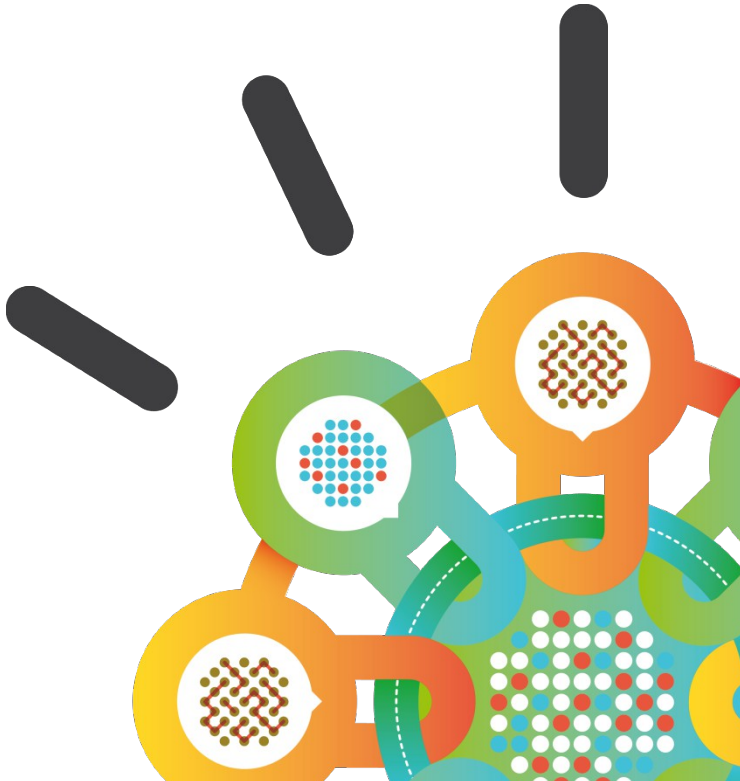
IBM

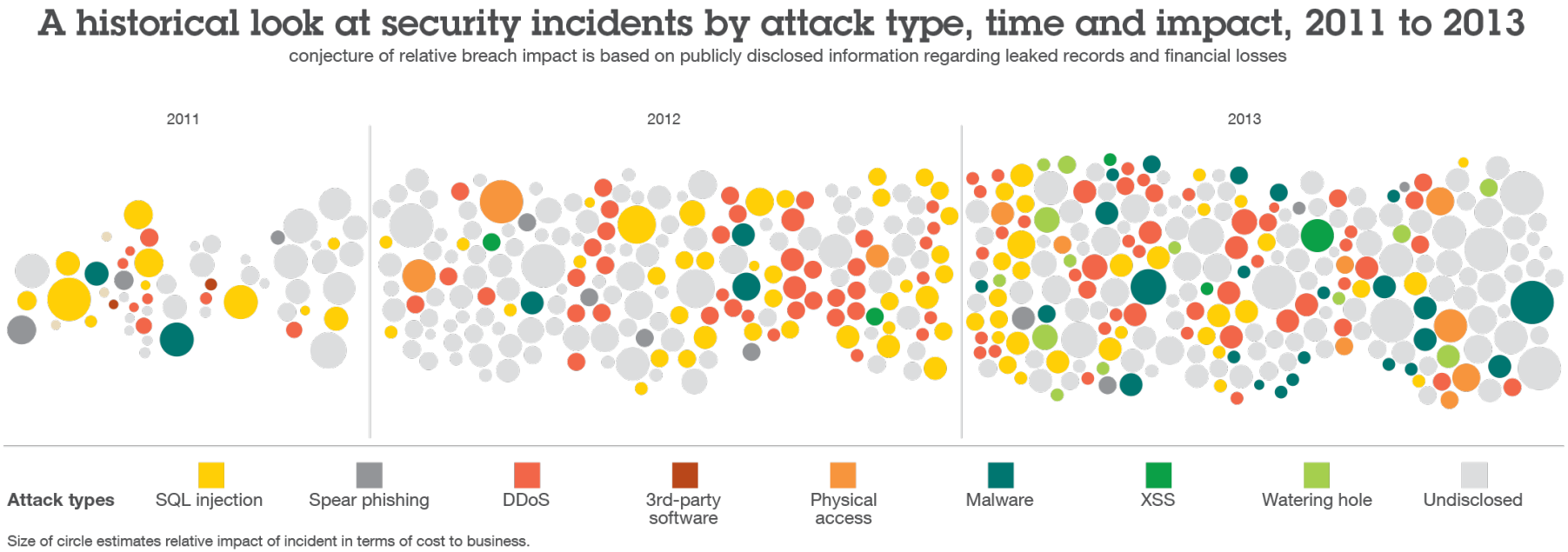
Security Intelligence.
Think Integrated.

# Attain Clarity of Your Security Posture with Enhanced Incident Forensics Capabilities

April 2014



# Reported attacks continue to increase



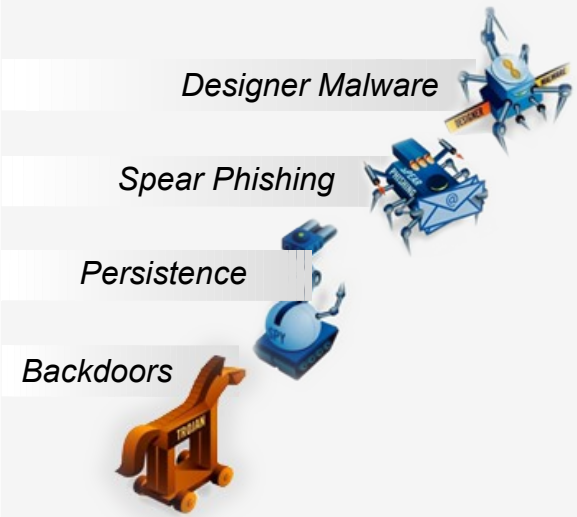

**500,000,000+ Billion records**

of personally identifiable information (PII) were leaked in 2013

Source: IBM X-Force® Research 2013 Trend and Risk Report

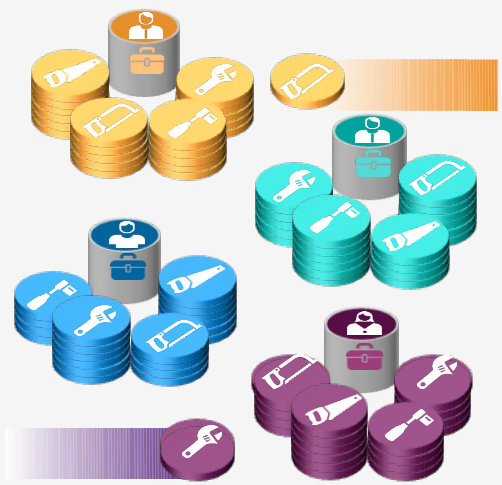
# Today's challenges

## Escalating Attacks




- Increasingly sophisticated attack methods
- Disappearing perimeters
- Accelerating security breaches

## Increasing Complexity



- Constantly changing infrastructure
- Too many products from multiple vendors; costly to configure and manage
- Inadequate and ineffective tools

## Resource Constraints


- Struggling security teams
- Too much data with limited manpower and skills to manage it all
- Managing and monitoring the increasing regulatory compliance demands

# Some examples of what a typical enterprise has to deal with

200,000+ face book, twitter, linked-in etc accesses a day

500+ files uploaded to internet sites a day

2,000+ files a day downloaded from the internet

30% of network use is remote

2 laptops a week go AWOL

20 new IT assets a week

10000+ SPAM/Fishing emails a week

External network scanned 50 times a day

100,000+ vulnerabilities in the network

5 network alerts per minute

100+ potentially malicious web site visits per day

20 Network configuration changes a week

# A Clear & Present Threat…

**Attackers spend** an estimated **243 days on a victim's network** before being discovered

In 2013, it took organizations **32 days** on average **to resolve a cyber-attack**

In 2012, **38%** of targets were **attacked again** once the original incident was remediated.

**63%** of victims **made aware** of their breaches **by an external organization**

**Annual cost of cyber-crime** in the U.S. now stands at **$11.56 million per organization**

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?

3

# When responding to incidents, every second is precious

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

**Difficulty identifying true incidents hidden in mounds of data**


Determining where to begin a forensics investigation leads to lost productivity and time-intensive ad-hoc analysis

**Inability to quickly retrace and analyze incidents without starting over**

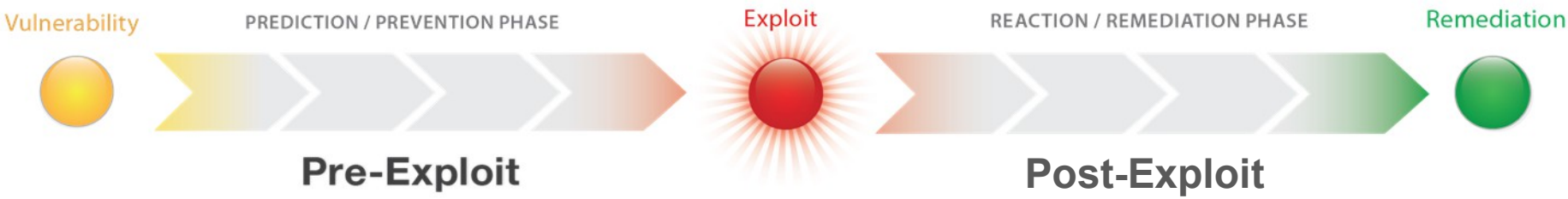
Lack of an integrated “security camera” leaves critical gaps in quickly understanding key elements of the attack

**Dependency on specialized skills to conduct detailed investigations**


Technically skilled analysts required to drive network forensics security investigations

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

# The Lifecycle of a Cyber Threat




## Prediction & Prevention

- Gain Visibility Over the Organization's Security Posture
- Detect Deviations from the Norm and Initiate Preventive Procedures
- Attain Awareness of Vulnerabilities and Assess Exposures

## Reaction & Remediation

- Discover Anomalies and Investigate to Evaluate the Risk
- Explore and Analyze Data to Devise Countermeasures for the Attack
- Formulate New Security Best Practices to Adapt to Emerging Threats

# Embedded intelligence offers automated offense identification

## Extensive Data Sources

- Security devices
- Servers and mainframes
- Network and virtual activity
- Data activity
- Application activity
- Configuration information
- Vulnerabilities and threats
- Users and identities
- Global threat intelligence

## Automated Offense Identification

- Unlimited data collection, storage and analysis
- Built in data classification
- Automatic asset, service and user discovery and profiling
- Real-time correlation and threat intelligence
- Activity baselining and anomaly detection
- Detects incidents of the box

# Extending the embedded intelligence of QRadar to deliver high clarity around incident investigations

# Why IBM Security 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

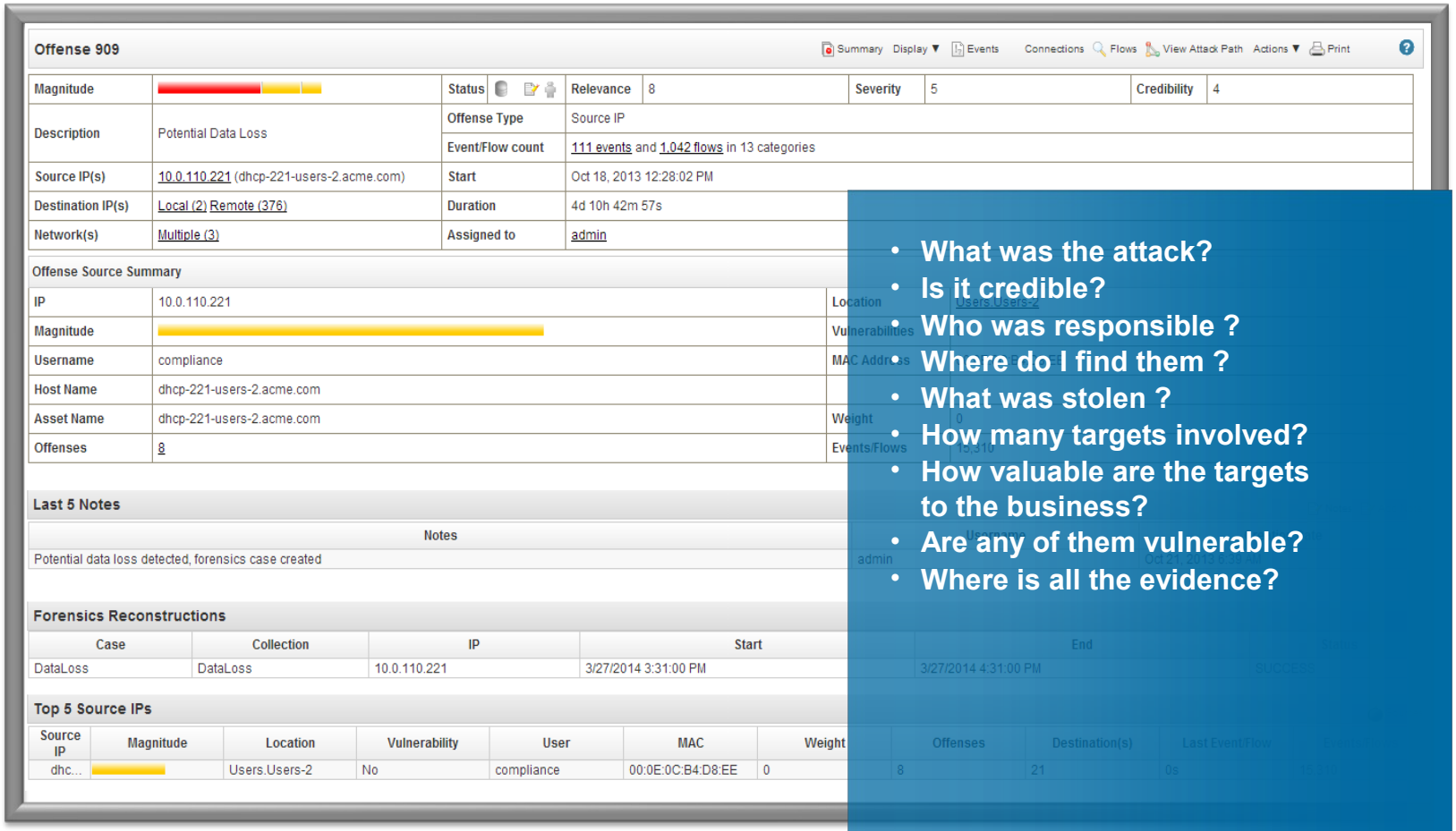
**4 Builds Intelligence**

- Automated detection and assembly of identities
- Automated detection of suspicious content/activity
- Content categorization informs data exclusion
- Reveals linkages between entities

**5 Enables Intuitive Investigative Analysis**

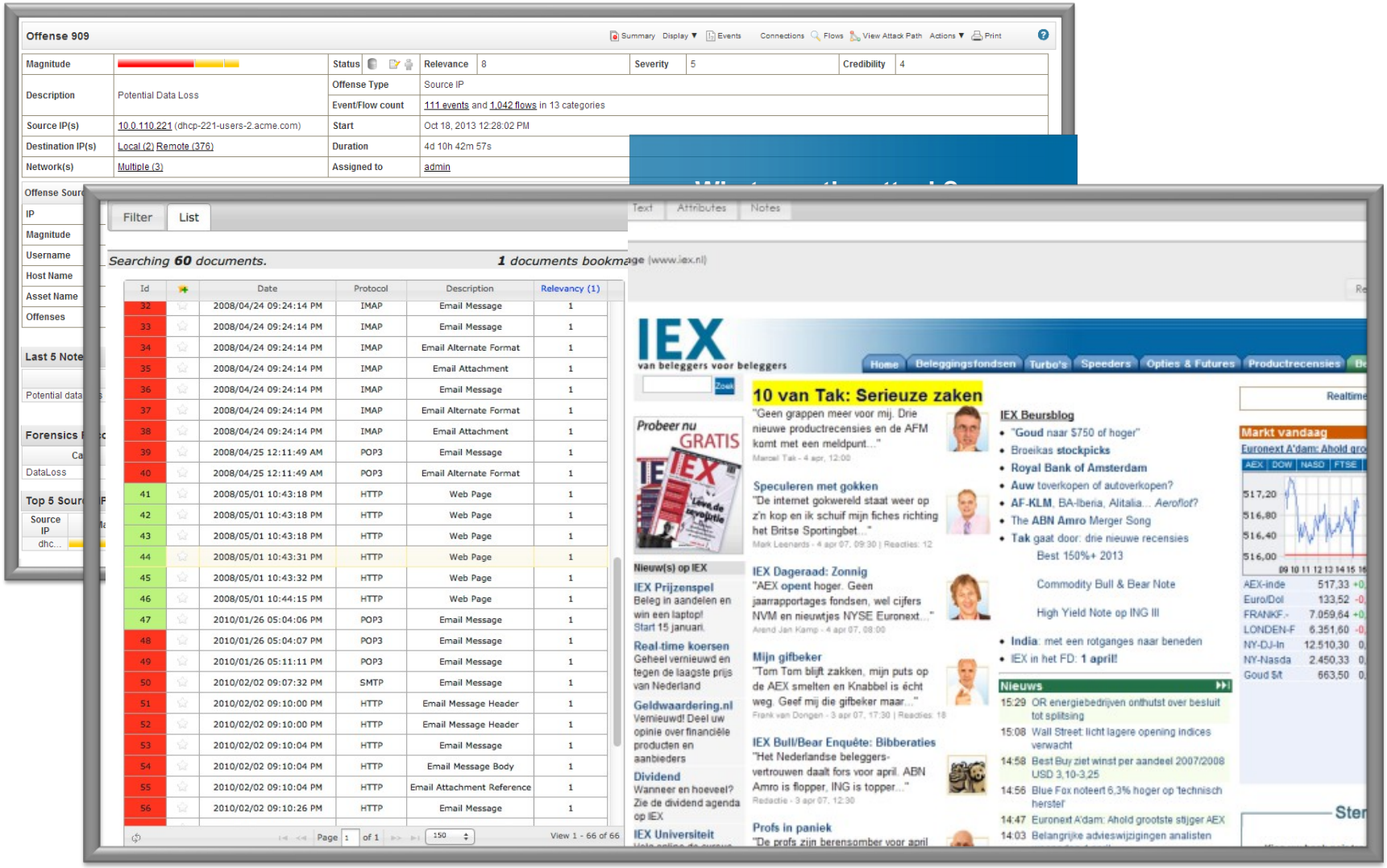
- Simple search engine interface
- Visual analytics
- Retrace activity in chronological order with reconstructed content

# Answering questions to help prevent and remediate attacks




- What was the attack?
- Is it credible?
- Who was responsible ?
- Where do I find them ?
- What was stolen ?
- How many targets involved?
- How valuable are the targets to the business?
- Are any of them vulnerable?
- Where is all the evidence?

# Incident Forensics tell you what happened

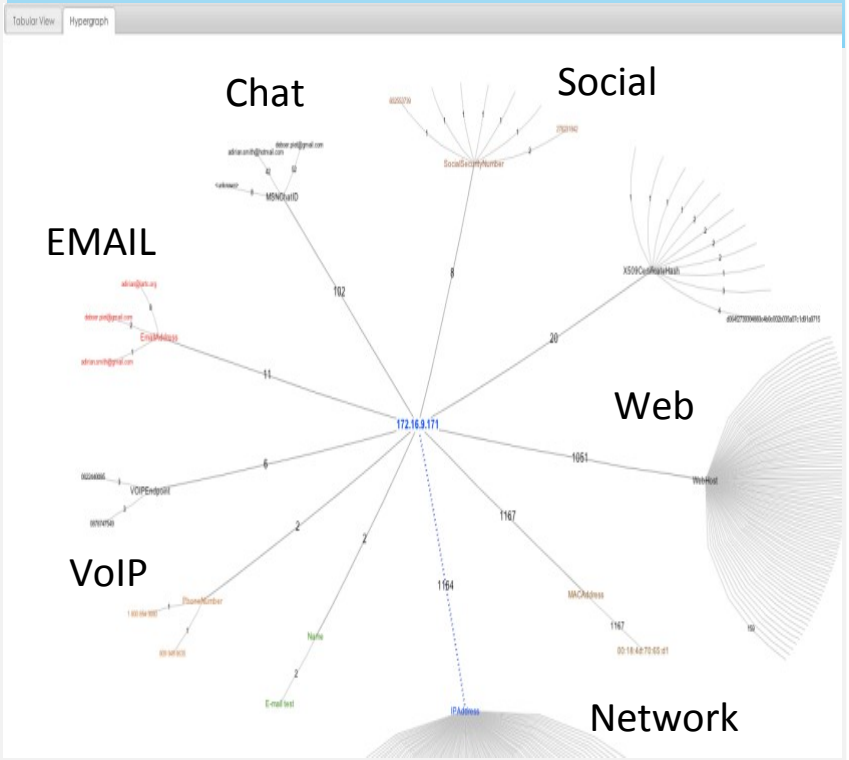


# And who was involved …

## From Asset Identity

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

## To Full Identity Trail Relationship Awareness & Context



# How Network Forensics is Done…

## Full Packet Capture

- Capture packets off the network
- Next-generation solutions enable ingestion of other structured and unstructured content

## Retrieval & Session Reconstruction

- For a security incident retrieve all the packets (time bounded) and re-assemble the packet data to get visibility of the content of the conversation(s) that transpired during that incident

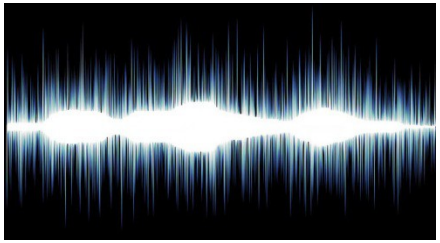
## Forensics Activity

- Navigate information to uncover knowledge of threats

The phase that delivers the greatest operational value to security analysts, empowering them to gain clarity of a security incident

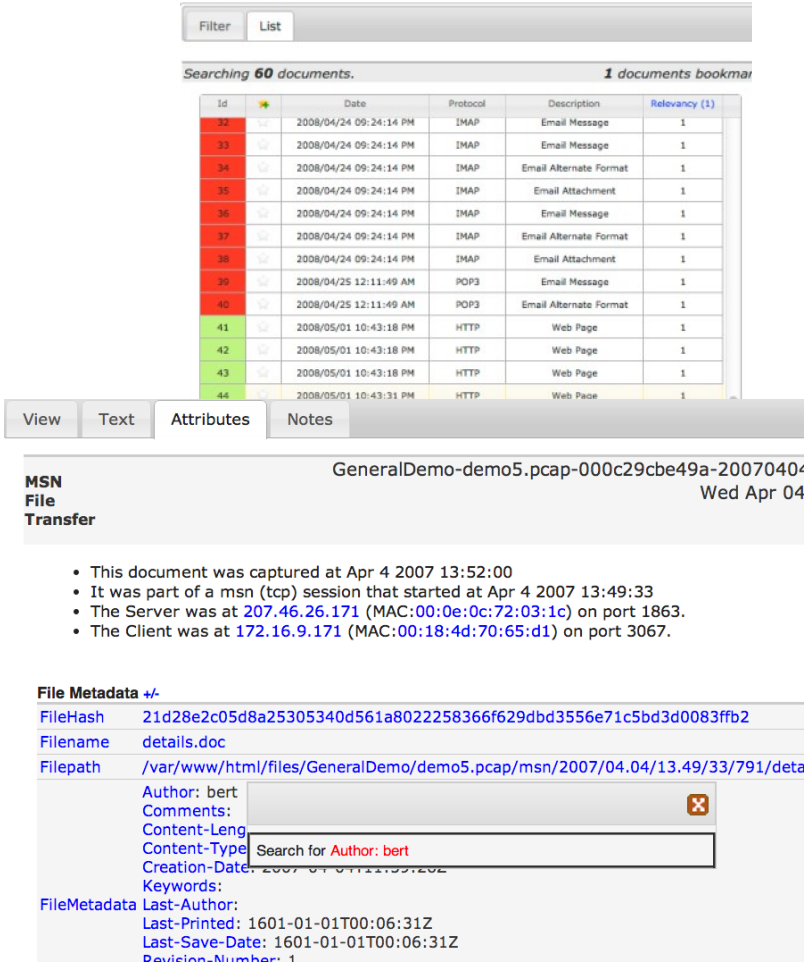
# QRadar Incident Forensics delivers ***High Fidelity*** forensics and comprehensive situational awareness

- Ingests PCAPs, XML files and <u>documents or archives</u> converting and storing everything in rich document format
- Applies search engine technology to highly indexed, file-based store using multiple types of metadata:
  - Network metadata
  - File metadata
  - Identity metadata
- Returns detailed, multi-level search results in seconds

# Making forensics fast and clear - Intuitive Data Exploration and Navigation

- Empower security analysts to operate like seasoned forensics specialists by offering capabilities that can be powered by intuition and logical deduction
- **Surveyor:** Retrace the activities in a chronological order
- **Searchable Results:** Quickly pivot on data items to go where the data takes you
- **Visual Analytics:** Navigate the data using visual indications of correlations between data items



# IBM Security QRadar Incident Forensics deployment model

## QRadar Security Intelligence

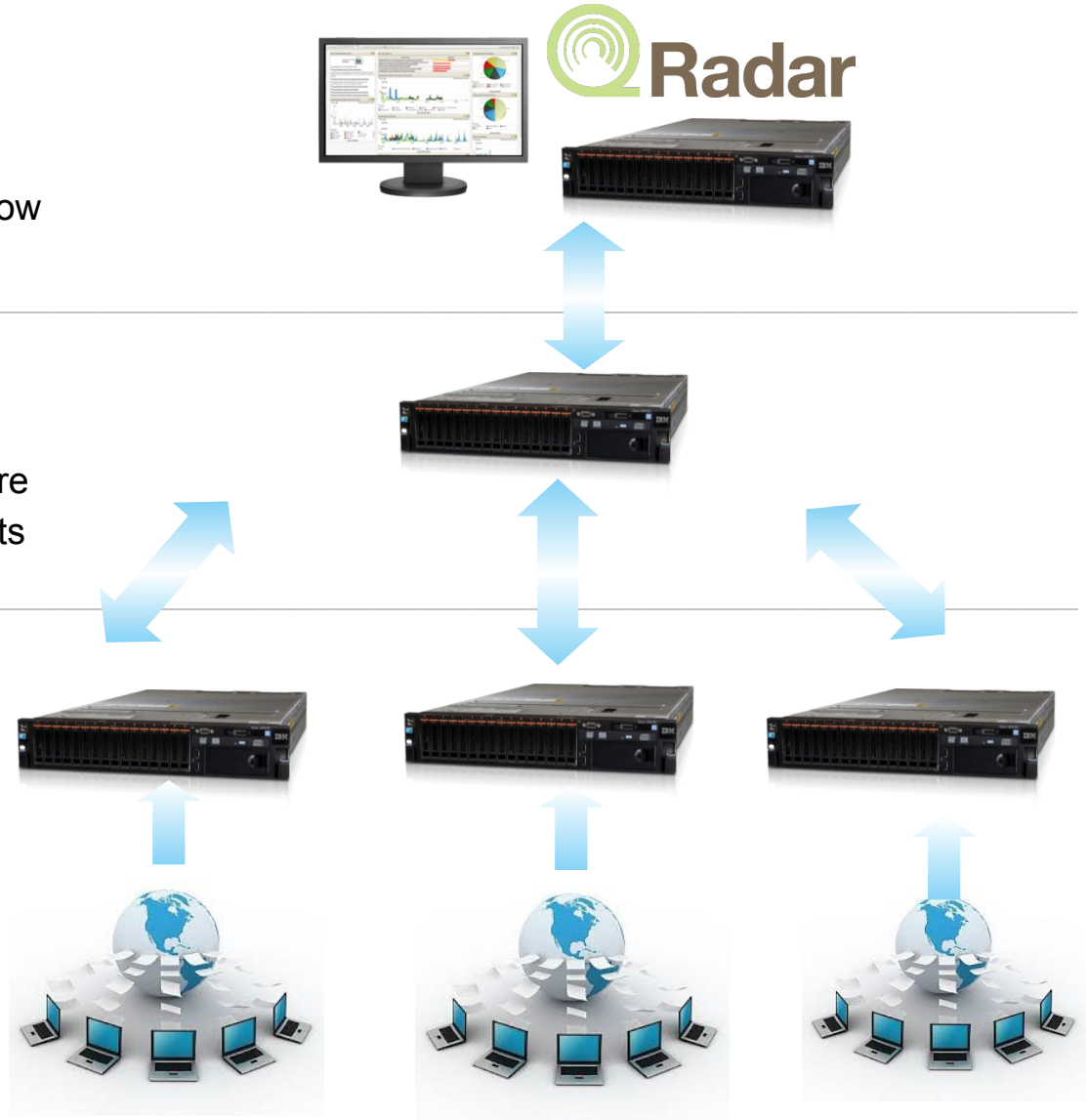
- Seamlessly integrated, single UI
- New ‘Forensics Tab’
- Supports incident investigation workflow

## QRadar Incident Forensics

- Scalable storage
- Appliance, virtual appliance or software
- Integrates with standard PCAP formats

## QRadar Packet Capture

- Up to 10Gb/s
- 2U, 20 Core, 128GB ram
- Scalable storage options
  - 40TB -> 90 TB -> 100’sTB
  - 1 day -> Week’s-> Month’s
- 1 to N Appliances



# Next generation network forensics: know what happened, fast

**Our Security Intelligence platform delivers powerful capabilities to limited IT security resources**

## 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 SIEM, leveraging the accuracy of built-in security analytics to discover true offenses
- Applies search engine technology to a highly-indexed, file-based store using multiple types of metadata
- Returns detailed, multi-level search results in seconds

### Allows you to quickly Retrace full incident activity

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

### Provides assistance with navigating investigations

- Visually construct threat actor relationships - helping answer what the entity is, and with whom and how it communicates
- Builds detailed user and application profiles helping discover extended relationships across multiple IDs

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**