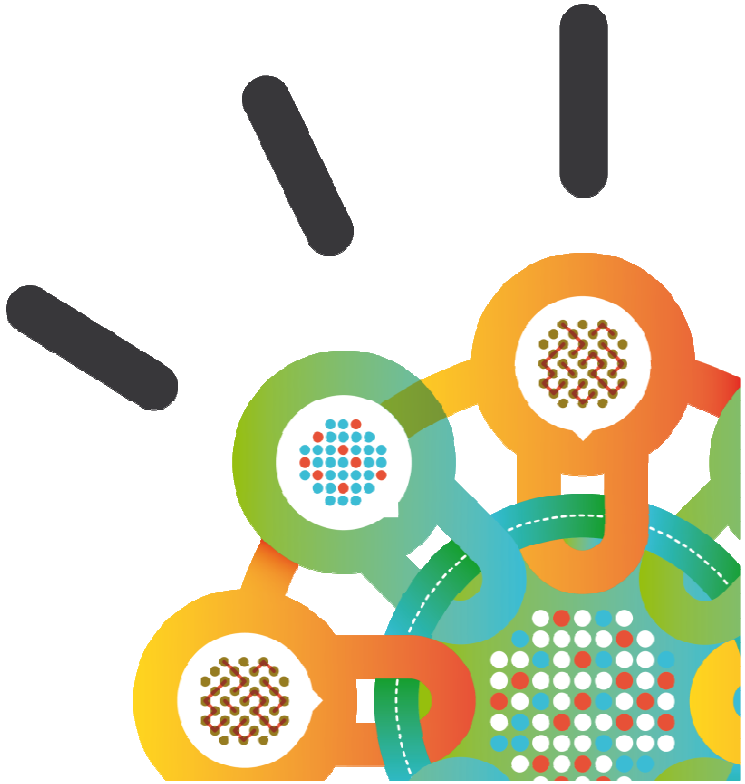
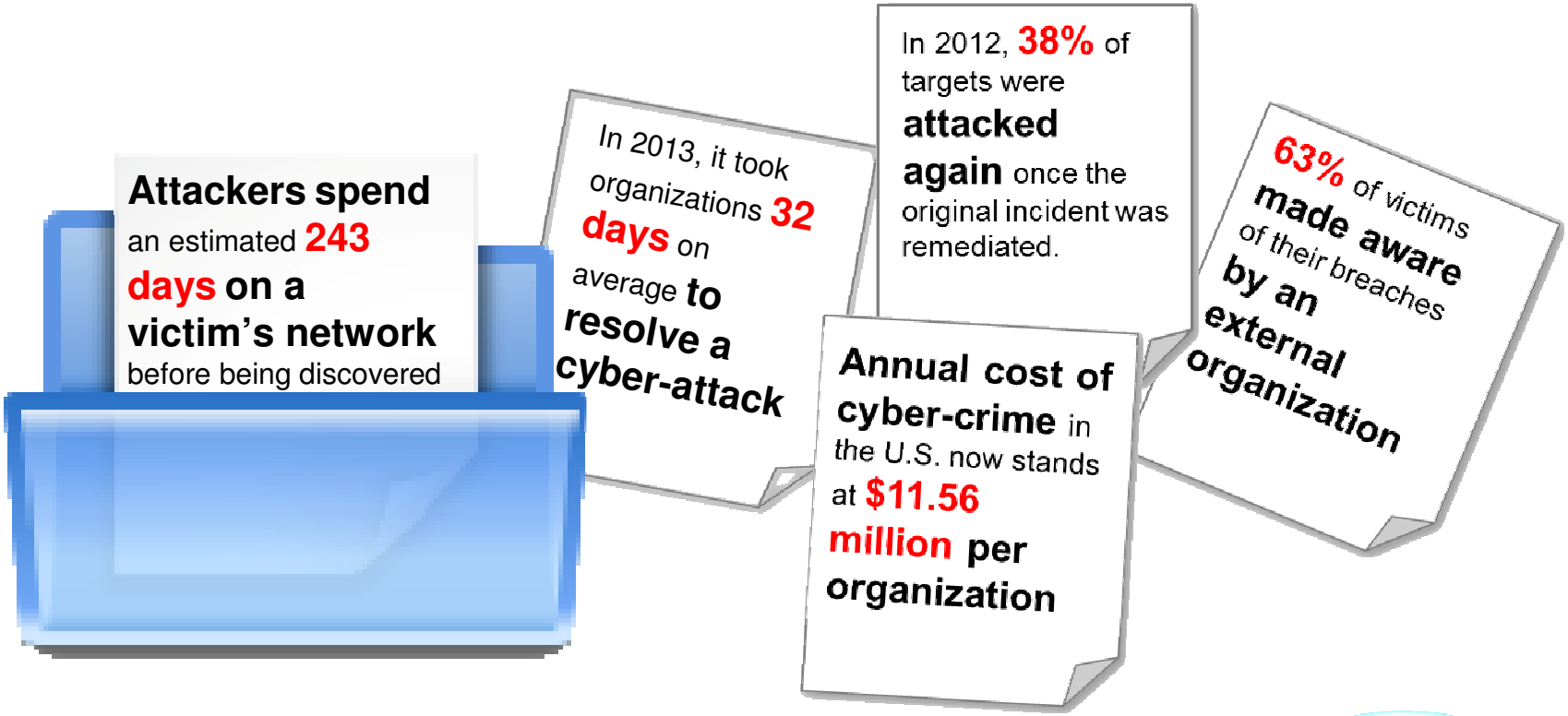
Security Intelligence.
Think Integrated.

IBM SECURITY QRADAR INCIDENT FORENSICS

DELIVERING CLARITY TO CYBER SECURITY INVESTIGATIONS



Harsh realities for many enterprise network CISOs



Has our organization been compromised?

When was our security breached?

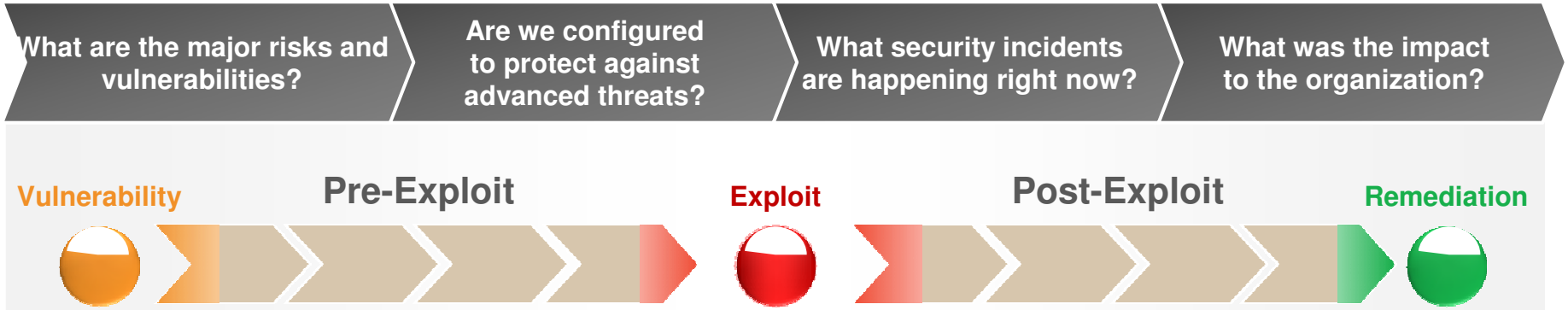
How do we identify the attack?

What type of attack is it?

What resources and assets are at risk?

How to avoid becoming a repeat victim?

Defending network requires appropriate solutions



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

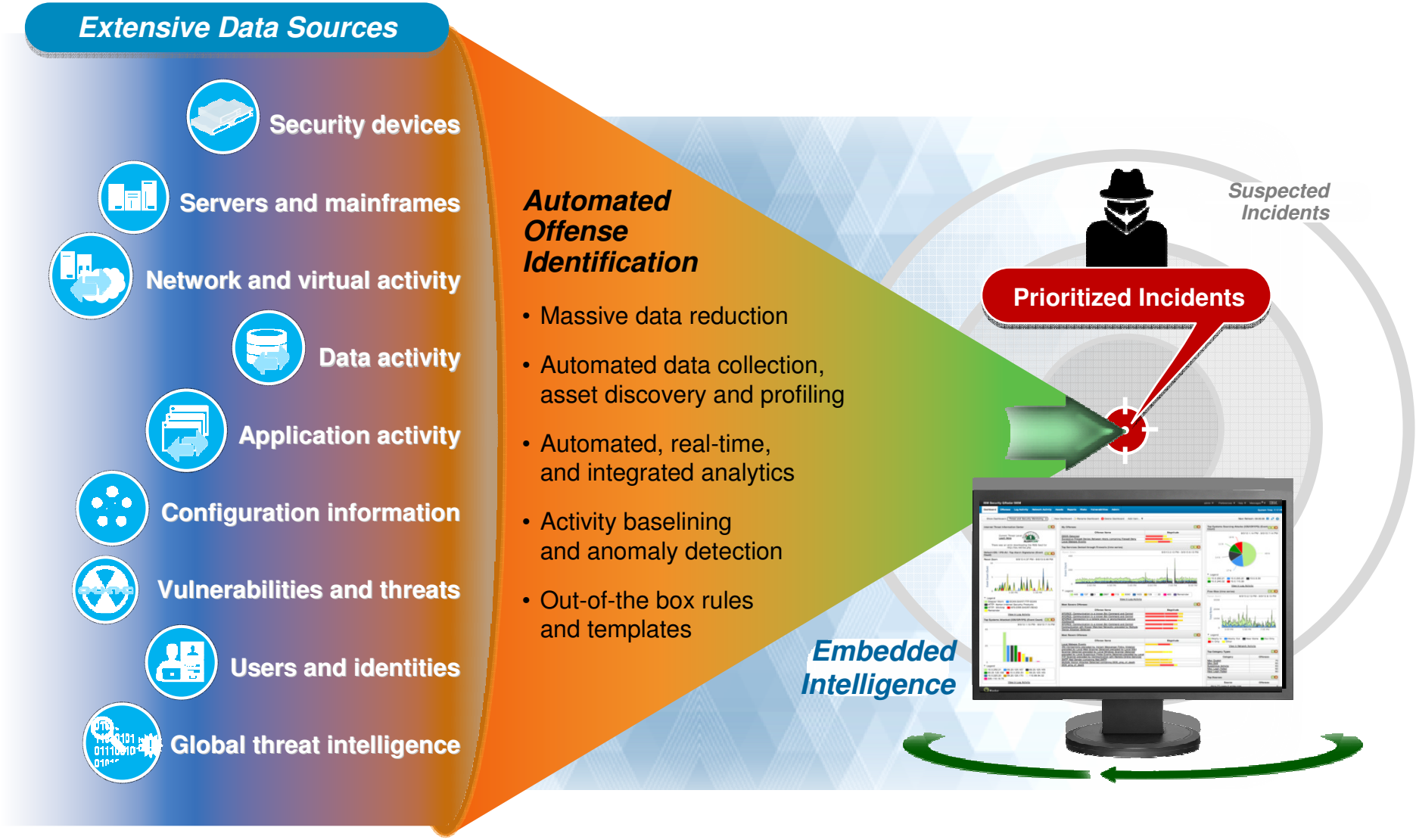
REACTION / REMEDIATION PHASE

- Automatically detect threats with prioritized workflow to quickly analyze impact
- Gather full situational awareness through advanced security analytics
- Perform forensic investigation reducing time to find root-cause; use results to drive faster remediation

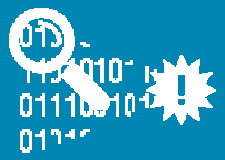
Security Intelligence

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

Embedded intelligence offers automated offense identification



Today's threats require greater clarity to detect & resolve

	Detect unauthorized activities targeting critical assets, uncover the motivations and develop an understanding of the full scope of the risk
 **Insider Threat Analysis**	Find the perpetrator, identify collaborators, pinpoint the systems compromised and document any data losses
 **Fraud and Abuse**	Uncover sophisticated schemes involving multiple seemingly disparate interactions aiming to perform fraudulent or abusive transactions
 **Evidence Gathering**	Compile evidence against malicious entities breaching secure systems and deleting or stealing sensitive data

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

Our Security Intelligence platform delivers powerful capabilities IT Security Operations Teams

Introducing QRadar Incident Forensics:

Leveraging the strengths of QRadar to optimize the process of investigating and gathering evidence on advanced attacks and data breaches

Tells you exactly when an incident occurred

- Integrated with QRadar to discover true offenses and prioritize 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

How network forensics is done

Full Packet Capture

- Capture packets off the network
- Include other, related structured and unstructured content stored within the network

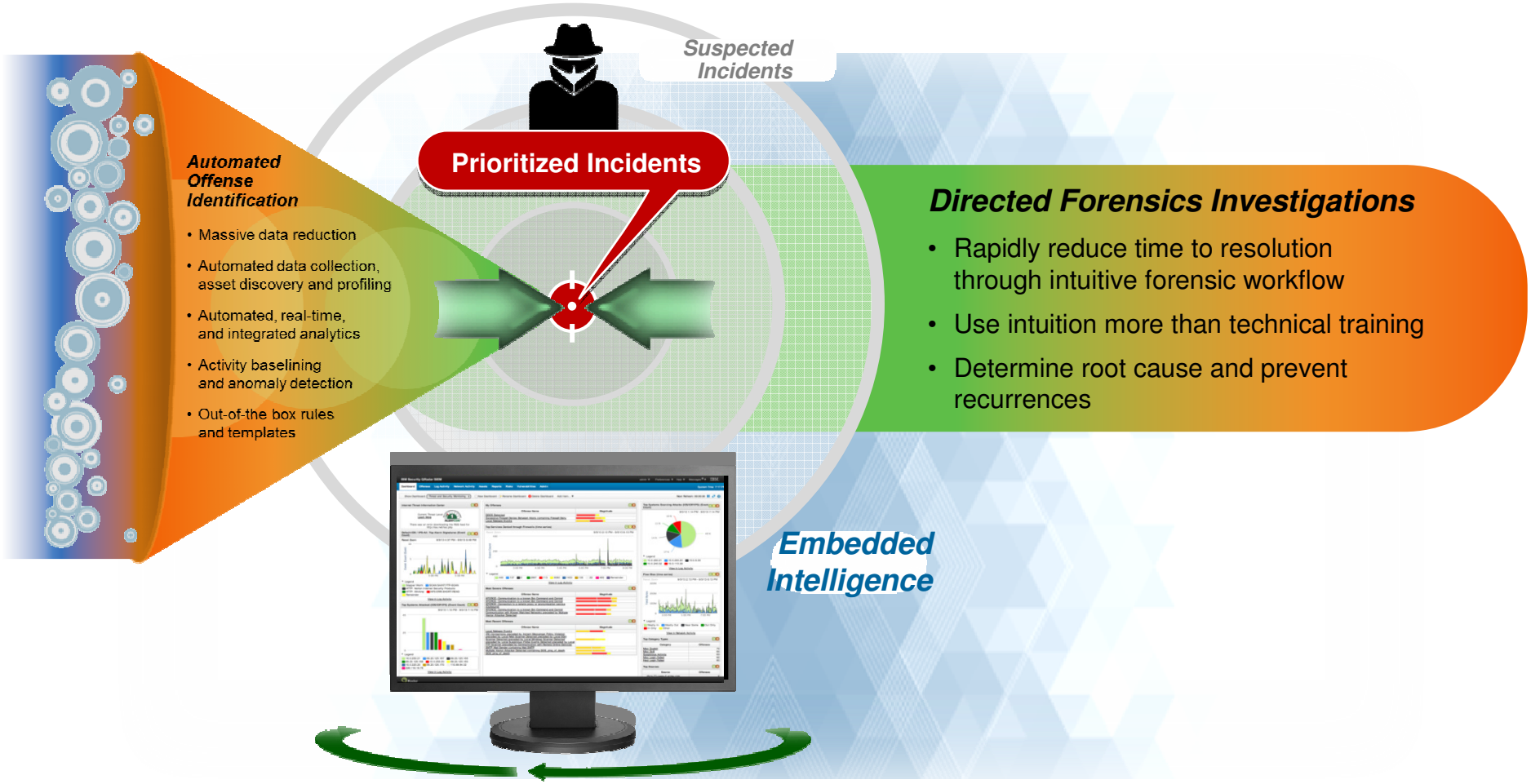
Retrieval & Session Reconstruction

- For a selected security incident, retrieve all the packets (time bounded)
- Re-assemble into searchable documents including full payload displayed in original form

Forensics Activity

- Navigate to uncover knowledge of threats
- Switch search criteria to see hidden relationships

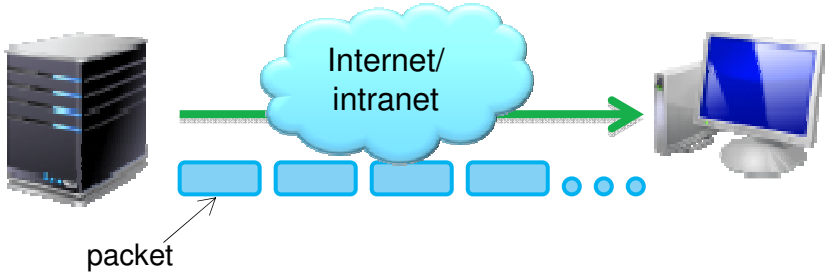
Extend clarity around incidents with in-depth forensics data



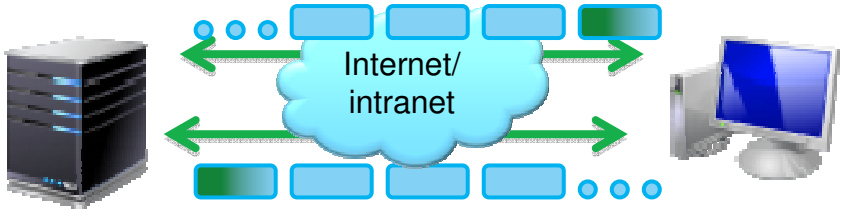
How Network Forensics is Done - with QRadar Incident Forensics

1	**Extension of QRadar Security Intelligence Platform**	• Built off high accuracy QRadar offense discovery • Improve efficiency of investigations
2	**Expands Data Available for Incident Forensics**	• Data-in-motion and data-at-rest • Structured and unstructured data
3	**Has Scalable Search Infrastructure**	• Index all the data • Correlate all the data • Prioritize search performance
4	**Builds Intelligence**	• Automated identification and assembly of identities • Automated distilling of suspicious content/activity • Content categorization informs data exclusion • Reveals linkages between entities
5	**Enables Intuitive Investigative Analysis**	• Simple search engine interface • Visual analytics • Retrace activity in chronological order with reconstructed content

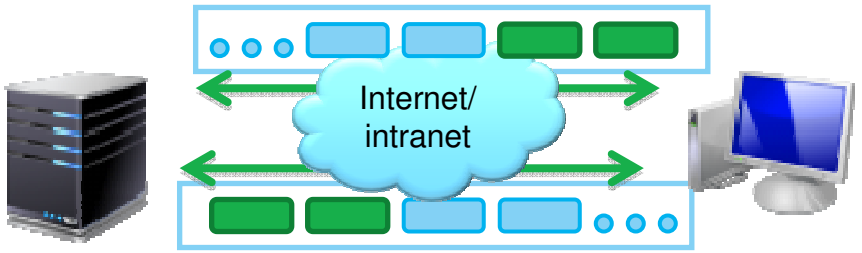
From NetFlow to QFlow to… …QRadar Incident Forensics



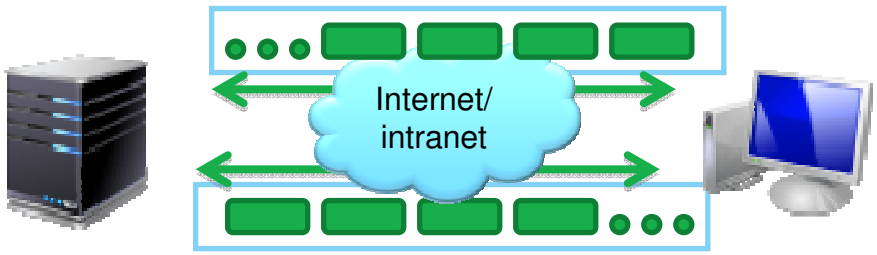
Netflow: packet oriented, identifies unidirectional sequences sharing source and destination IPs, ports, and type of service



QFlow: packet oriented, identifies bi-directional sequences aggregated into sessions, also identifies applications by capturing the beginning of a flow.



Competitive solutions: session oriented, some only capture a subset of each flow and index only the metadata—not the payload.



QRadar Incident Forensics: session oriented, captures all packets in a flow indexing the metadata and payload to enable fast search driven data exploration

Changing the dynamics of network forensics activities

QRadar Incident Forensics helps simplify the task, accelerate results, and ensure better results

Before

- Performed by technically trained forensics researchers
- Hunt for anomalous activities within specified time frame
- Identify threat actor and remediate malicious conditions

After

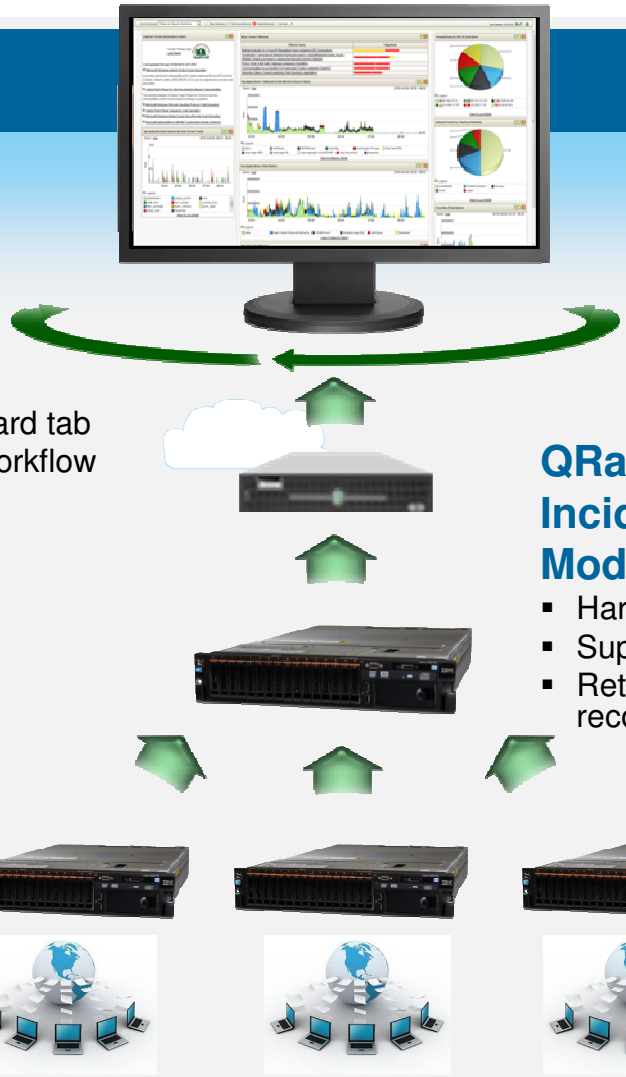
- Initiated using intuition with Internet search engine simplicity
- Follow security analytics or threat intelligence feed directives
- Retrace step-by-step movements for complete clarity

Benefit

- Address skills gap for forensics analysis
- Win race against time finding true threats and halting data loss
- Determine root cause and prevent breach recurrences

IBM Security QRadar Incident Forensics deployment model

Security Intelligence Platform



QRadar Security Intelligence Console

- Seamlessly integrated, single UI
- Includes new 'Forensics' dashboard tab
- Supports incident investigation workflow

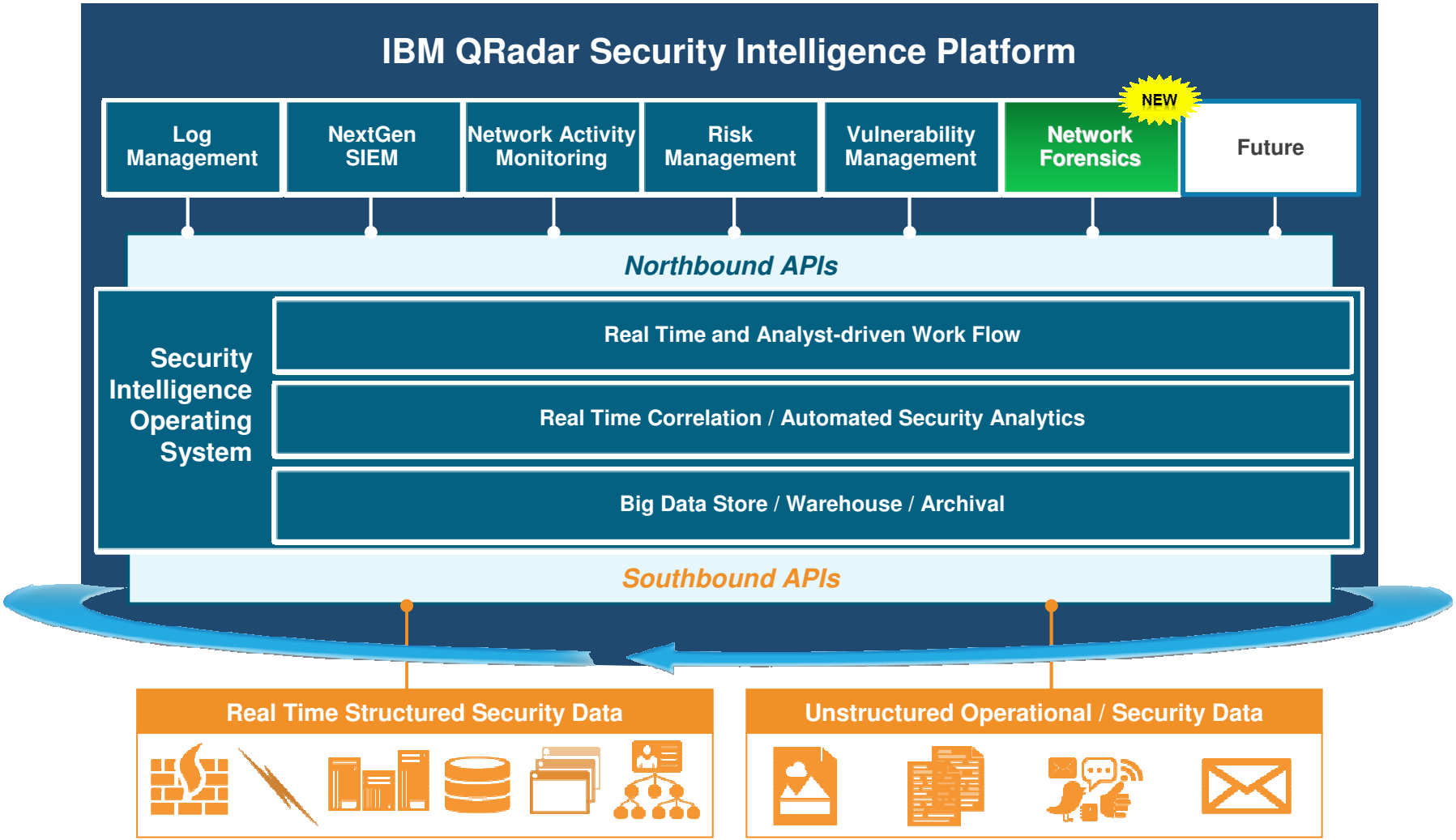
QRadar Incident Forensics Module

- Hardware, software, virtual appliance
- Supports standard PCAP format
- Retrieves PCAPs for an incident and reconstructs sessions for forensics

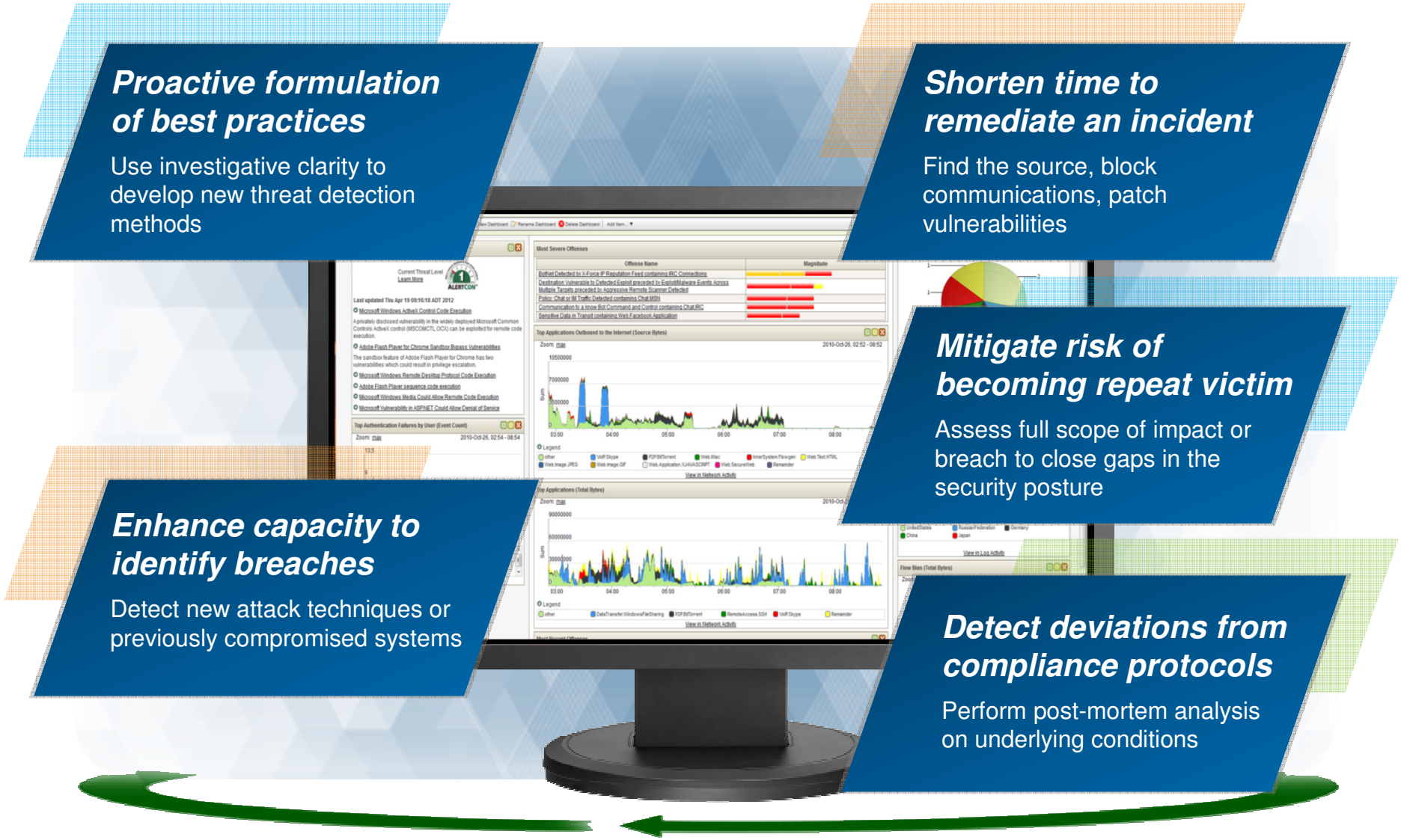
QRadar Packet Capture Appliances

- Performs Full Packet Capture
- Optimized appliance solution
- Scalable storage

Security Intelligence architecture provides continuity with total context



Clarity throughout the lifecycle of a security incident



Proactive formulation of best practices

Use investigative clarity to develop new threat detection methods

Shorten time to remediate an incident

Find the source, block communications, patch vulnerabilities

Mitigate risk of becoming repeat victim

Assess full scope of impact or breach to close gaps in the security posture

Enhance capacity to identify breaches

Detect new attack techniques or previously compromised systems

Detect deviations from compliance protocols

Perform post-mortem analysis on underlying conditions

Learn more about IBM Security Intelligence and Analytics

Visit the
IBM Security Intelligence Website

Watch the videos on the
IBM Security Intelligence YouTube Channel

Read new blog posts
SecurityIntelligence.com

Follow us on Twitter
@ibmsecurity

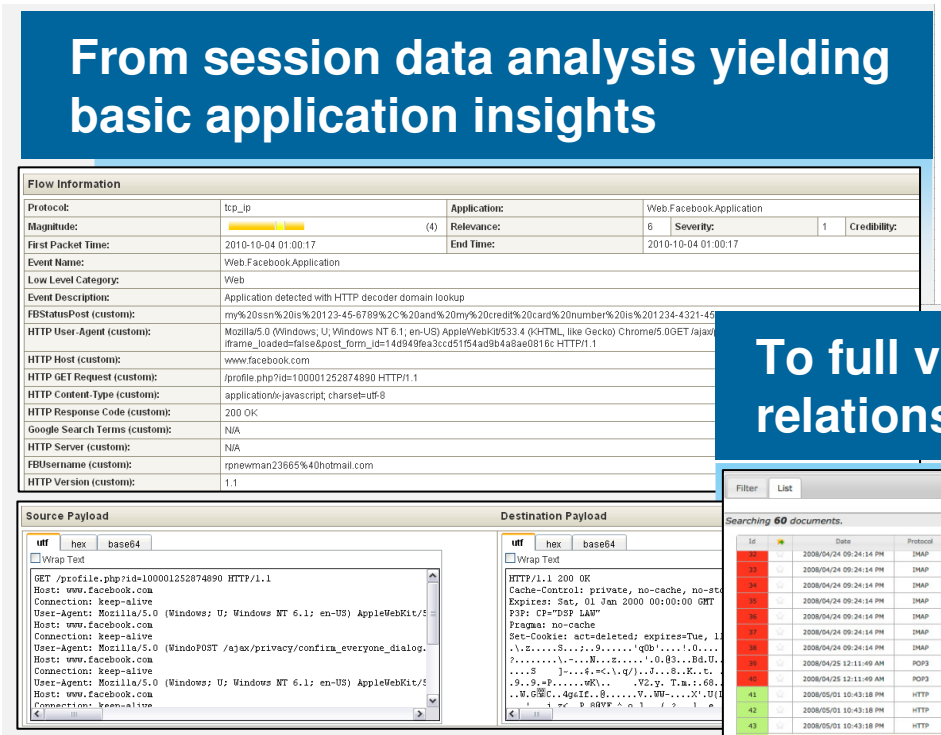
Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or 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

Better clarity into network activity

From session data analysis yielding basic application insights



Flow Information

Protocol:	tcp_ip	Application:	Web.Facebook.Application
Magnitude:	(4)	Relevance:	6 Severity: 1 Credibility:
First Packet Time:	2010-10-04 01:00:17	End Time:	2010-10-04 01:00:17
Event Name:	Web.Facebook.Application		
Low Level Category:	Web		
Event Description:	Application detected with HTTP decoder domain lookup		
FBStatusPost (custom):	my%20ssn%20is%20123-45-6789%2C%20and%20my%20credit%20card%20number%20is%201234-4321-45		
HTTP User-Agent (custom):	Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0 GET /ajax/ iframe_loaded=false&post_form_id=14d949fea3ccd51f54ad9b44a8ae0816c HTTP/1.1		
HTTP Host (custom):	www.facebook.com		
HTTP GET Request (custom):	/profile.php?id=100001252874890 HTTP/1.1		
HTTP Content-Type (custom):	application/x-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		

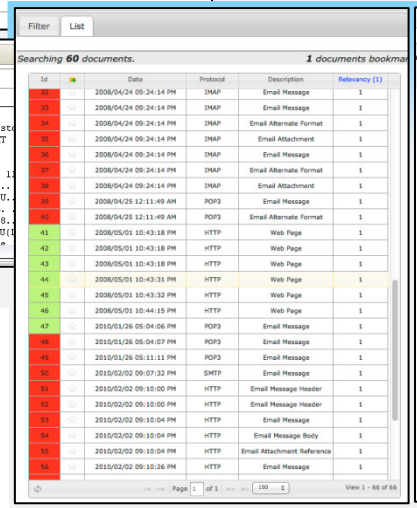
Source Payload / Destination Payload

utf | hex | base64 — Wrap Text

```
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/5
Host: www.facebook.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (WindoPOST /ajax/privacy/confirm_everyone_dialog.
Host: www.facebook.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/5
Host: www.facebook.com
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Cache-Control: private, no-cache, no-st
Expires: Sat, 01 Jan 2000 00:00:00 GMT
P3P: CP="DSP LAW"
Pragma: no-cache
Set-Cookie: act=deleted; expires=Tue, 1
```

To full visualization of extended relationships and embedded content



Filter | List — Searching 60 documents. 1 documents bookmar

Id	Date	Protocol	Description	Relevancy (1)
32	2008/04/24 09:24:14 PM	IMAP	Email Message	1
33	2008/04/24 09:24:14 PM	IMAP	Email Message	1
34	2008/04/24 09:24:14 PM	IMAP	Email Alternate Format	1
35	2008/04/24 09:24:14 PM	IMAP	Email Attachment	1
36	2008/04/24 09:24:14 PM	IMAP	Email Message	1
37	2008/04/24 09:24:14 PM	IMAP	Email Alternate Format	1
38	2008/04/24 09:24:14 PM	IMAP	Email Attachment	1
39	2008/04/25 12:11:49 AM	POP3	Email Message	1
40	2008/04/25 12:11:49 AM	POP3	Email Alternate Format	1
41	2008/05/01 10:43:18 PM	HTTP	Web Page	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 05:11:11 PM	POP3	Email Message	1
50	2010/02/02 09:07:32 PM	SMTP	Email Message	1
51	2010/02/02 09:10:00 PM	HTTP	Email Message Header	1
52	2010/02/02 09:10:00 PM	HTTP	Email Message Header	1
53	2010/02/02 09:10:04 PM	HTTP	Email Message	1
54	2010/02/02 09:10:04 PM	HTTP	Email Message Body	1
55	2010/02/02 09:10:04 PM	HTTP	Email Attachment Reference	1
56	2010/02/02 09:10:26 PM	HTTP	Email Message	1

Better clarity into user identities

From standard asset identity information

Attacker Summary	Details		
Magnitude		User	dwight.spencer
Description	10.100.50.21	Asset Name	
Vulnerabilities	0	MAC	
Location	Server_Network.Server_Network	Asset Weight	

To rich visualizations of digital impressions showing extended relationships