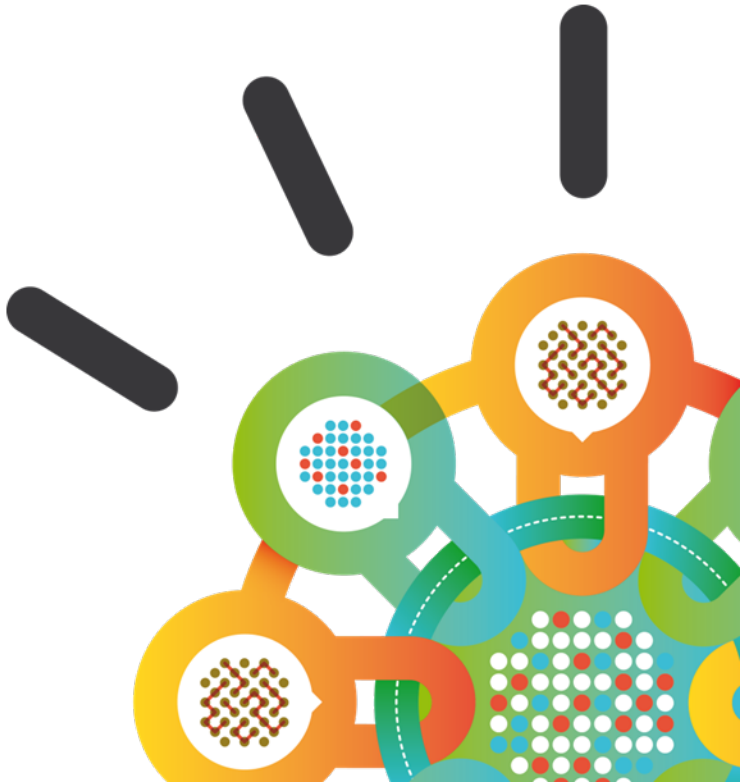
Security Intelligence.
Think Integrated.

IBM Security
Átfogó megoldások a komplex támadások ellen

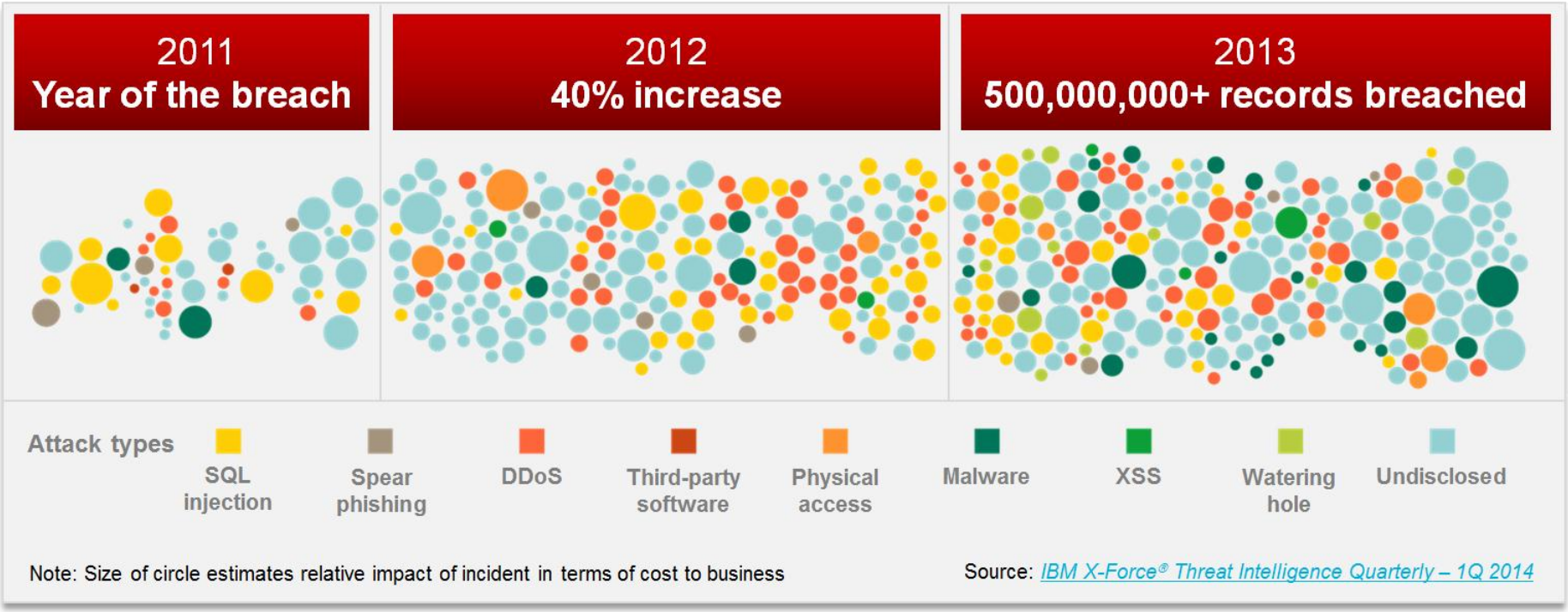
Csendes Balázs
Security Intelligence Leader, CEE
IBM

Tel: +36 (20) 492 3202
E-mail: balazs.csendes@cz.ibm.com

March 17, 2015



Sophisticated attackers break through safeguards every day



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

Source: *IBM X-Force® Threat Intelligence Quarterly – 1Q 2014*

61% of organizations say **data theft and cybercrime** are their greatest threats

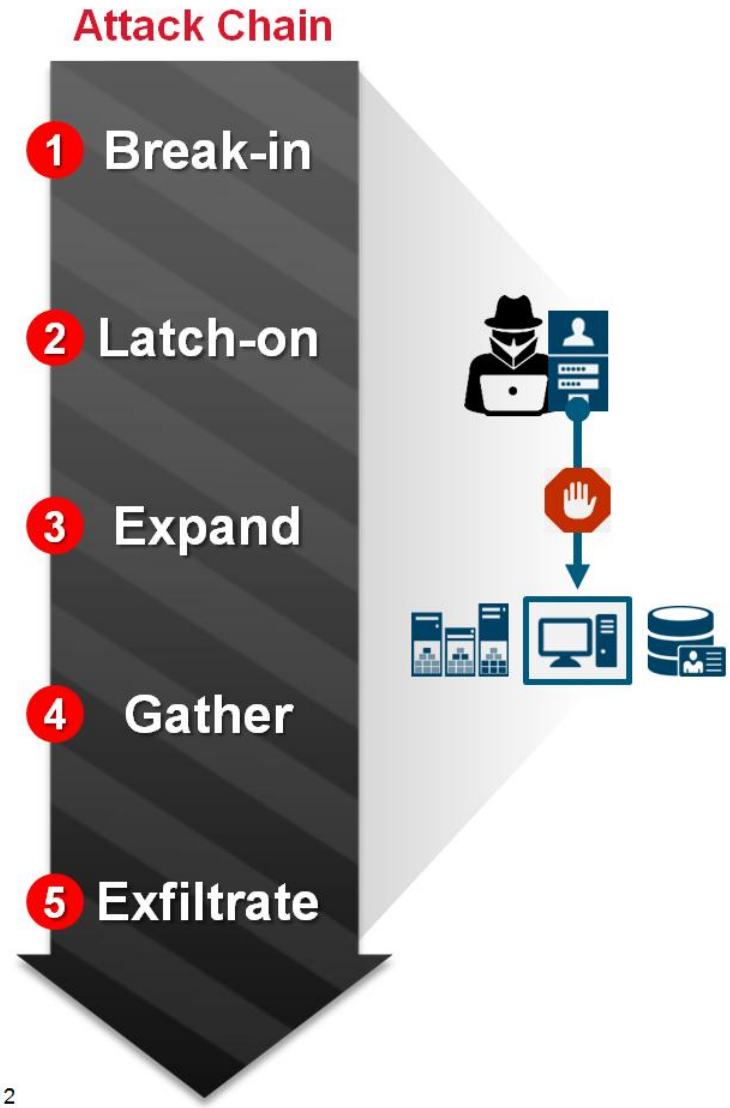
2012 IBM Global Reputational Risk & IT Study

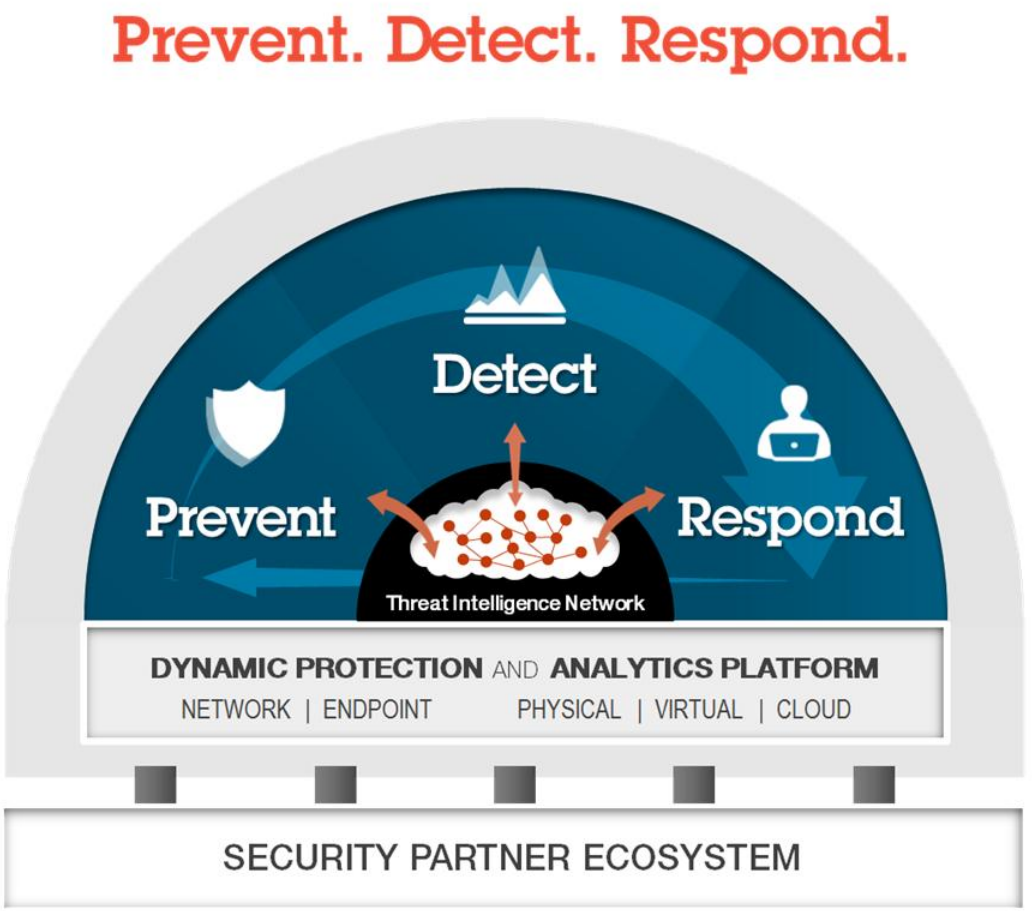
$3.5M+ average cost of a **data breach**

2014 Cost of Data Breach, Ponemon Institute

Introducing the IBM Threat Protection System

IBM delivers a dynamic, integrated system to disrupt the lifecycle of advanced threats





Focus on critical points in the attack chain with preemptive defenses on both the endpoint and network

	Exploit Disruption	Malware Quarantine	User Protection
ENDPOINT	**Prevent malware installs** • Verify the state of applications • Block exploit attempts used to deliver malware	**Prevent control channels** • Stop direct outbound malware communications • Protect against process hijacking	**Prevent credential loss** • Block keyloggers • Stop credential use on phishing sites • Limit reuse of passwords
NETWORK	**Prevent mutated exploits** • Verify the state of network protocols • Block unknown exploits with behavioral heuristics	**Prevent active beaconing** • Stop malware and botnet control traffic with real-time reputation and SSL inspection	**Prevent malicious apps** • Block access to malicious websites • Protect against web application misuse

On the Endpoint
Trusteer Apex Malware Protection

On the Network
IBM Security Network Protection XGS

Continuously monitor security-relevant activity from across the entire organization

Pre-Attack Analytics

Predict and prioritize security weaknesses before adversaries

- Use automated vulnerability scans and rich security context
- Emphasize high-priority, unpatched, or defenseless assets requiring attention

IBM Security QRadar Security Intelligence Platform

Real-time Attack Analytics

Detect activity and anomalies outside normal behavior

- Correlate and baseline massive sets of data
- From logs, events, flows, user activity, assets, locations, vulnerabilities, external threats, and more

IBM Security QRadar Vulnerability Manager

IBM Security QRadar SIEM

Rapidly investigate breaches, retrace activity, and learn from findings to remediate weaknesses

Post-Attack Incident Forensics

Reduce the time to fully discover what happened and when it occurred

- Index and reconstruct attack activity and content from full-packet network data
- Apply search engine technology and advanced visualizations

IBM Security QRadar Incident Forensics

Rapid Response Integrations

Quickly expand security coverage to prevent further harm

- Share indicators across control points
- Dynamically apply customized rules

IBM Security Capability Integrations

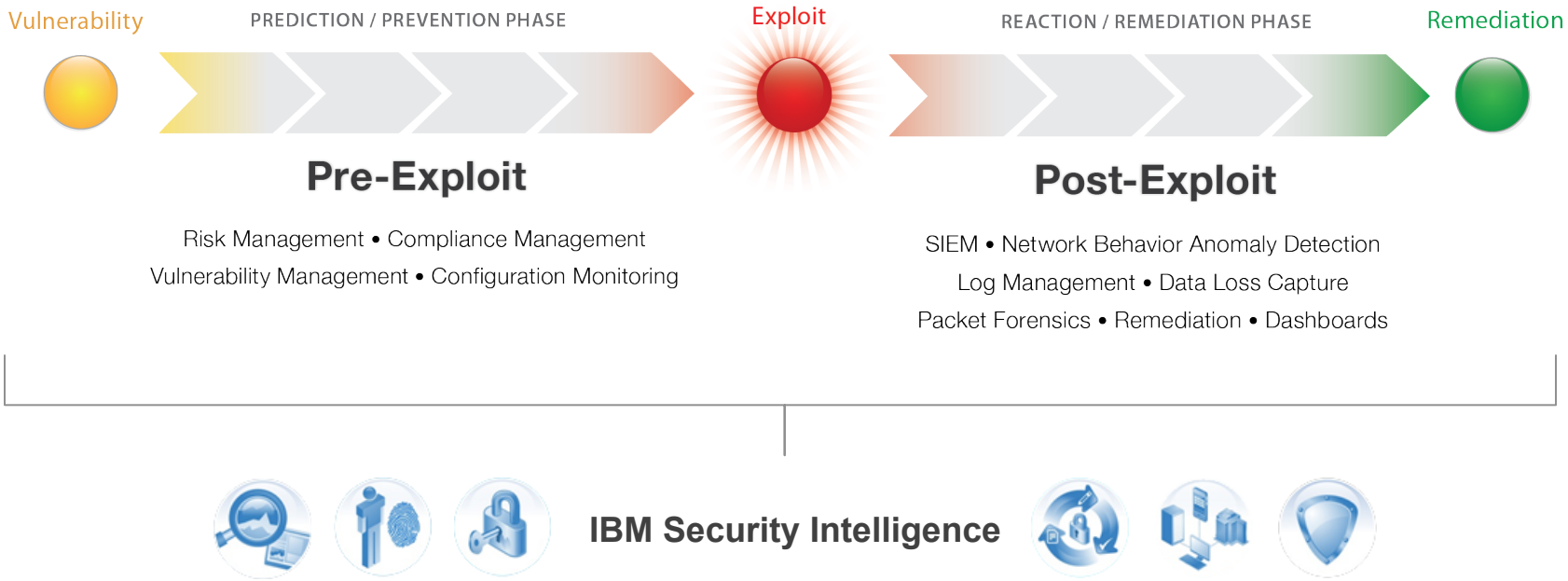
Emergency Response Services

Help prepare for and withstand security breaches more effectively

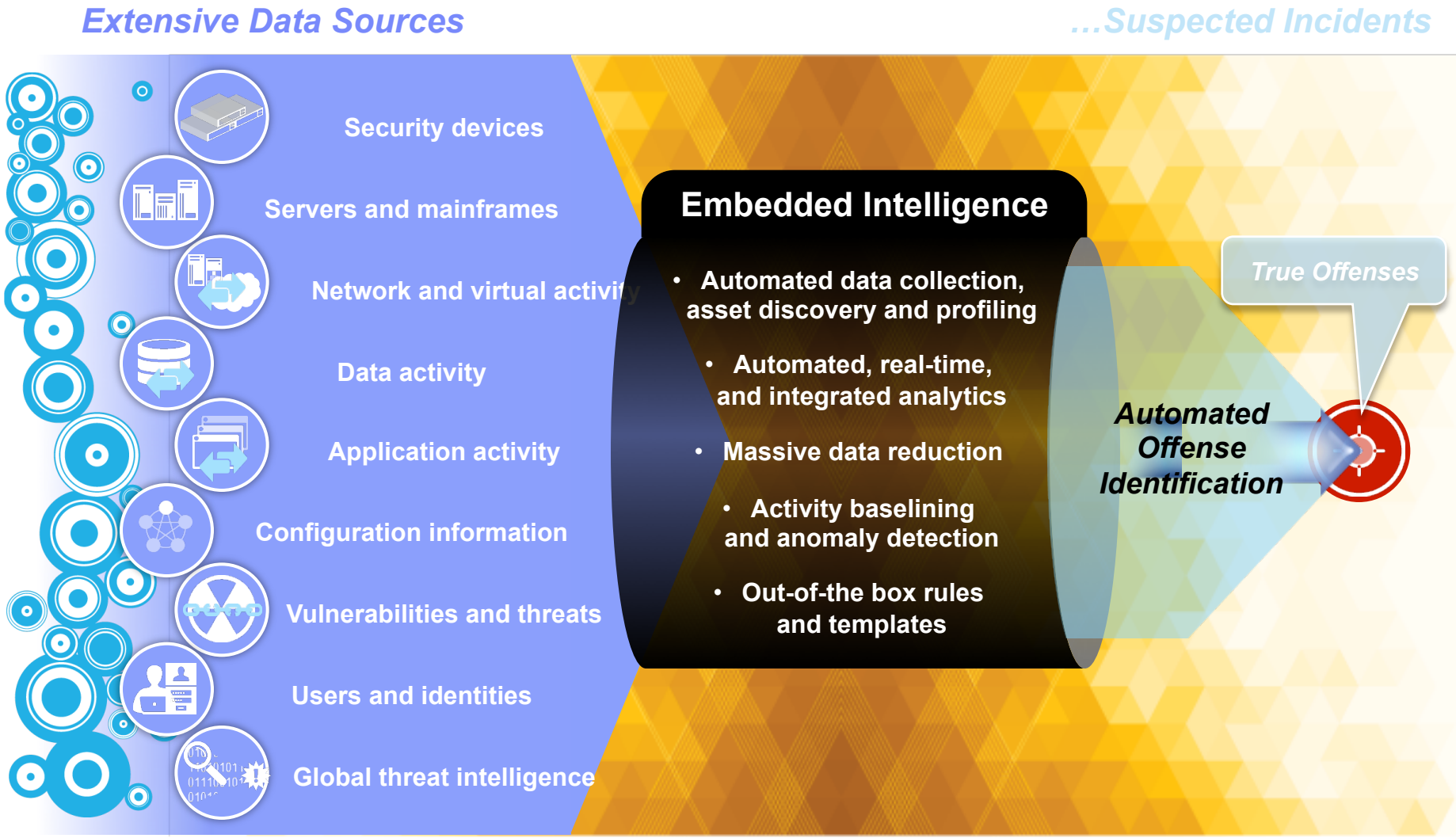
- Gain access to key resources that can enable faster recovery and help reduce incident business impact

IBM Emergency Response Services

The Security Intelligence Life Cycle: Boundaries of QRadar Roadmap



QRadar delivers embedded intelligence to find true offenses



QRadar Product Portfolio

Area of Focus

Security Intelligence platform that enables security optimization through advanced threat detection, meet compliance and policy demands and eliminating data silos

Portfolio Overview

QRadar Log Manager
- Turnkey log management for SMB and Enterprises
- Upgradeable to enterprise SIEM

QRadar SIEM
- Integrated log, flow, threat, compliance mgmt
- Asset profiling and flow analytics
- Offense management and workflow

Network Activity Collectors (QFlow)
- Network analytics, behavior and anomaly detection
- Layer 7 application monitoring

QRadar Risk Manager
- Predictive threat modeling & simulation
- Scalable configuration monitoring and audit
- Advanced threat and impact analysis

QRadar Vulnerability Manager
- Integrated Network Scanning & Workflow
- Leverage SIEM, Threat, Risk to prioritize vulnerabilities

QRadar Incident Forensics
- Reconstruct raw network packets to original format
- Determine root cause of security incidents and help prevent recurrences

A Real World Example

About Target Corporation

- Target Corporation is an American retailing company, founded in 1902 and headquartered in Minneapolis, Minnesota. It is the second-largest discount retailer in the United States, Walmart being the largest. The company is ranked 36th on the Fortune 500 as of 2013 and is a component of the Standard & Poor's 500 index. Its bullseye trademark is licensed to Wesfarmers, owners of the separate Target Australia chain, which is unrelated to Target Corporation.

- The first Target store was opened in 1962 in Roseville, Minnesota. Target grew and eventually became the largest division of Dayton Hudson Corporation, culminating in the company being renamed as Target Corporation in August 2000. Target operates 1,916 stores in the United States; it began operations in Canada in March 2013 and operates 127 locations through its Canadian subsidiary. **In December 2013, a data breach of Target's systems affected up to 110 million customers.**

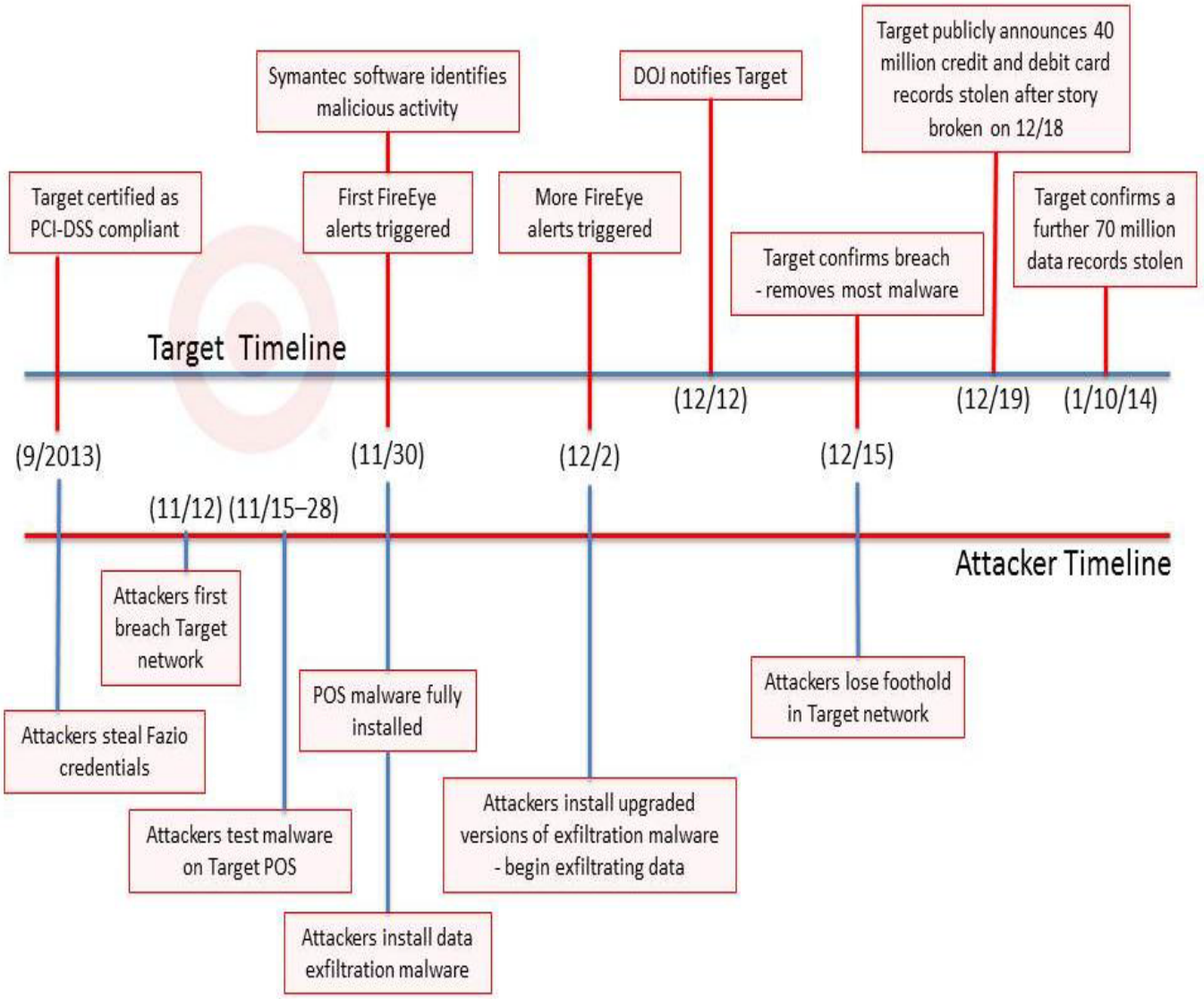
Source: Wikipedia

In November and December 2013, cyber thieves executed a successful cyber attack against Target, one of the largest retail companies in the United States. The attackers surreptitiously gained access to Target's computer network, stole the financial and personal information of as many as 110 million Target customers, and then removed this sensitive information from Target's network to a server in Eastern Europe.

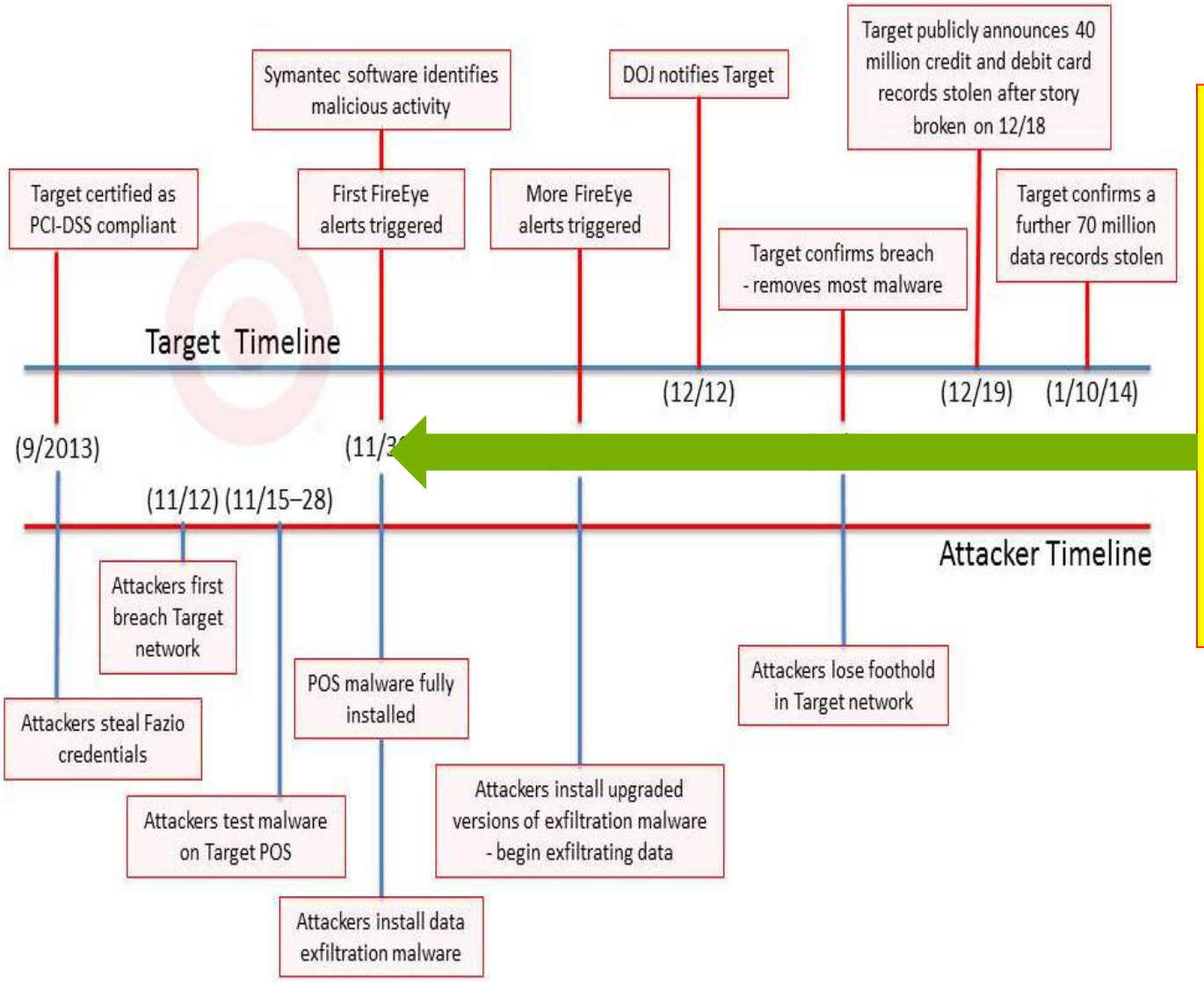
John Mulligan, Target's Executive Vice President and Chief Financial Officer, testified that his company "had in place multiple layers of protection, including firewalls, malware detection software, intrusion detection and prevention capabilities and data loss prevention tools." He further stated that Target had been certified in September 2013 as compliant with the Payment Card Industry Data Security Standards (PCI-DSS), which credit card companies require before allowing merchants to process credit and debit card payments.

Source: "Kill Chain" Analysis of the 2013 Target Data Breach; Committee On Commerce, Science and Transportation

Kill Chain Timeline

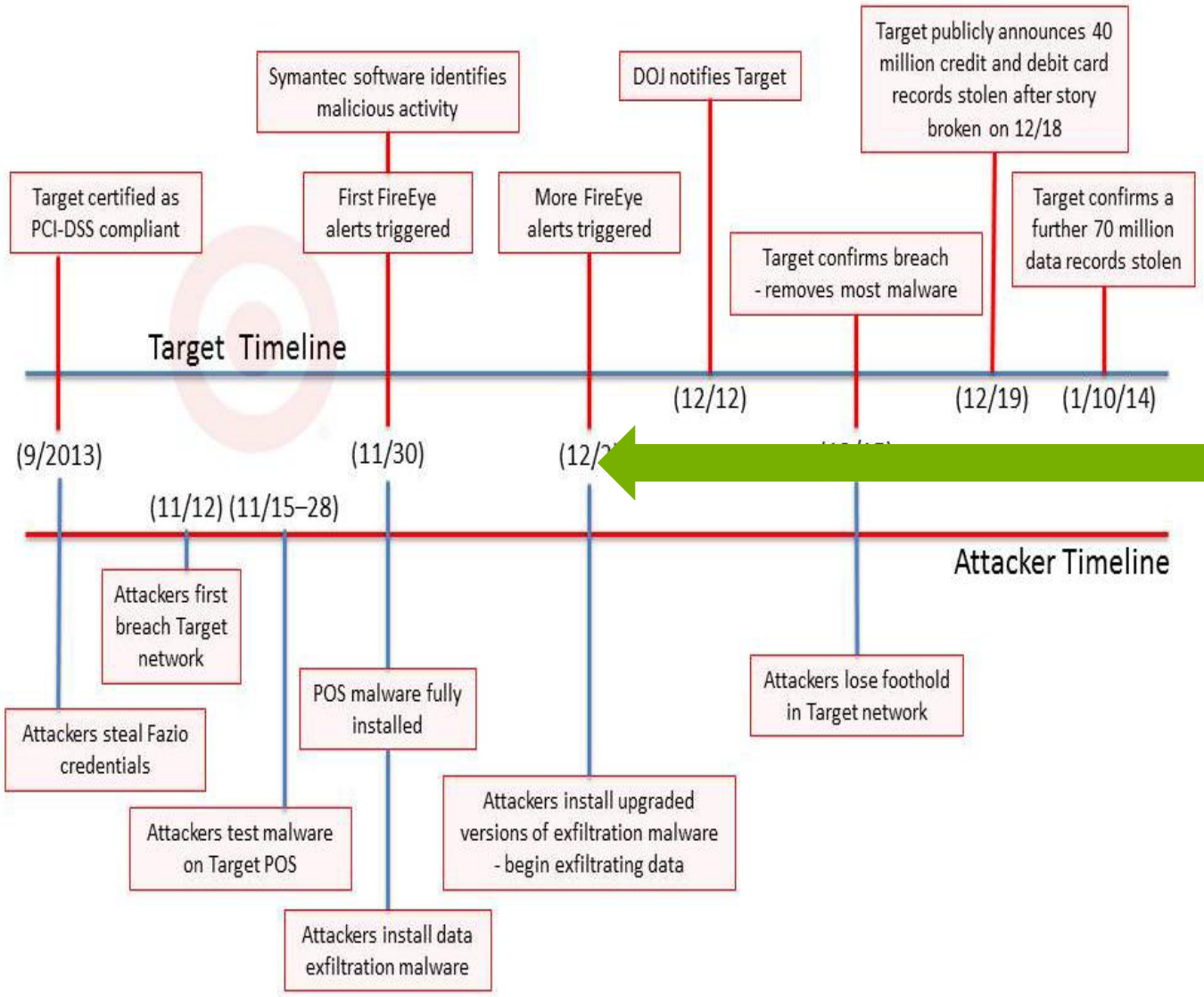


First Trigger – Already Compromised



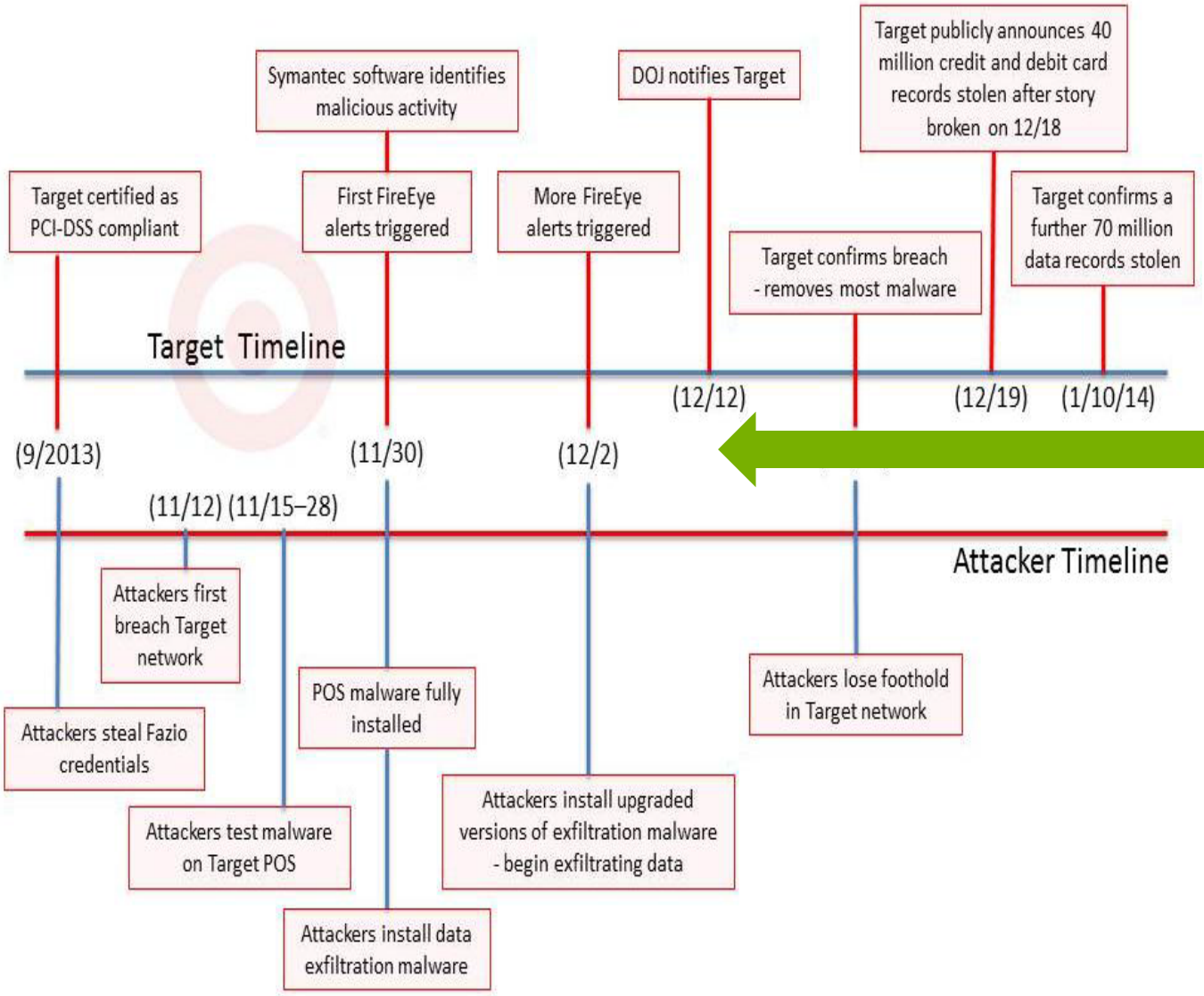
- Fire eye event
- False position prone
- Users don't fully trust
- No additional activity information
  - What traffic preceeded and followed, from and to where ?
- Network and business context
- Are these or can they reach critical assets
- No business process for triaging and analysing
- **Ignored !**

More Alerts – No Linkage



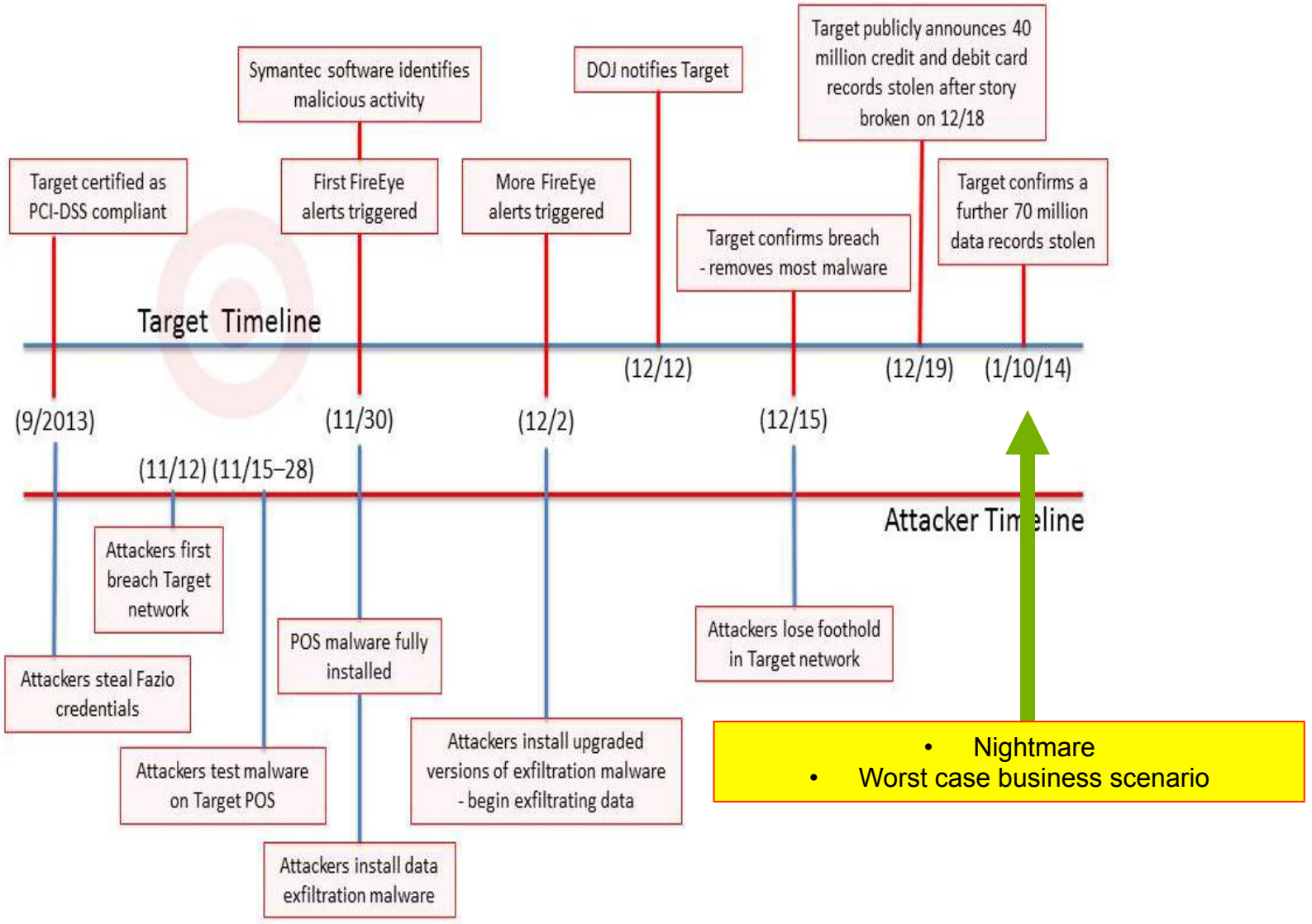
- More alerts
- Different areas of network
- Not correlated with other activity or in the context of the business or network
- **Not enough visibility or context**
- **Still ignored !**

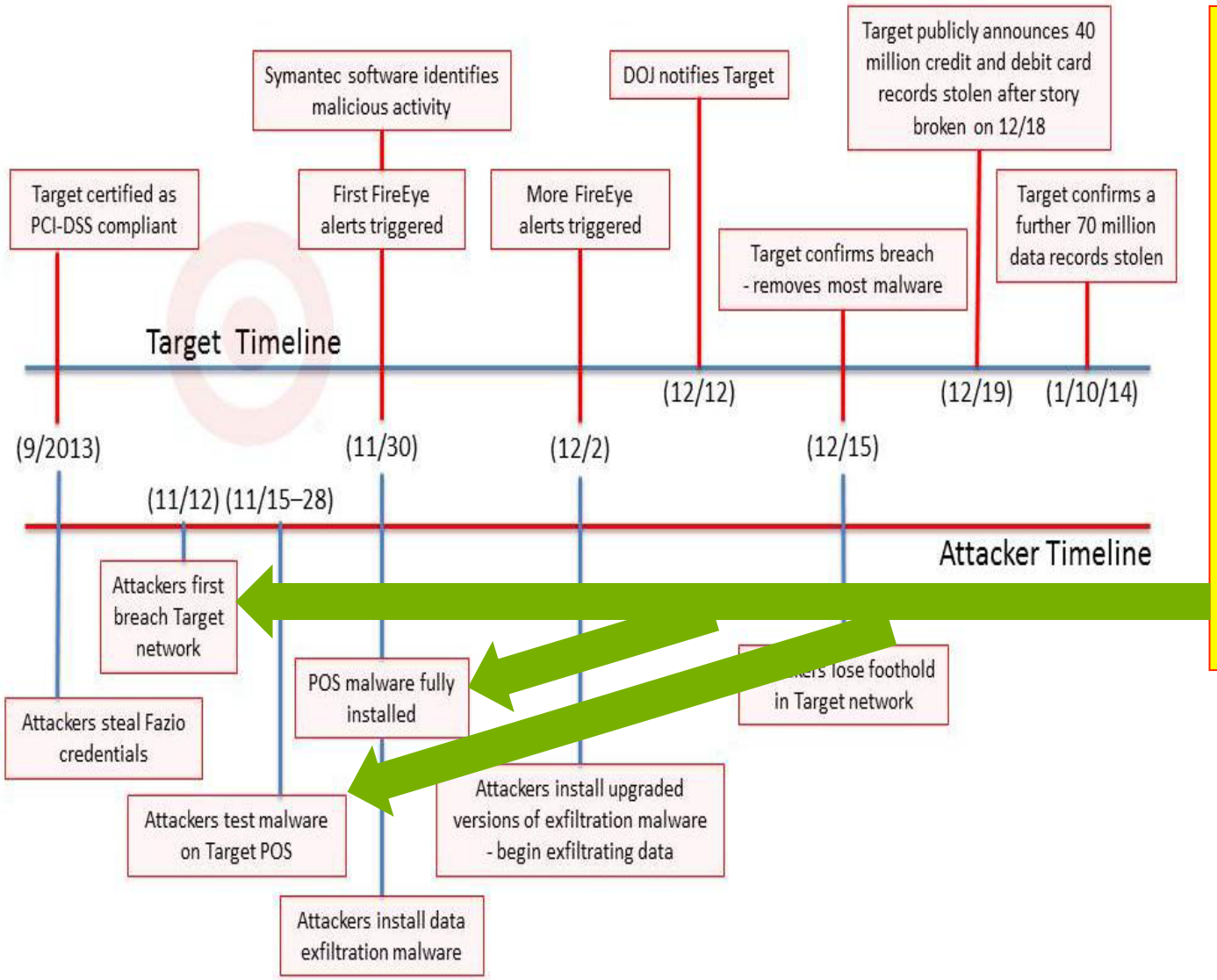
DOJ Notification – 40 Million Records Gone



- Too Late
- **Nightmare business scenario unfolds**

Continued Breaches Undetected





- Security Logs + Events
- Network Flow Data
- Vulnerability Data
- Network Topology
- Asset profile with business context, risk, ownerships
- Correlation Rules
- Behavioural Analysis

- **Increased incident relevance**
- **One incident case and analysis workflow**
- **Integrated Forensics – Rapid confirmation of attack**
- **Massive reduction of window of exposure**

Analysts have noticed

Domain	Market Segment / Report	Gartner Magic Quadrant	Forrester Wave	IDC Market Share / Scape
Security Intelligence	Security Information and Event Management (SIEM)	**Leader** *2014*		**Leader** *2013*
Fraud Protection	Web Fraud Detection *(Trusteer)*	**Leader** *2013*		
Identity and Access Management	Federated Identity Management and Single Sign-On			**Leader** *2013*
	Identity and Access Governance	**Leader** *2015*	**Strong Contender** *2013*	
	Role Management and Access Recertification		**Contender** *2011*	
	Web Access Management (WAM)	**Leader** *2013 MarketScope*		
	Mobile Access Management	**Leader,** *2014 Customer Value, Frost & Sullivan*		
	Identity Provisioning Management	**Leader,** *2014 Leadership Compass, KuppingerCole*		
Data Security	Database Auditing and Real-Time Protection		**Leader** *2011*	
	Data Masking	**Leader** *2014*		
Application Security	Application Security Testing *(dynamic and static)*	**Leader** *2014*	**Leader** *2014*	**Leader** *2013*
Network, Endpoint and Mobile Security	Network Intrusion Prevention Systems (NIPS)	**Challenger** *2014*		
	Endpoint: Client Management Tools	**Leader** *2014*		
	Endpoint Protection Platforms (EPP)	**Visionary** *2014*	**Strong Performer** *2013*	
	Mobile Security *(Fiberlink)*	**Leader** *2014*		
Consulting and Managed Services	Managed Security Services (MSS)	**Leader** *2014 (AP, NA, WW)*	**Leader** *2014 (NA)*	**Leader** *2014*
	Information Security Consulting Services		**Leader** *2013*	
	Public Cloud Service Providers' Security (IBM Bluemix)		**Strong Contender** *2014*	

Note: Rankings compiled as of January, 2015

☐ *Rankings not yet available*

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, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, 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 ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security