

# Security Intelligence. Think Integrated.

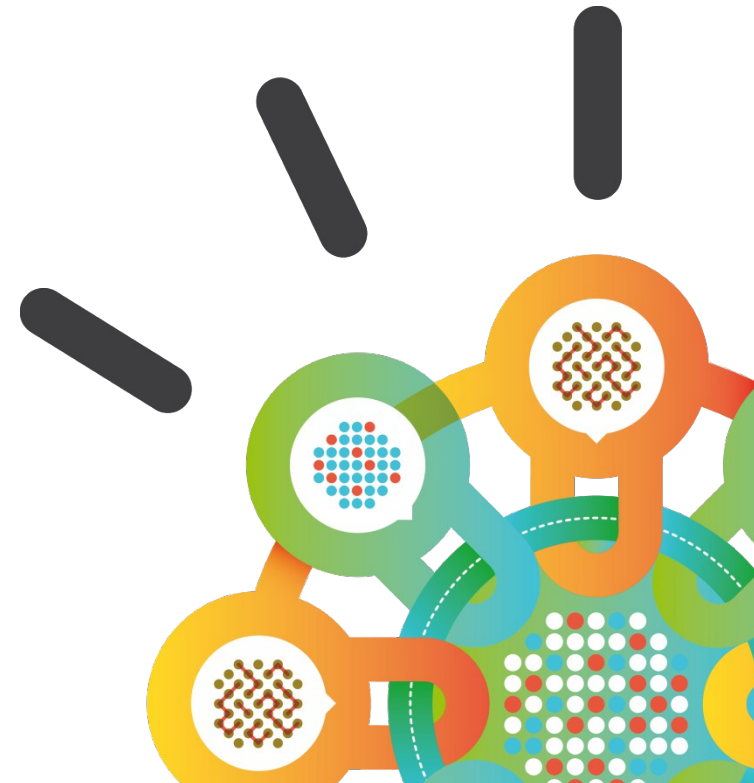
- IBM Security Intelligence
- *Intelligent Detection and Optimized Response*



**Chris Meenan**  
World-Wide Product Manager  
IBM Security QRadar



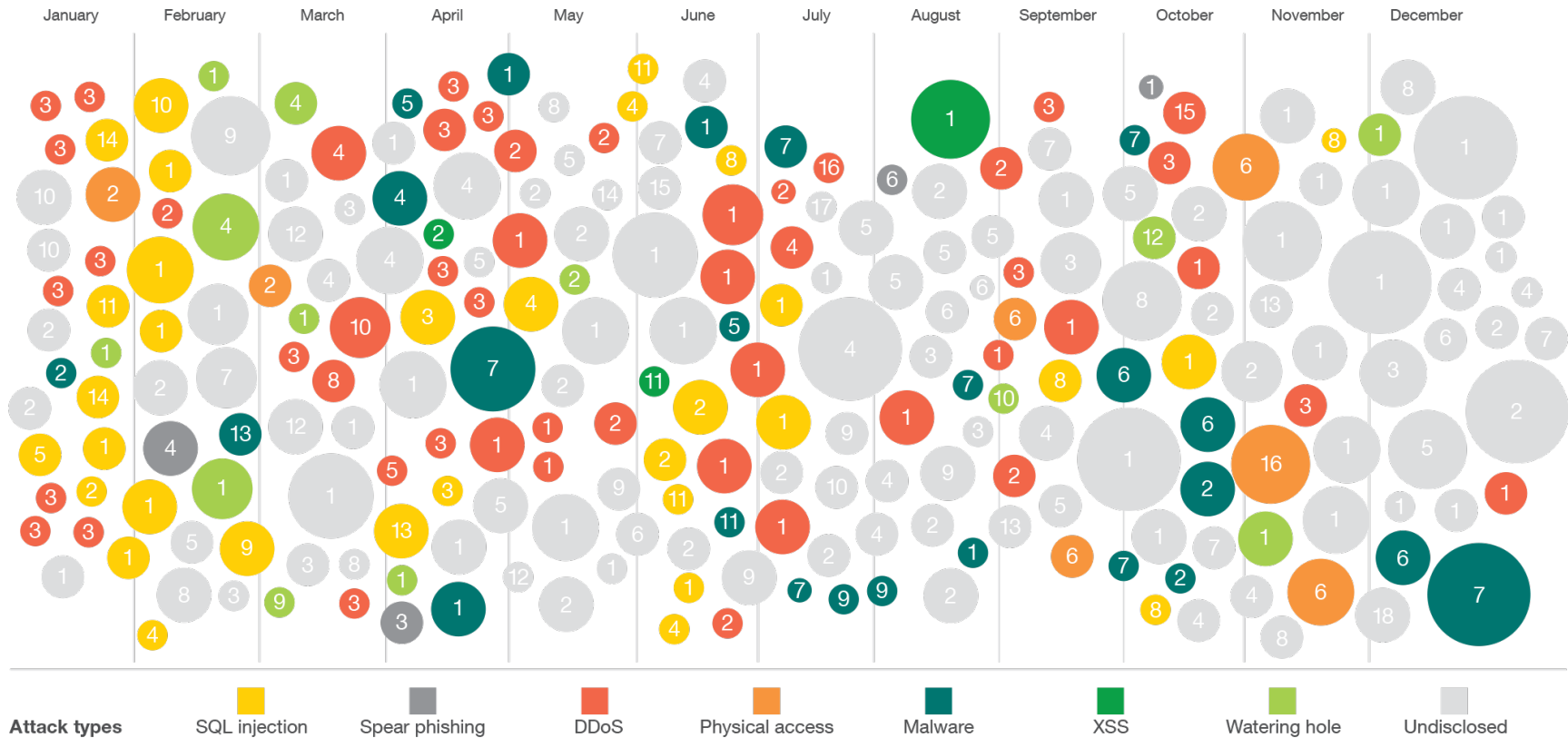
**Vijay Dheap**  
World-Wide Product Manager  
IBM Security QRadar



# IBM X-Force Report - Need for intelligent detection and response

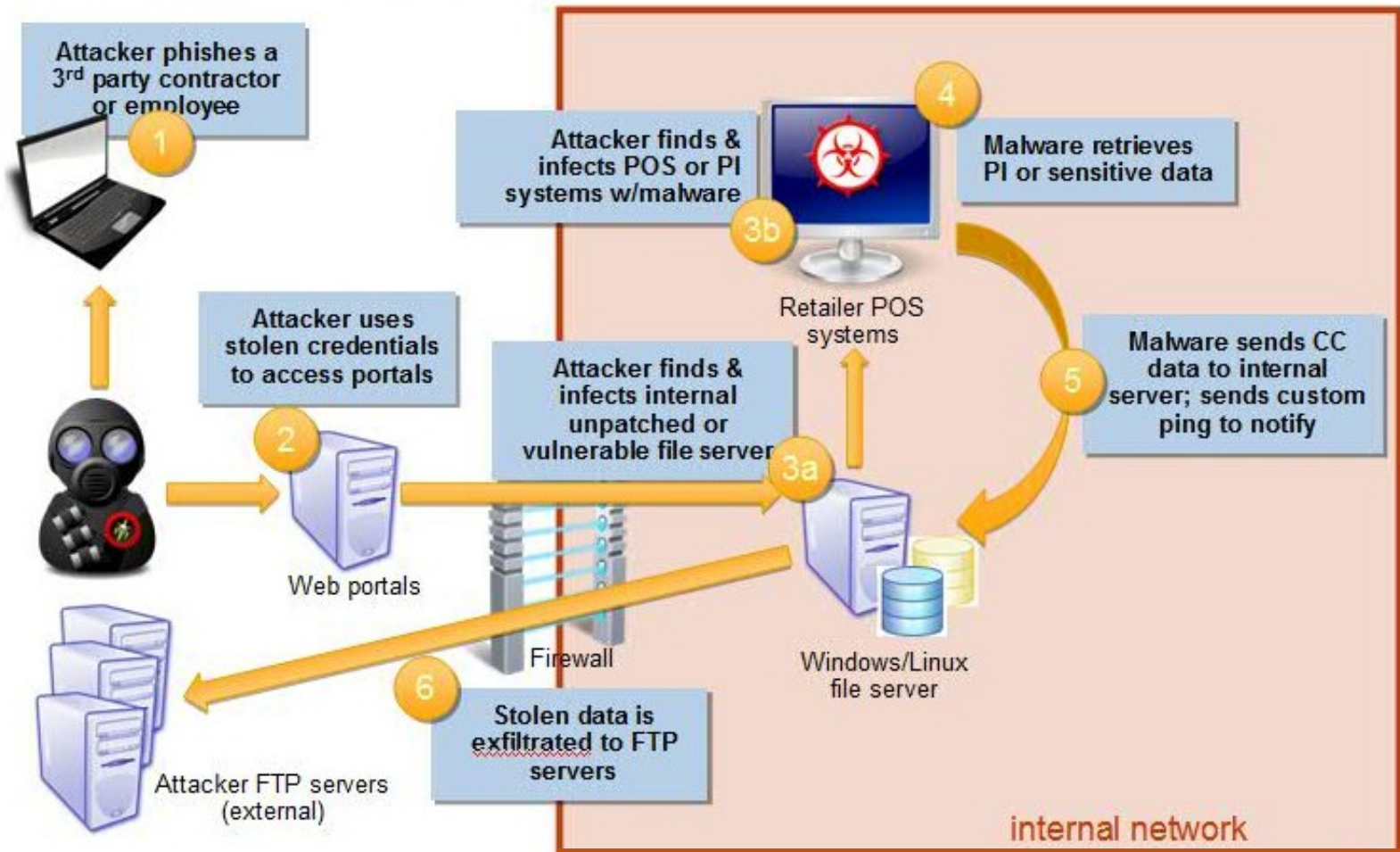
## Sampling of 2013 security incidents by attack type, time and impact

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.

# Perimeter defenses are not enough against today's kill chain





## Cost of cyber-crime is increasing



The annual cost of cyber-crime in the U.S. now stands at **\$11.6 million** per organization, up 26 percent from 2012.

Source: "2013 Cost of Cyber-Crime Study", Ponemon Institute



## And Breach Duration is Increasing



Attackers spend an estimated **243 days** on a victim's network before they are discovered<sup>1</sup>.

Once they have been discovered, it takes **32 days** on average to resolve a cyber-attack, up from 24 days (33%) in 2012<sup>2</sup>.

Total time from attack to resolution: **275 days**

Sources: <sup>1</sup>Mandiant M-Trends 2013 Report: Attack the Security Gap, <sup>2</sup>2013 Cost of Cyber-Crime Study", Ponemon Institute,



## Making detection and response more important than ever


Nearly ***two-thirds*** (63%) of organizations learn they are breached from an external source.

**38%** of targets were attacked again once the original incident was remediated

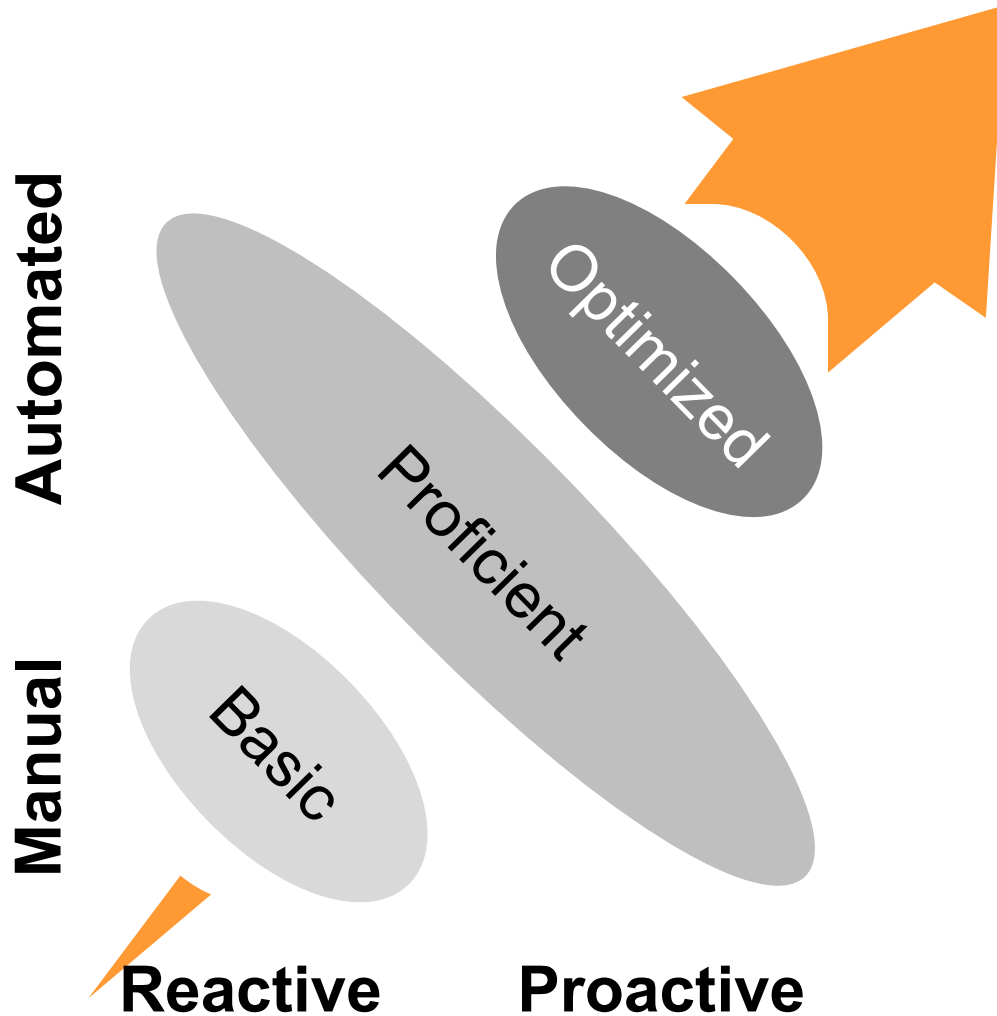
Source: Mandiant M-Trends 2013 Report - Attack the Security Gap



# Why are attackers so successful?

Escalating Threats	Increasing Complexity	Resource Constraints
 <ul style="list-style-type: none"> <li>· Increasingly sophisticated attack methods</li> <li>· Disappearing perimeters</li> <li>· Accelerating number of security breaches</li> </ul>	 <ul style="list-style-type: none"> <li>· Constantly changing infrastructure</li> <li>· Too many products from multiple vendors; costly to configure and manage</li> <li>· Inadequate and ineffective tools</li> </ul>	 <ul style="list-style-type: none"> <li>· Security teams struggling with lack of skills and staff</li> <li>· Too much data with limited human resources to manage it all</li> </ul>

# Self-Assessment: On a day-to-day basis, where is your organization?



- **Basic**
  - Log management
  - Compliance
  - Vulnerability scans
- **Proficient**
  - Security information and event management
  - Network flow monitoring
  - Vulnerability management
  - Configuration and risk management
- **Optimized**
  - Defined processes
  - Incident investigation
  - Proactive remediation



## Best Practices – Intelligent Detection and Optimized Response

1

### Prevention - Predict and prioritize security weaknesses

- Gather threat intelligence information
- Manage vulnerabilities and risks
- Augment vulnerability scan data with context for optimized prioritization
- Manage device configurations (firewalls, switches, routers, IPS/IDS)

2

### Real-time reaction to exploits

- Correlate logs, events, network flows, identities, assets, vulnerabilities, configurations and add context
- Use automated solutions to make data actionable by existing staff

3

### Rapidly investigate incidents when they occur

- Quickly and easily trace step-by-step actions of an attacker (forensic analysis)
- Uncover the root cause of a breach, remediate, take corrective and preventative action

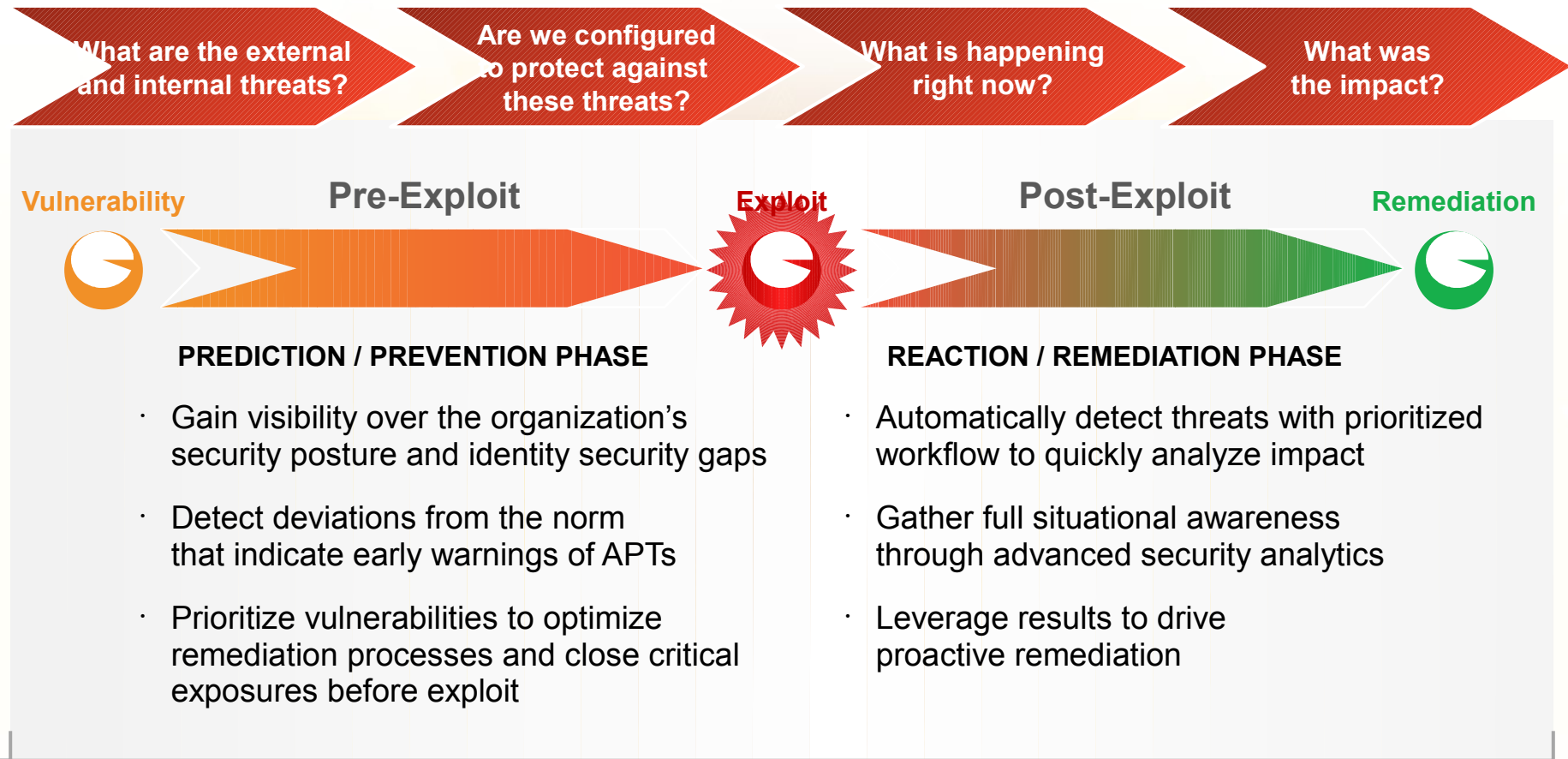
4

### Detect deviations from normal to identify malicious activity

- Establish baseline behaviors
- Monitor and investigate anomalies

Security covers a range of activities – integration across technologies is required

# Security Intelligence - Insights across the event timeline



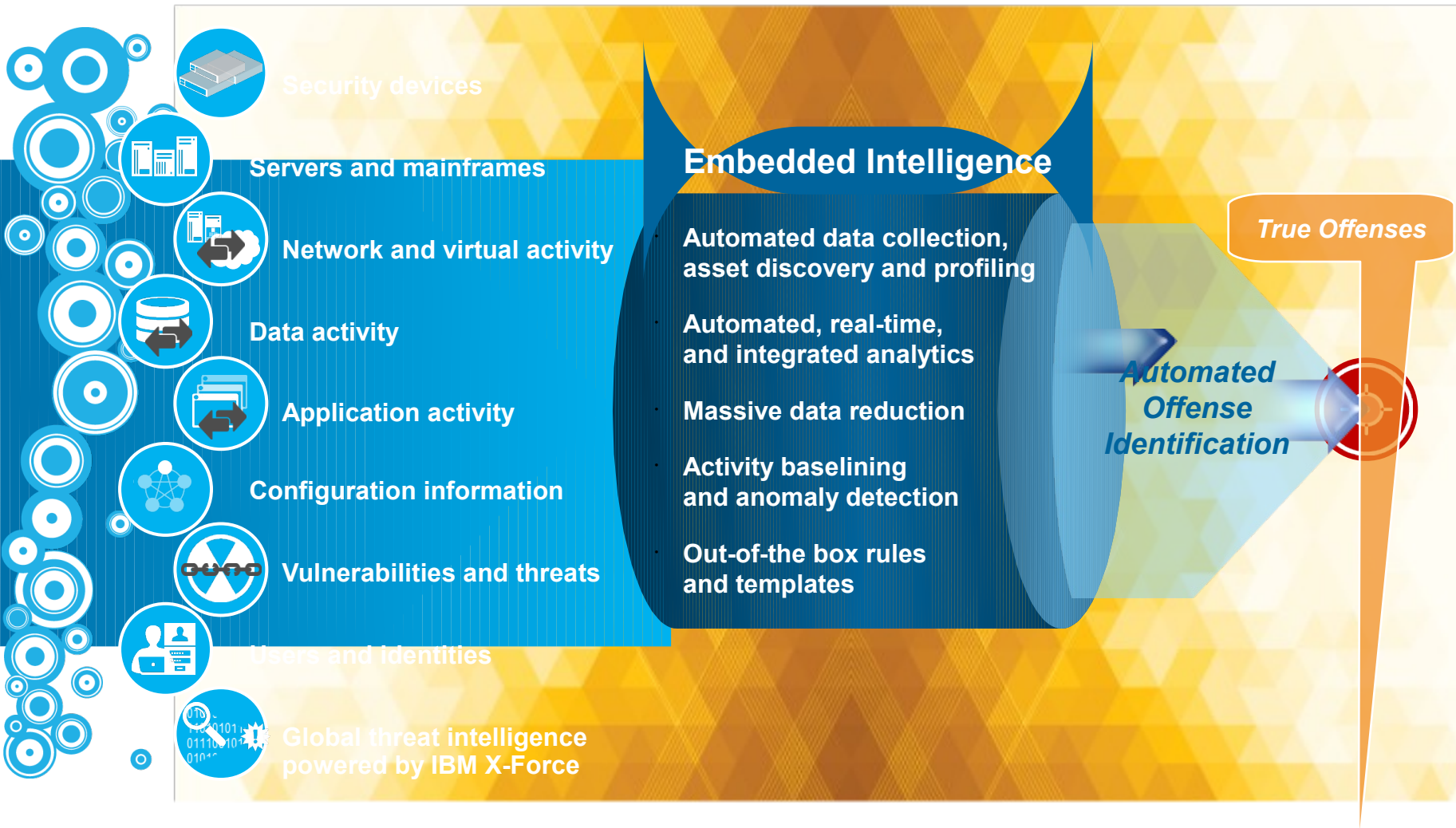
## Security Intelligence

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

# Security Information and Event Management

## Extensive Data Sources

## ...Suspected Incidents



# Single console for intelligent detection and optimized response

**Offense 3063** Summary Attackers Targets Categories Annotations Networks Events

<b>Magnitude</b>		<b>Relevance</b>	0	<b>Severity</b>	8	<b>Credibility</b>	3
<b>Description</b>	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Preceded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan		<b>Event count</b>	1428 events in 3 categories			
<b>Attacker/Src</b>	202.153.48.66		<b>Start</b>	2009-09-29 16:05:01			
<b>Target(s)/Dest</b>	Local (717)		<b>Duration</b>	1m 32s			
<b>Network(s)</b>	Multiple (3)		<b>Assigned to</b>	Not assigned			
<b>Notes</b>	Vulnerability Correlation Use Case Illustrates a scenario involving correlation of vulnerability data with IDS alerts An attacker originating from China (202.153.48.66) is exploiting the Conficker worm exploit (CVE 2008-4250). The attack is preceded by Recon - External - Potential Network Scan.						

**Attacker Summary** Details

<b>Magnitude</b>		<b>User</b>	Karen
<b>Description</b>	202.153.48.66	<b>Asset Name</b>	Unknown
<b>Vulnerabilities</b>	0	<b>MAC</b>	Unknown
<b>Location</b>	China	<b>Asset Weight</b>	Unknown

**Top 5 Categories** Categories

Name	Magnitude	Local Target Count	Global Target Count	Last Seen
Buffer Overflow		8	1417	09-29 16:06:33
Misc Exploit		3	1417	09-29 16:06:33
Network Sweep		716	1417	09-29 16:05:01

**Targets**

IP/DNS Name	Assigned	User	MAC	Location	Weight
Windows AD 10.101.3.11	Unknown	Unknown	Unknown	main	8
10.101.3.11	Unknown	Unknown	Unknown	main	0
DC106 10.101.3.11	Yes	Unknown	Unknown	main	10
10.101.3.11	Unknown	Unknown	Unknown	main	0

**Top 10 Events** Events

Event Name	Magnitude	Log Source	Category	Destination	Host Port	Time
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-vm	Misc Exploit	10.101.3.15	445	09-29 16:06:33
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @ 10.1.1.5	Buffer Overflow	10.101.3.10	445	09-29 16:06:28
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Custom Rule Engine-5 :: qradar-vm	Buffer Overflow	10.101.3.15	445	09-29 16:06:33
Misc Exploit - Event CRE		Custom Rule Engine-5 :: qradar-vm	Buffer Overflow	10.101.3.13	445	09-29 16:06:31
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm	Network Sweep	10.101.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm	Network Sweep	10.101.3.15	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm	Network Sweep	10.101.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm	Network Sweep	10.101.3.15	445	09-29 16:05:01

What was the attack?

Who was responsible?

Was it successful?

Where do I find them?

How valuable are the targets to the business?

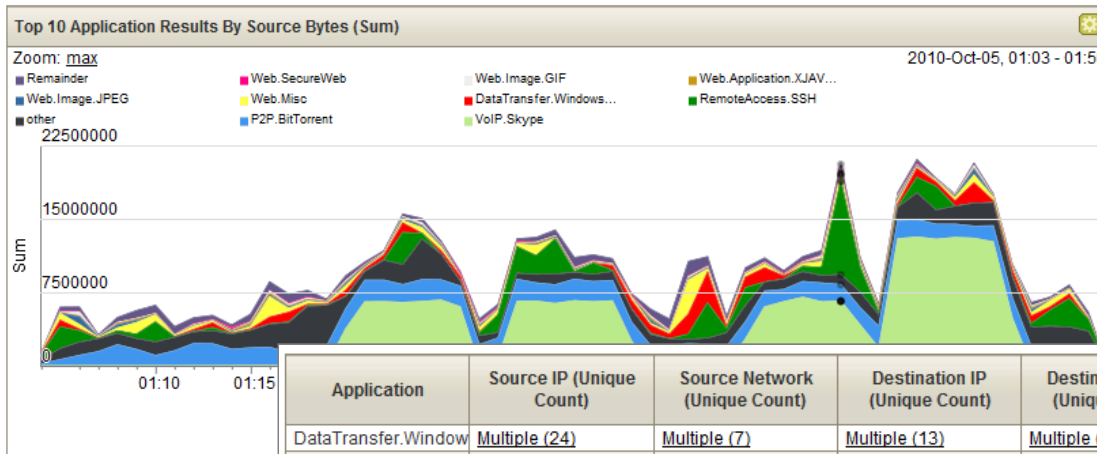
How many targets involved?

Are any of them vulnerable?

Where is all the evidence?

# 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

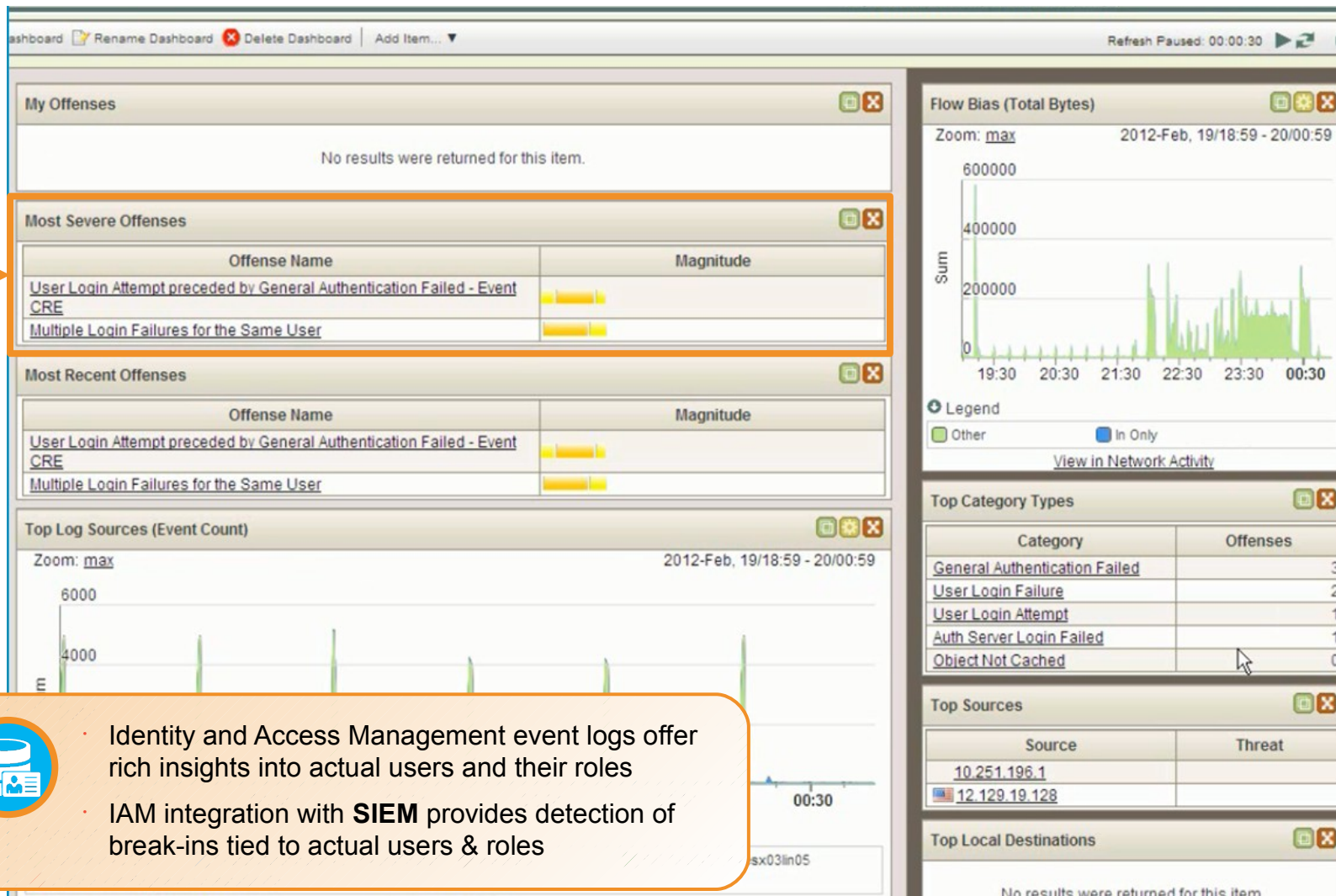
**Reports traffic from an IP address known to be in a country that does not have remote access right.**

*“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



# Identity and Access Management Integration with SIEM



The dashboard displays several key components:

- My Offenses:** No results were returned for this item.
- Most Severe Offenses:**

Offense Name	Magnitude
<a href="#">User Login Attempt preceded by General Authentication Failed - Event CRE</a>	High
<a href="#">Multiple Login Failures for the Same User</a>	Medium
- Most Recent Offenses:**

Offense Name	Magnitude
<a href="#">User Login Attempt preceded by General Authentication Failed - Event CRE</a>	High
<a href="#">Multiple Login Failures for the Same User</a>	Medium
- Flow Bias (Total Bytes):** A line chart showing network activity from 19:30 to 00:30. The y-axis represents 'Sum' from 0 to 600,000. A legend indicates 'Other' (green) and 'In Only' (blue). A 'View in Network Activity' link is present.
- Top Log Sources (Event Count):** A bar chart showing event counts from 00:30 to 00:30. The y-axis ranges from 0 to 6,000.
- Top Category Types:**

Category	Offenses
<a href="#">General Authentication Failed</a>	3
<a href="#">User Login Failure</a>	2
<a href="#">User Login Attempt</a>	1
<a href="#">Auth Server Login Failed</a>	1
<a href="#">Object Not Cached</a>	0
- Top Sources:**

Source	Threat
<a href="#">10.251.196.1</a>	
<a href="#">12.129.19.128</a>	
- Top Local Destinations:** No results were returned for this item.



- Identity and Access Management event logs offer rich insights into actual users and their roles
- IAM integration with **SIEM** provides detection of break-ins tied to actual users & roles



# Identity and Access Management with SIEM Use Case

**An attacker steals system administrator login credentials then grants increased permissions to invalid user**

1 Privileged Identity Management sends SIEM details of the privilege escalation

2 SIEM notifies security analyst

3 Security analyst views a recording that shows compromised administrator granting a user rights outside of the formal process

Low Level Category	Source IP	Destination IP
Misc System Event	Multiple (4)	127.0.0.1
User Login Success	Multiple (3)	127.0.0.1
User Account Changed	Multiple (2)	127.0.0.1
General Audit Event	Multiple (2)	127.0.0.1
Password Change Succeeded	9.127.13.87	127.0.0.1
User Account Added	9.127.13.87	127.0.0.1
User Login Failure	Multiple (2)	127.0.0.1
User Right Assigned	9.127.12.111	127.0.0.1

**Event Information**

Event Name: ADD\_ROLE

Low Level Category: User Right Assigned

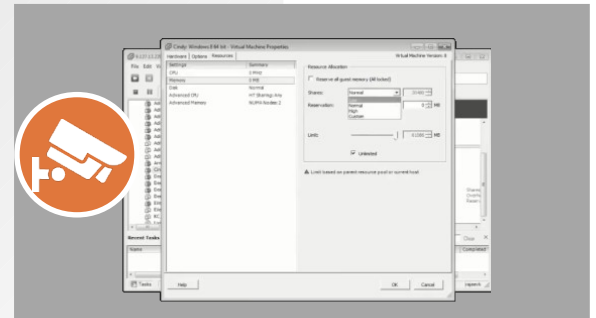
Event Description: Add role to user

Magnitude: ■■■ (2) Relevance: 1

Username: qa.encentuate.com/bouncy15

Start Time: Oct 9, 2013 3:56:45 PM Storage Time: Oct 9, 2013 3:56:45 PM

Changed User (custom): qa.encentuate.com/bouncy17



**Security analyst revokes compromised account access to prevent further malicious action**

# Extending Security Intelligence to Incident Forensic Investigations



# Customer Challenges in Employing Network Forensics

Critical gaps exist in available forensics and threat mitigation offerings to recover from an incident

Difficulty identifying true incidents hidden in mounds of data



Dependency on specialized skills to conduct detailed investigations



Disparate tools with limited intelligence inhibit productivity and efficacy in analysing incidents



Security teams must ***reduce the time to detect and respond to threats***. Confusion and wasted time aid the attacker.



## Next generation network forensics: know what happened, fast



Leverage Security Information and Event Management to optimize the process of investigating and gathering evidence on advanced attacks and data breaches

### **Tells you exactly when an incident occurred**

- Discovers true offenses and prioritizes forensics investigations
- Enables search-driven data exploration to return detailed, multi-level results in seconds

### **Merges powerful forensics capability with simplicity**

- Full packet capture for complete session reconstruction
- Unified view of all flow, user, event, and forensic information
- Retrace activity in chronological order

### **Delivers intelligence to guide forensics investigations**

- Visually construct threat actor relationships
- Builds detailed user and application profiles across multiple IDs



# Improved Network Security

## From session data analysis yielding basic application insights

Flow Information					
Protocol:	tcp_ip	Application:	Web.Facebook.Application		
Magnitude:		(4)	Relevance:	6	
First Packet Time:	2010-10-04 01:00:17	End Time:	2010-10-04 01:00:17	Severity:	1
Event Name:	Web.Facebook.Application				
Event Description:	Web				
Low Level Category:	Application detected with HTTP decoder domain lookup				
FBStatusPost (custom):	my%20asn%20is%20123456789%20C%20and%20my%20credit%20card%20number%20is%201234-4321-4567890				
HTTP User-Agent (custom):	Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.0.0 Safari/537.36				
HTTP Host (custom):	www.facebook.com				
HTTP GET Request (custom):	/profile.php?id=100001252874890 HTTP/1.1				
HTTP Content-Type (custom):	application/javascript, charset=utf-8				
HTTP Response Code (custom):	200 OK				
Google Search Terms (custom):	N/A				
HTTP Server (custom):	N/A				
FBUsername (custom):	rpnewman23665%40hotmail.com				
HTTP Version (custom):	1.1				

Source Payload	Destination Payload
<pre> GET /profile.php?id=100001252874890 HTTP/1.1 Host: www.facebook.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.0.0 Safari/537.36 Host: www.facebook.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.0.0 Safari/537.36 Host: www.facebook.com Connection: keep-alive </pre>	<pre> HTTP/1.1 200 OK Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Vary: Accept-Encoding Pragmas: no-cache Set-Cookie: act=deleted; expires=Tue, 11 Feb 2003 00:00:00 GMT; path=/; domain=www.facebook.com; HttpOnly= </pre>

## To full visualization of extended relationships and embedded content

ID	Date	Protocol	Description	Relevancy (1)
34	2008/04/24 09:24:14 PM	SMTP	Email Message	1
35	2008/04/24 09:24:14 PM	SMTP	Email Message	1
36	2008/04/24 09:24:14 PM	SMTP	Email Alternate Format	1
37	2008/04/24 09:24:14 PM	SMTP	Email Attachment	1
38	2008/04/24 09:24:14 PM	SMTP	Email Alternate Format	1
39	2008/04/24 09:24:14 PM	SMTP	Email Attachment	1
40	2008/04/25 12:11:49 AM	POP3	Email Message	1
41	2008/04/25 12:11:49 AM	POP3	Email Alternate Format	1
42	2008/05/01 10:43:18 PM	HTTP	Web Page	1
43	2008/05/01 10:43:18 PM	HTTP	Web Page	1
44	2008/05/01 10:43:31 PM	HTTP	Web Page	1
45	2008/05/01 10:43:32 PM	HTTP	Web Page	1
46	2008/05/01 10:44:15 PM	HTTP	Web Page	1
47	2010/01/26 05:04:06 PM	POP3	Email Message	1
48	2010/01/26 05:04:07 PM	POP3	Email Message	1
49	2010/01/26 05:11:31 PM	POP3	Email Message	1
50	2010/02/02 09:00:00 PM	SMTP	Email Message	1
51	2010/02/02 09:00:00 PM	HTTP	Email Message Header	1
52	2010/02/02 09:00:00 PM	HTTP	Email Message Header	1
53	2010/02/02 09:00:04 PM	HTTP	Email Message Body	1
54	2010/02/02 09:00:04 PM	HTTP	Email Message Body	1
55	2010/02/02 09:00:04 PM	HTTP	Email Attachment Reference	1
56	2010/02/02 09:00:04 PM	HTTP	Email Message	1

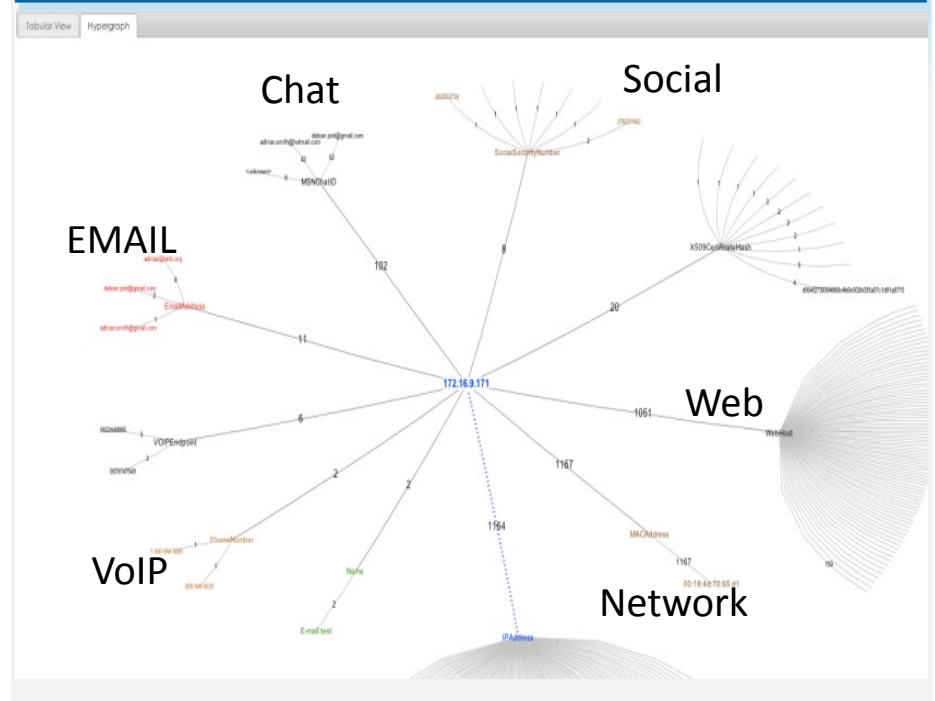
The screenshot shows the IEX website interface. At the top, there are navigation tabs for 'Home', 'Beleggingsfondsen', 'Turbo's', 'Spenders', 'Options & Futures', and 'Productrecensies'. The main content area features several news articles and market updates. A prominent article is titled '10 van Tak: Serieuze zaken' with a sub-headline 'Geen graspen meer voor mij. Drie nieuwe productiecrises en de AFM komt met een midpunt...'. Other articles include 'Speculeren met gokken', 'IEX Dageraad: Zonnig', and 'Mijn gilbecker'. On the right side, there is a 'Marktvandaag' section with a line chart and a table of market indices including 'AEX 517.33 +0.3', 'Euro Stoxx 50 338.62 +0.1', and 'NYSE 7059.64 +0.2'. The bottom of the page has a 'Ster' logo and a 'Kies uw bank par' link.

# Better clarity into entities and identities

## From standard asset identity information

Attacker Summary			
Magnitude		User	dwight.spencer
Description	10.100.50.21	Asset Name	Unknown
Vulnerabilities	0	MAC	
Location	<a href="#">Server_Network.Server_Network</a>	Asset Weight	0

## To rich visualizations of digital impressions showing extended relationships





# Helps IT Security teams

**1** Use intuition more than technical training

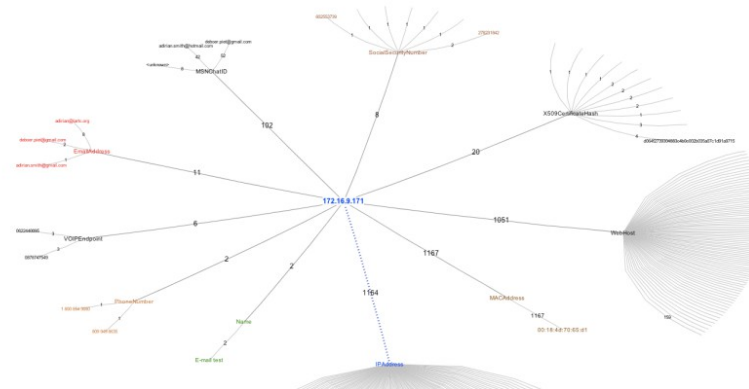
From aspepard to rucoulter aluminum nitrate shipment 83

Searching 36619 documents.

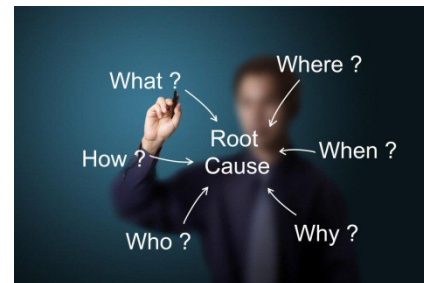
Row	Set	Score	Time Stamp	Protoct	Description	Suspect	Content	From	To
1		1	2008/04/24 01	SMTF	Email Message		That's very interesting - I G	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
2		1	2008/04/24 01	SMTF	Email Alternate		That's	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
3		1	2008/04/24 01	SMTF	Email Message		That's very interesting - I G	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
4		1	2008/04/24 01	SMTF	Email Alternate		That's	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
5		1	2008/04/24 01	POP3	Email Message		That's very interesting - I G	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
6		1	2008/04/24 01	POP3	Email Alternate		That's	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
7		1	2008/04/24 01	SMTF	Email Message		I'm a little concerned about	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
8		1	2008/04/24 01	SMTF	Email Alternate		is	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
9		1	2008/04/24 01	POP3	Email Message		I'm a little concerned about	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
10		1	2008/04/24 01	POP3	Email Alternate		is	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
11		1	2008/04/24 01	SMTF	Email Message		The aluminum nitrate ship(Dana Tomaszewski <dtoma@RussellCouturier.com>	"Russell Couturier" <...>	"Russell Couturier" <...>
12		1	2008/04/24 01	POP3	Email Message		Is the aluminum nitrate pur(Dana Tomaszewski <dtoma@RussellCouturier.com>	"Russell Couturier" <...>	"Russell Couturier" <...>
13		1	2008/04/24 08	SMTF	Email Message		Is the aluminum nitrate pur(Dana Tomaszewski <dtoma@RussellCouturier.com>	"Russell Couturier" <...>	"Russell Couturier" <...>
14		1	2008/04/24 08	SMTF	Email Alternate		Is the aluminum nitrate pur(Dana Tomaszewski <dtoma@RussellCouturier.com>	"Russell Couturier" <...>	"Russell Couturier" <...>
15		1	2008/04/24 08	POP3	Email Message		Is the aluminum nitrate pur(Dana Tomaszewski <dtoma@RussellCouturier.com>	"Russell Couturier" <...>	"Russell Couturier" <...>
16		1	2008/04/24 08	POP3	Email Alternate		Is the aluminum nitrate pur(Dana Tomaszewski <dtoma@RussellCouturier.com>	"Russell Couturier" <...>	"Russell Couturier" <...>
17		1	2008/04/24 01	SMTF	Email Message		How many pounds of the al(Dana Tomaszewski <dtoma@RussellCouturier.com>	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
18		1	2008/04/24 01	POP3	Email Message		How many pounds of the al(Dana Tomaszewski <dtoma@RussellCouturier.com>	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
19		1	2008/04/24 01	POP3	Email Message		How many pounds of the al(Dana Tomaszewski <dtoma@RussellCouturier.com>	"Andrew E. Copeland" <...>	"Russell Couturier" <...>
20		1	2008/04/24 01	SMTF	Email Message		Don't forget the money, las	"Andrew E. Copeland" <...>	"Dana Tomaszewski" <...>
21		1	2008/04/24 01	SMTF	Email Message		Don't forget the money, las	"Andrew E. Copeland" <...>	"Dana Tomaszewski" <...>
22		1	2009/03/12 12	MSN	MSN Chat Mess		Did I tell you about the alur	saimvvn@hotmail.com	slshstnre@hotmail.com

Page 1 of 2 ... 110 - 1

**2** Visualize digital impressions of attackers



**3** Prevent re-occurrence of successful breach





Client example: An international energy company reduces billions of events per day to find those that should be investigated

## *Optimize threat analysis*

An international energy firm analyzes

**2 billion**

events per day to find

**20-25**

potential offenses to investigate



### ***Business challenge***

- Reducing huge number of events to find the ones that need to be investigated
- Automating the process of analyzing security data

### ***Solutions*** (SIEM, Flow Analysis, Risk Management)

Combined analysis of historical data with real-time alerts to gain a 'big picture' view and uncover patterns of unusual activity humans miss and immediately block suspected traffic

# Client example: A financial information provider hardens defenses against threats and fraud

## Optimize risk management

financial information provider tracks

**250 activity baselines**

and saved

**50-80%**

on staffing versus alternative solutions



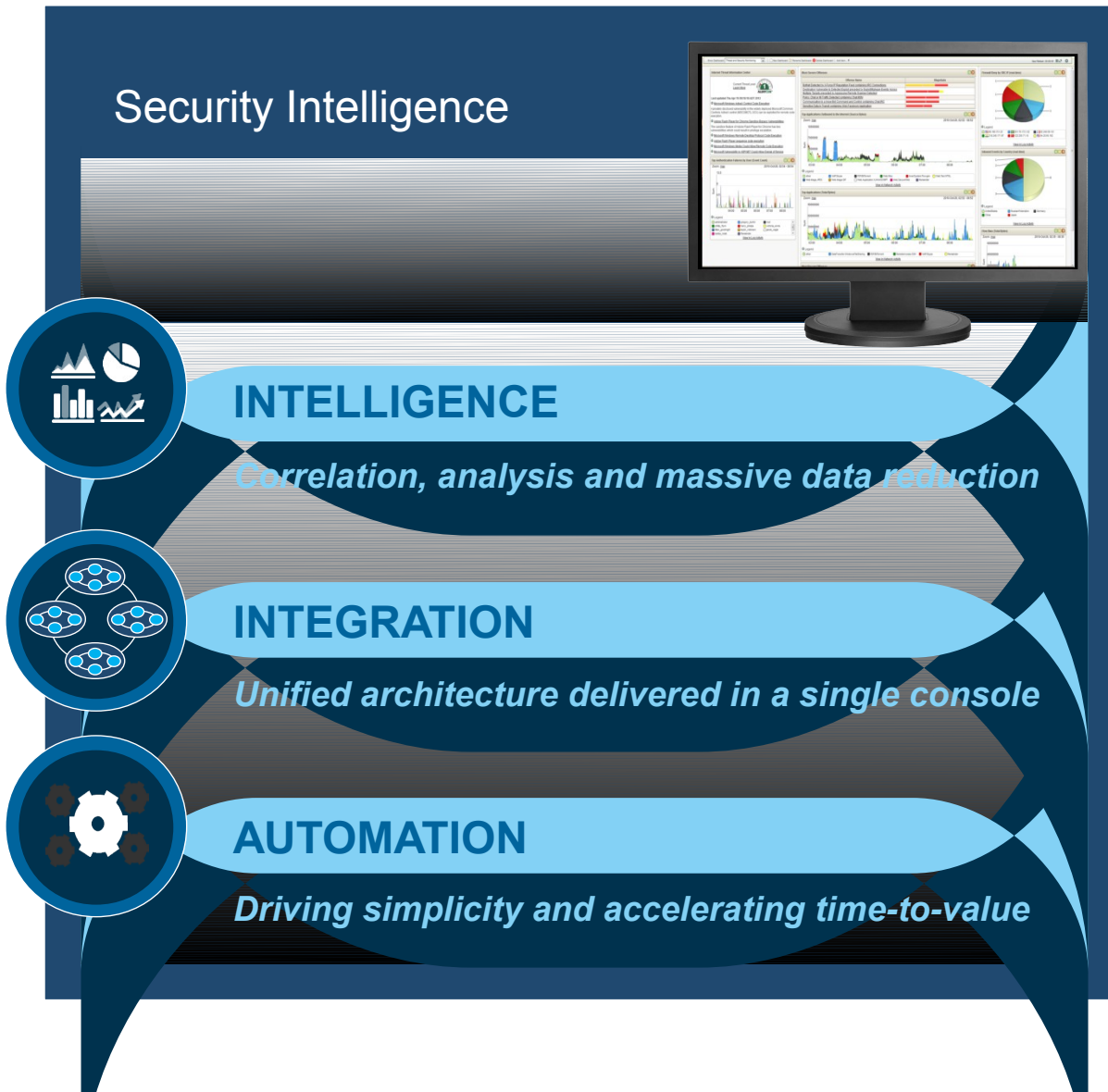
### **Business challenge**

- Detect wide range of security threats affecting public-facing Web applications
- Help identify subtle changes in user behavior that could indicate fraud or misuse
- Exceed ISO 27001 standard

### **Solutions** (SIEM, Flow Analysis, X-Force, Network IPS)

Combine analysis of historical data with real-time alerts to gain a 'big picture' view and uncover patterns of unusual activity humans miss and immediately block suspected traffic

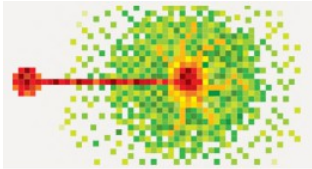
# Summary: Security Intelligence for Detection and Response



## Learn more about IBM Security Intelligence



Visit our Website



Download our new X-Force Report



Review our new Incident Forensics announcement



Read new blog posts: [securityintelligence.com](http://securityintelligence.com)



Follow us on Twitter: [@ibmsecurity](https://twitter.com/ibmsecurity)



# Questions?

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](http://www.ibm.com/security)



© Copyright IBM Corporation 2013. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.