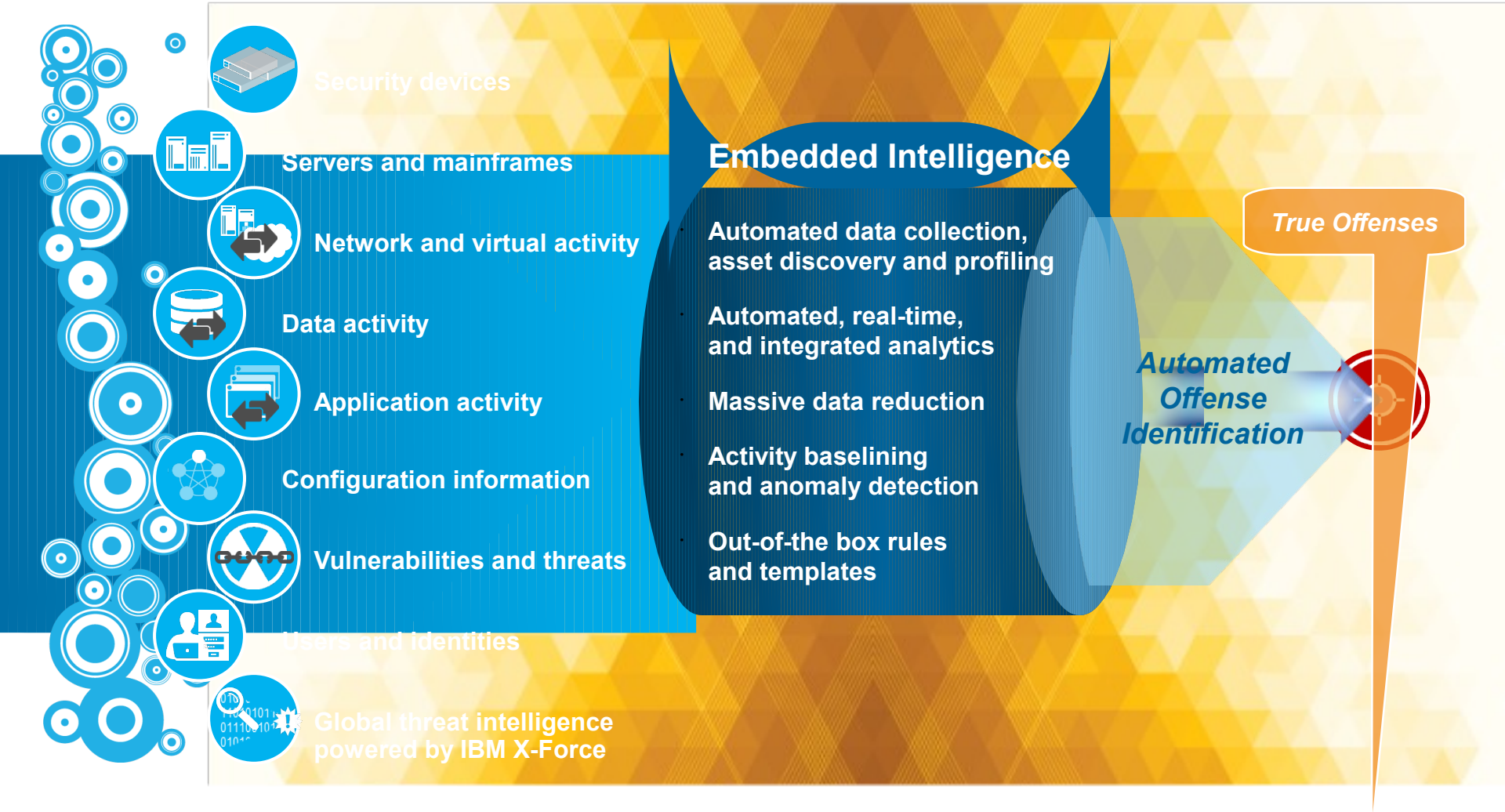
Company	Global leader in Advanced Threat Protection
Intelligence	Analysis of events from millions of protected endpoints
Technology	Stateful Application Control

Stopping advanced malware and APTs by preventing malicious downloads and data exfiltration

Breaking the Attack Chain Post-Exploit

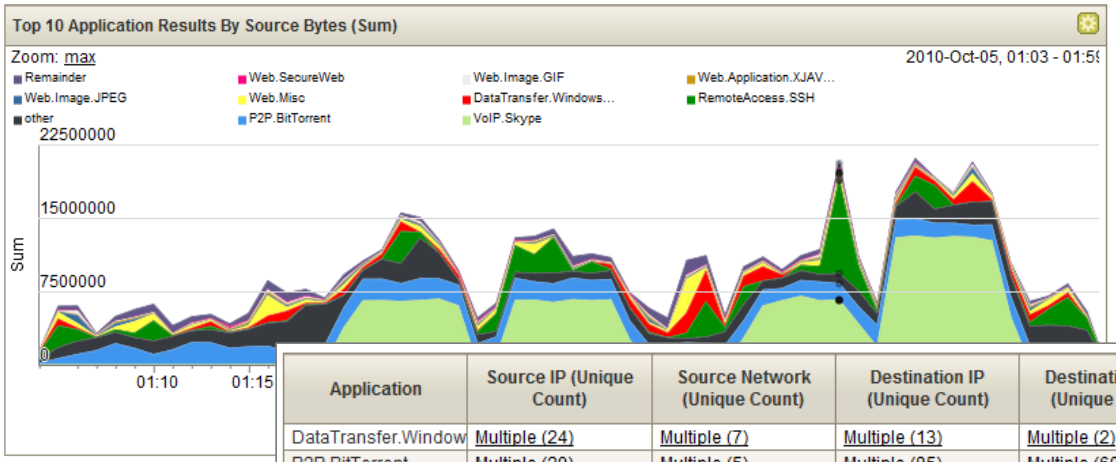
Extensive Data Sources

…Suspected Incidents



“Slow and Low” Threats and the Role of Network Flow Analytics

- Network traffic doesn’t lie. Attackers can stop logging and erase their tracks, but can’t cut off the network (flow data)
  - Deep packet inspection for Layer 7 flow data
  - Pivoting, drill-down and data mining on flow sources for advanced detection and forensics



Application	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)
DataTransfer.Window	Multiple (24)	Multiple (7)	Multiple (13)	Multiple (2)	Multiple (7)	16 319 315	531 531 708
P2P.BitTorrent	Multiple (20)	Multiple (5)	Multiple (85)	Multiple (60)	Multiple (3)	44 216 868	191 621 654
other	Multiple (259)	Multiple (9)	Multiple (3 063)	Multiple (2 877)	Multiple (10)	37 349 699	168 802 101
VoIP.Skype	Multiple (5)	Multiple (4)	Multiple (40)	Multiple (40)	other	131 172 458	46 819 290
RemoteAccess.SSH	Multiple (10)	Multiple (5)	Multiple (7)	22	Multiple (4)	37 885 116	111 228 020
Web.Misc	Multiple (16)	Multiple (5)	Multiple (295)	80	other	10 726 080	20 635 741
Web.Application.Misc	Multiple (9)	Multiple (4)	Multiple (31)	80	other	654 743	23 125 267

Providing visibility into attacker communications to detect anomalies that might otherwise get missed

Anomaly Detection

- Flexible anomaly detection capabilities identify meaningful discrepancies by rule, threshold, or deviation from normal range

Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply Anomaly: Remote Inbound Communication from a Foreign Country on flows which are detected by the Local system
and when a flow matches any of the following BB:CategoryDefinition: Countries with no Remote Access
and when the flow context is Remote to Local
and when a flow matches any of the following BB:CategoryDefinition: Successful Communication
and NOT when the source or destination port is any of 53, 25

Notes (Enter your notes about this rule)

Reports traffic from an IP address known to be in a country that does not have remote access right. Before you enable this rule, we recommend that you configure the BB:CategoryDefinition: Countries with no Remote Access building block. SMTP and DNS have been removed from this test as you have little control over that activity. You may also have to remove WebServers in

Reports traffic from an IP address known to be in a country that does not have remote access right.

"Information security is becoming a big data and analytics problem. ...Some of the most sophisticated attacks can only be found with detailed activity monitoring to determine meaningful deviations from 'normal' behavior."

Neil MacDonald, Gartner, June 2012

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security