



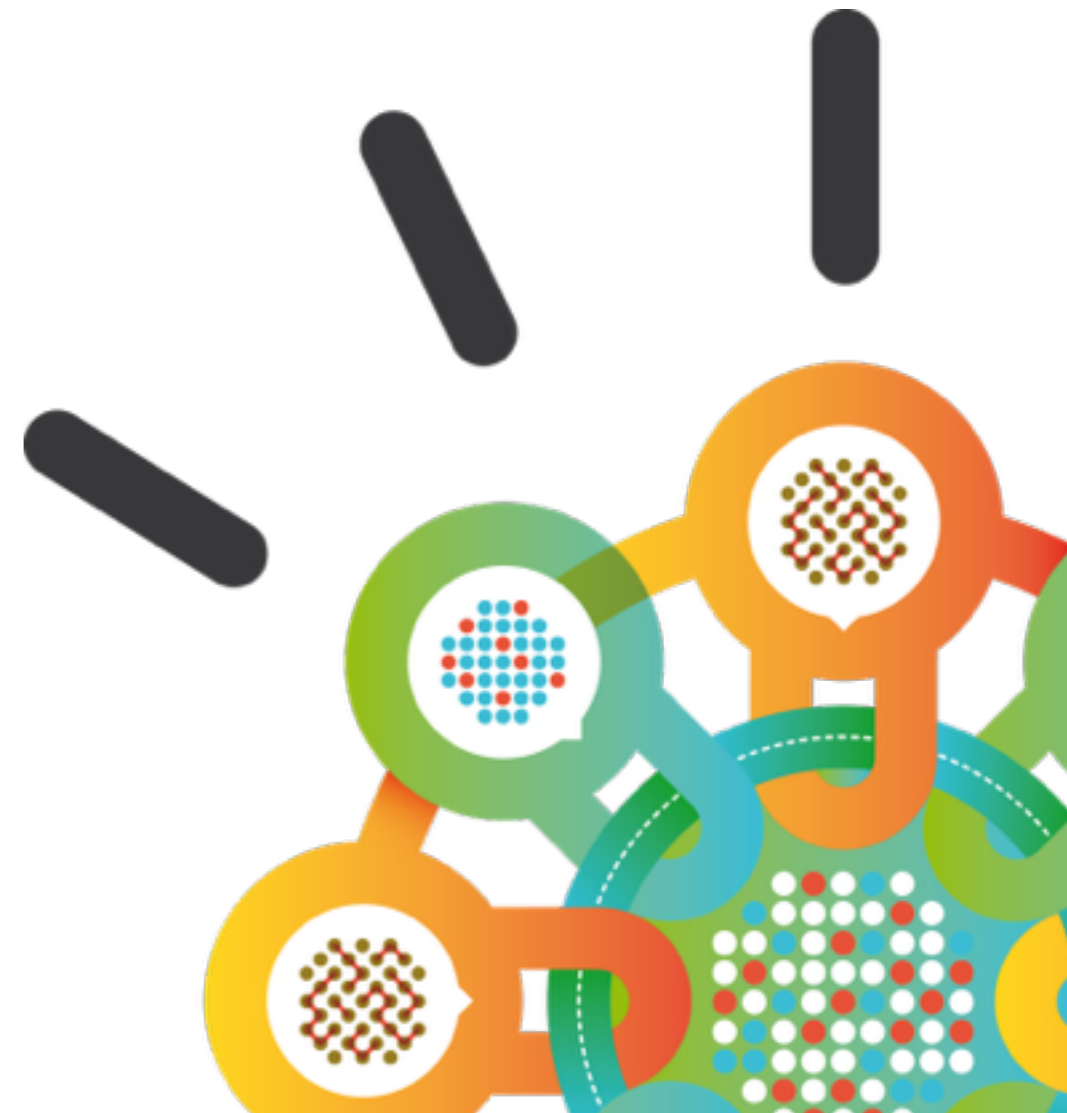
everything you have seen here has been an illusion.

Security Intelligence.
Think Integrated.

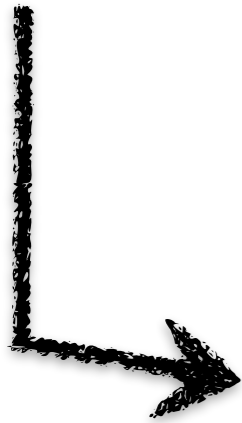
IBM QRadar SIEM

Freestyle presentation

Andrzej Wojtkowiak
IBM Security IT Specialist for Central & Eastern Europe



Why We have problems ???



EVERYTHING IS EVERYWHERE

Organizations continue to move to new platforms including cloud, virtualization, mobile, social business and more



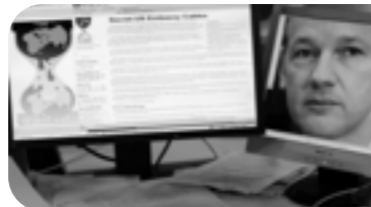
CONSUMERIZATION OF INFRASTRUCTURE

With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data has disappeared



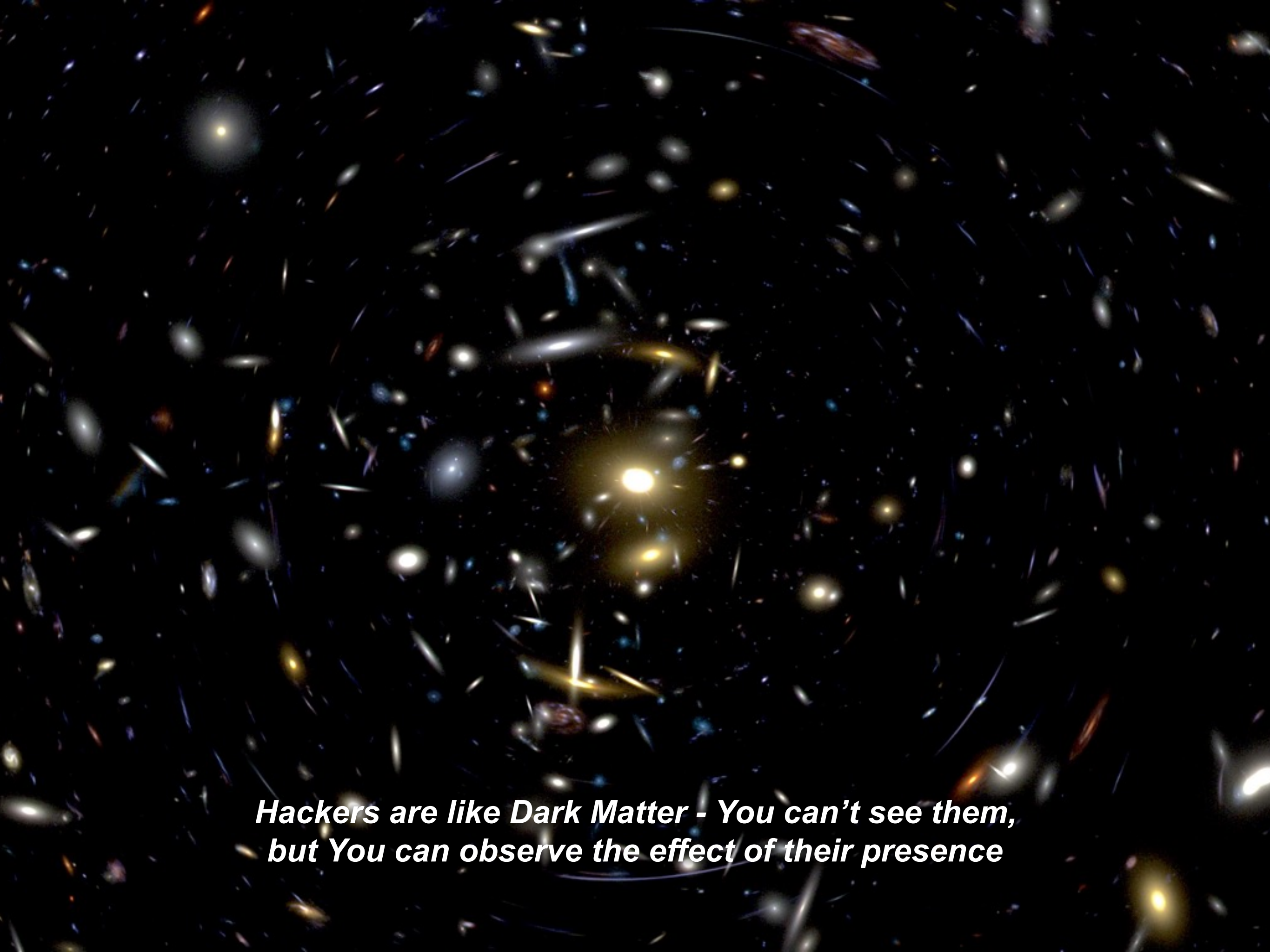
DATA EXPLOSION

The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere



ATTACK SOPHISTICATION

The speed and dexterity of attacks has increased coupled with new motivations from cyber crime to state sponsored to terror inspired

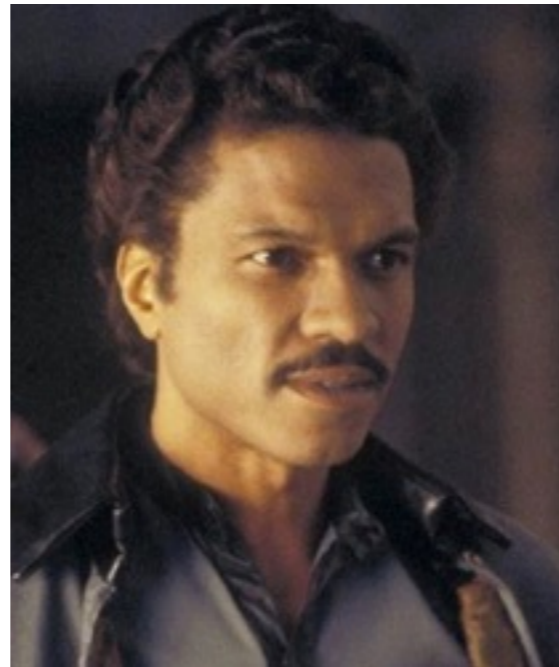


***Hackers are like Dark Matter - You can't see them,
but You can observe the effect of their presence***

With whom we are fighting with ???



Criminals



Insiders



Motivated Actors

\$ \$ \$

REWARD

\$ \$ \$

What is their motivation ???

- **\$**

- **Intellectual Property** →

\$ \$

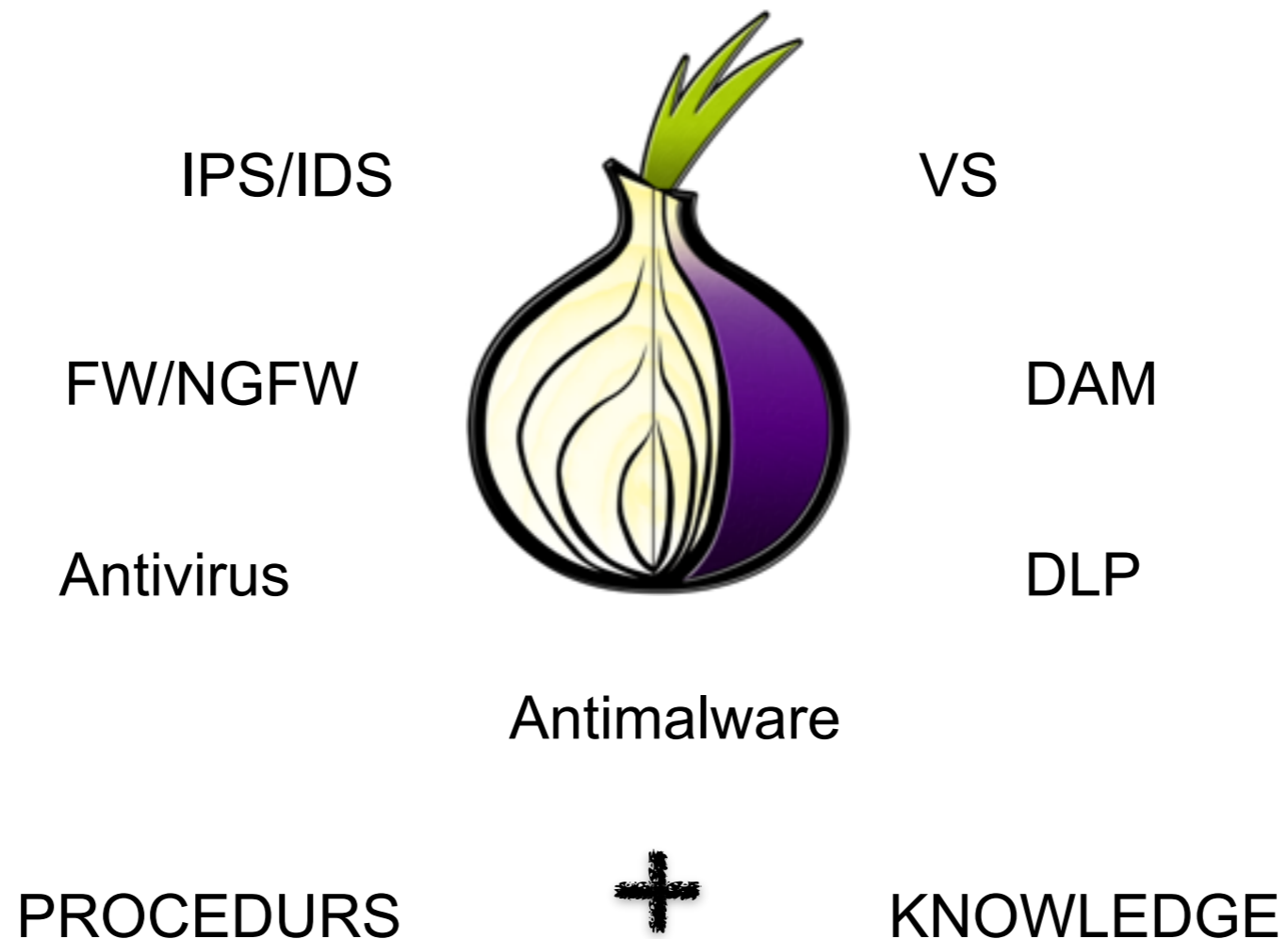
- **Personal Information** →

\$ \$ \$

How do I protect ???



Security is like an onion it has got layers



Security is like an onion



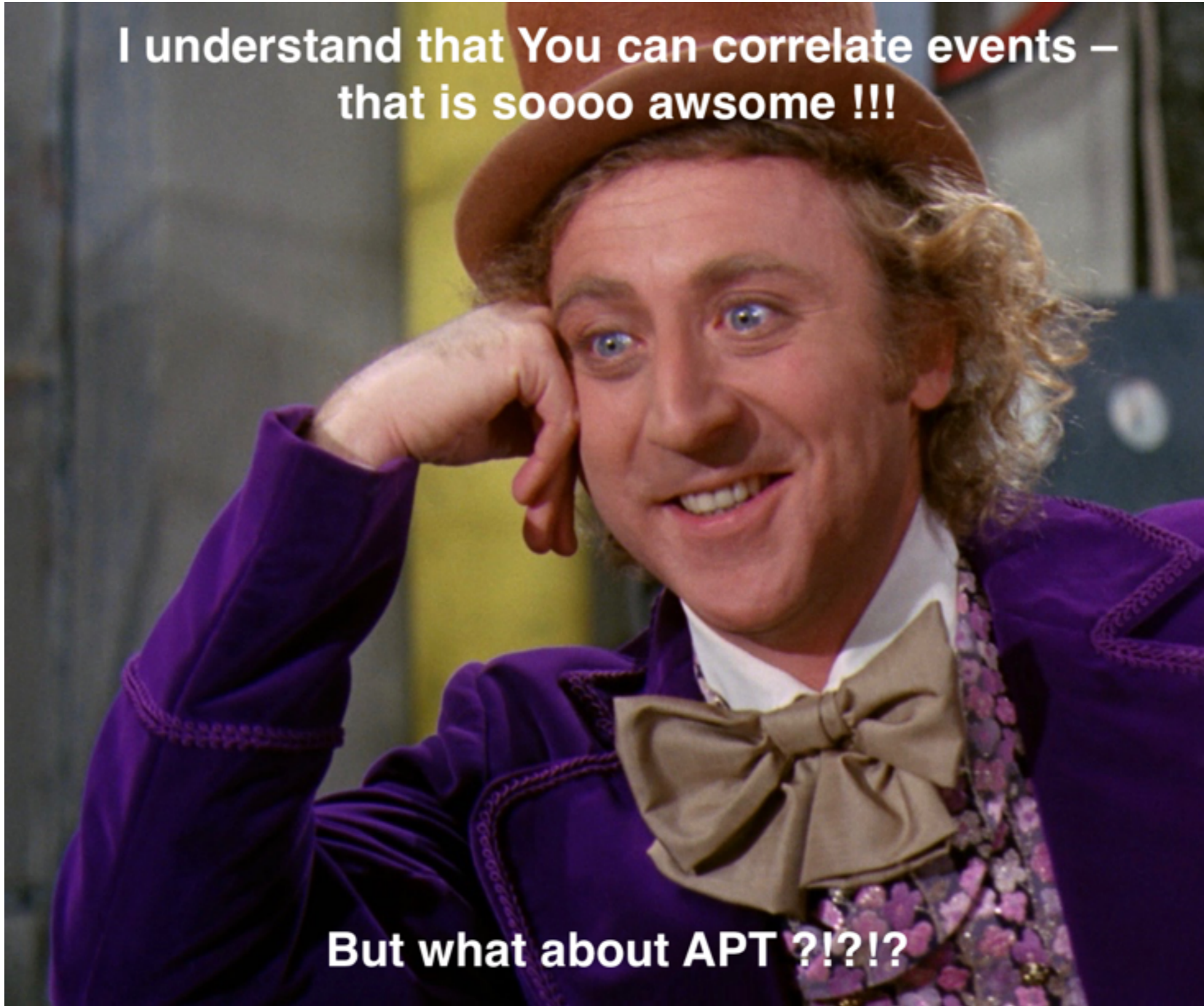
.... it can make You cry

Typical definition of SIEM

Security Information and Event Management (SIEM) is to build understandable logic from the events in a real time to detect security incidents

**I understand that You can correlate events –
that is soooo awsome !!!**

But what about APT ?!?!?

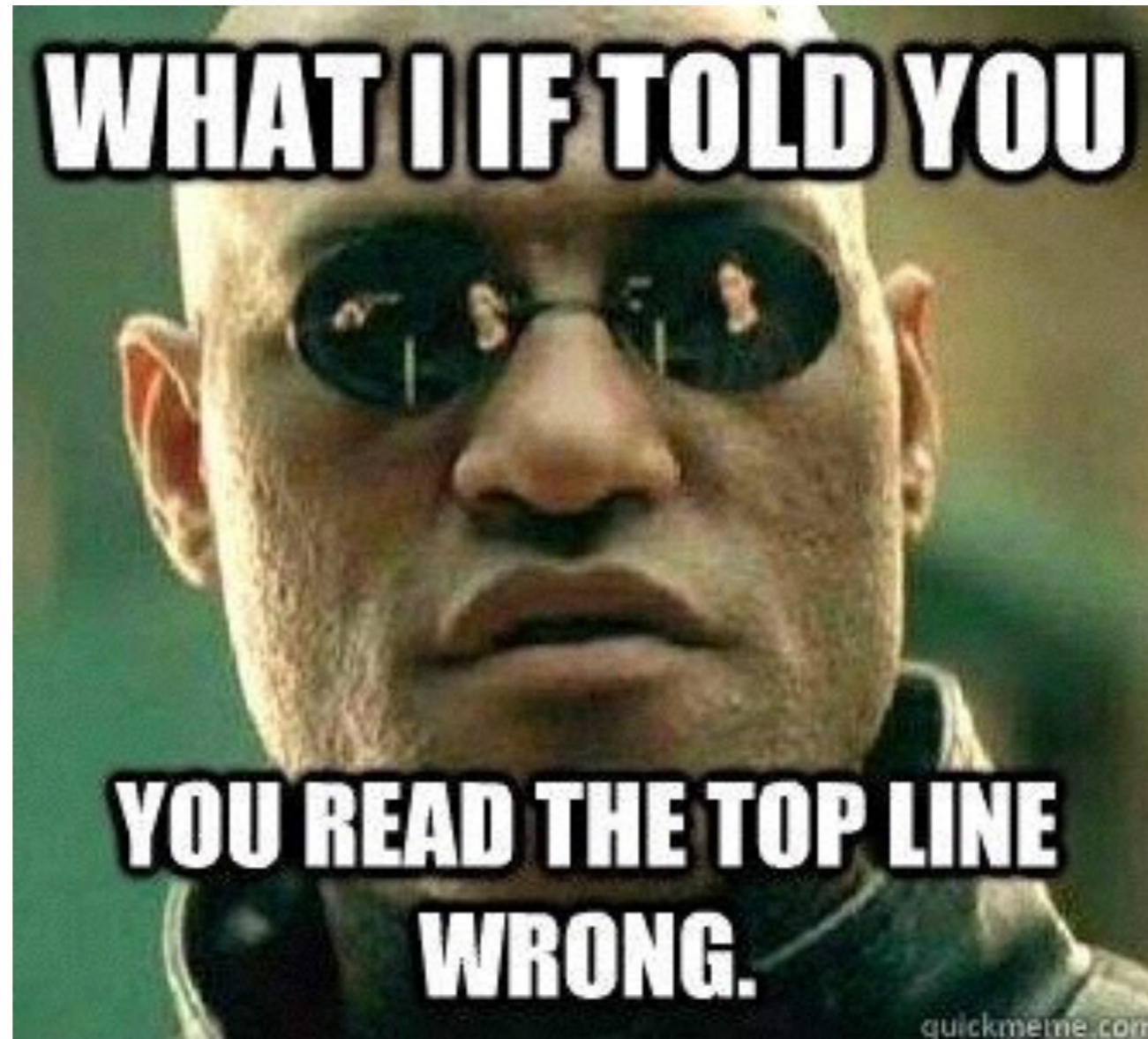




APT? - What does it mean?

No one knows what it means, but it's provocative!
It gets the people GOING !!!

Advanced Persistent Threat is to fake You



Advanced Persistent Threat - the „invisible" attacks

1

Advanced

- *Use vulnerabilities that were not revealed yet (Zero Days) ← NO LOGS...
- *Advanced malware specially crafted for dedicated attack ← WRONG LOGS...
- *Use coordination of different attack vectors - pretended attacks ← ...I STILL KNOW WHAT YOU DID LAST SUMMER...
- *OSINT - Open Source Intelligence espionage ←

2

Persistent

- *Attacks that last months & years
- *Attacks highly motivated to get data.... until they get it! ← NO RAMBO STYLE...

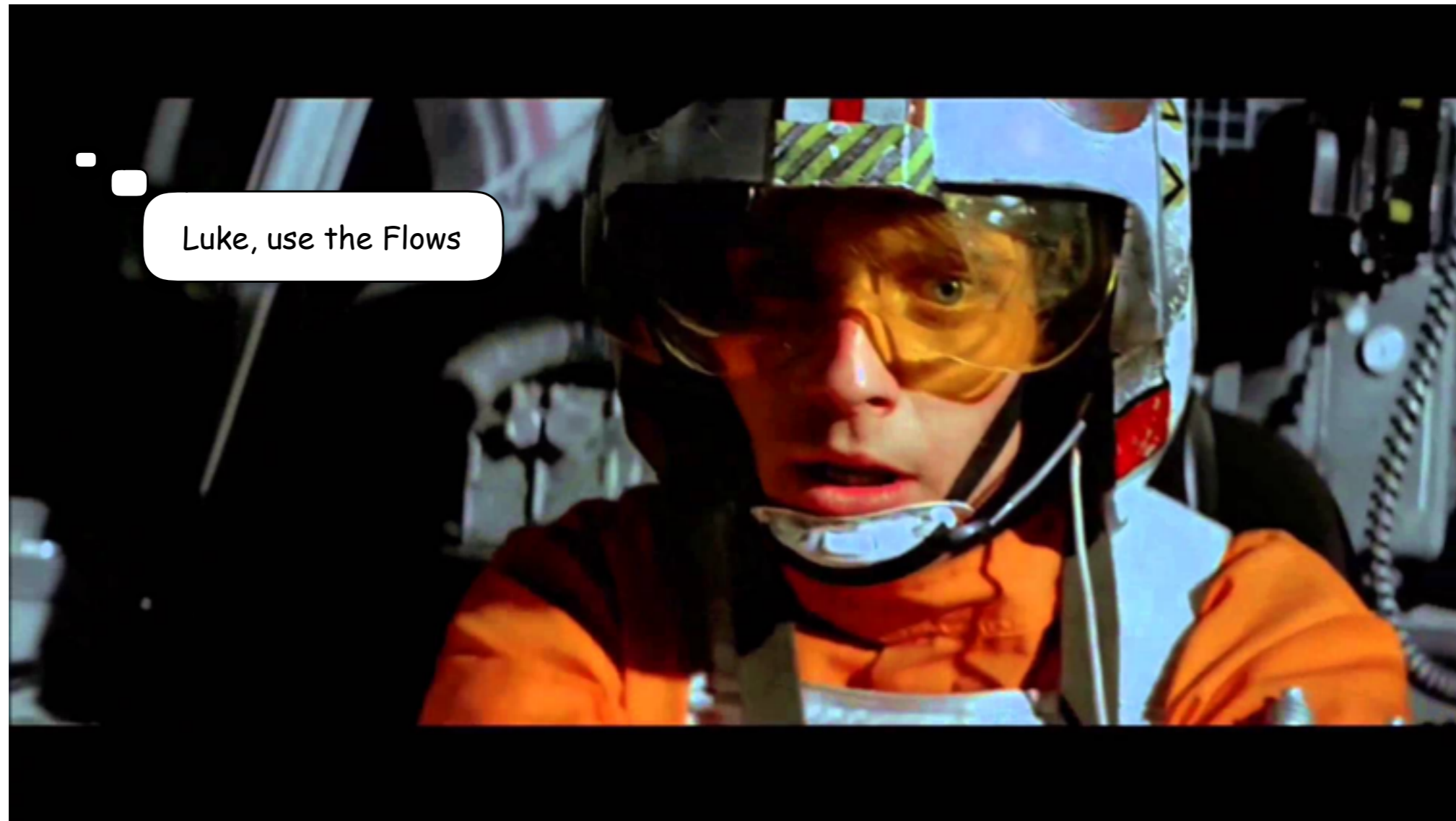
3

Threat

- *Attacks that are targeted to carefully selected individual identities inside organization
- *Carefully selected attacks



Advanced Persistent Threat



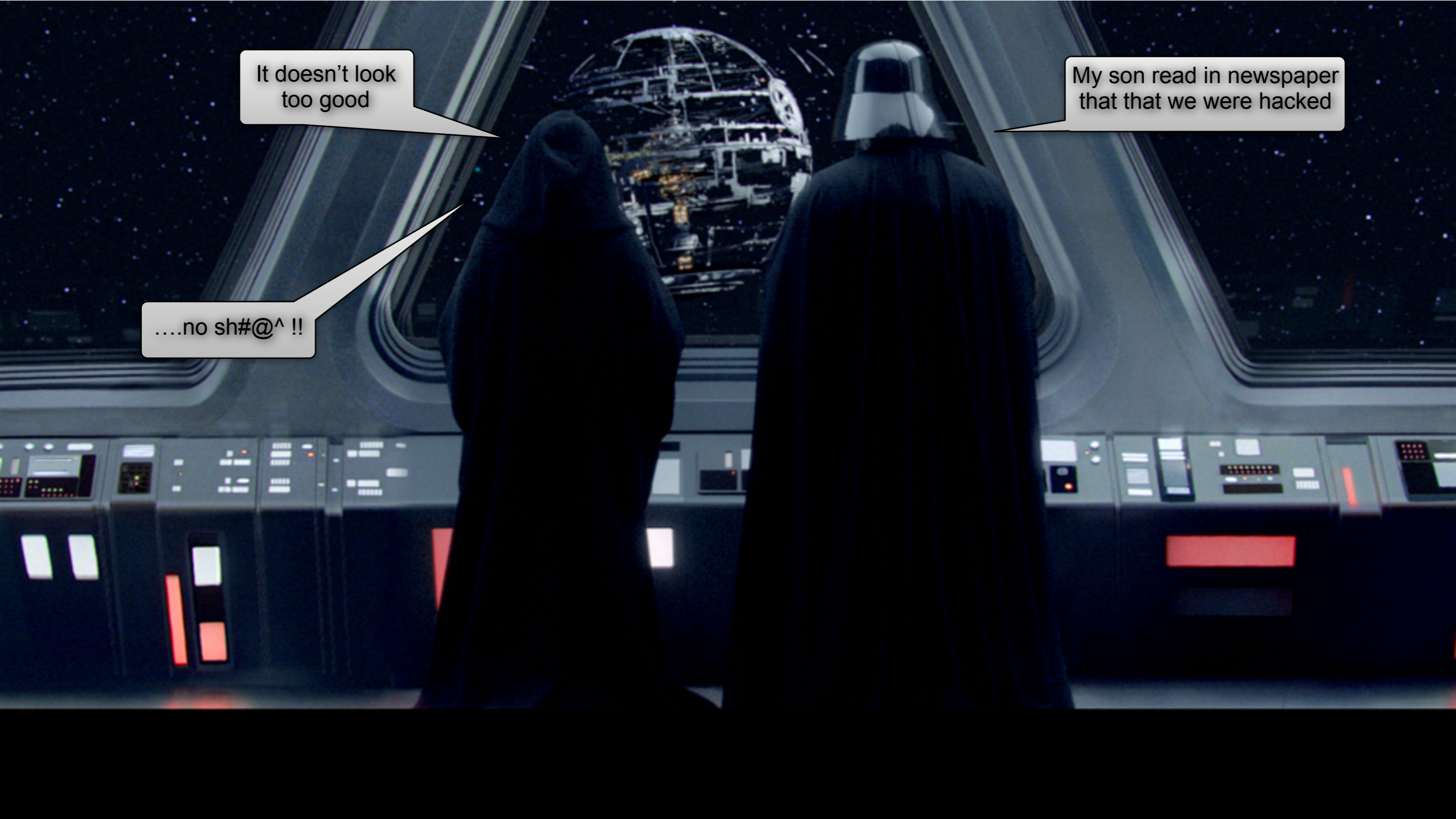
You can't simply detect APT, You can observe the symptoms of APT attacks by monitoring anomalies in the network traffic

How fast we will discover this?

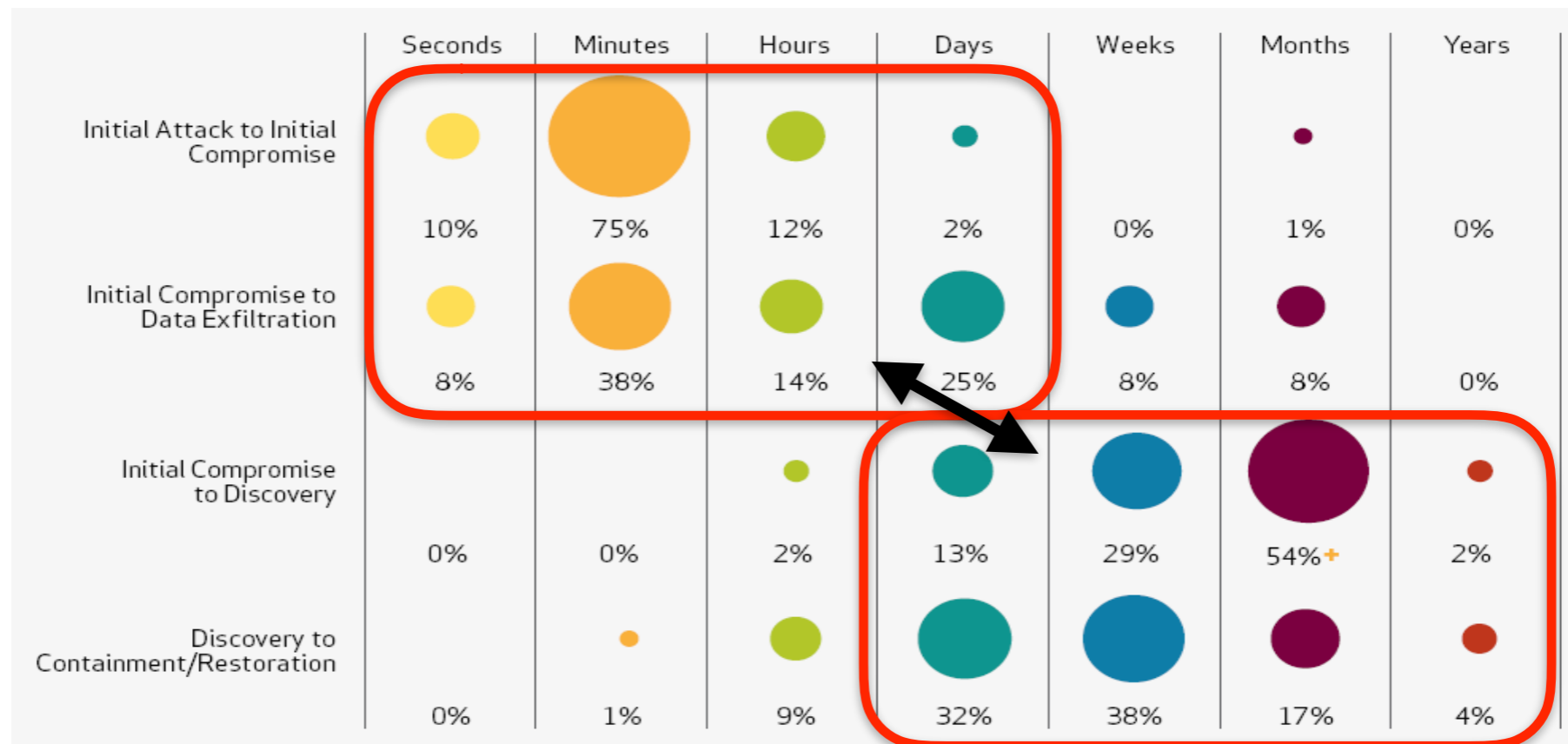
It doesn't look too good

My son read in newspaper that that we were hacked















....no sh#@^ !!



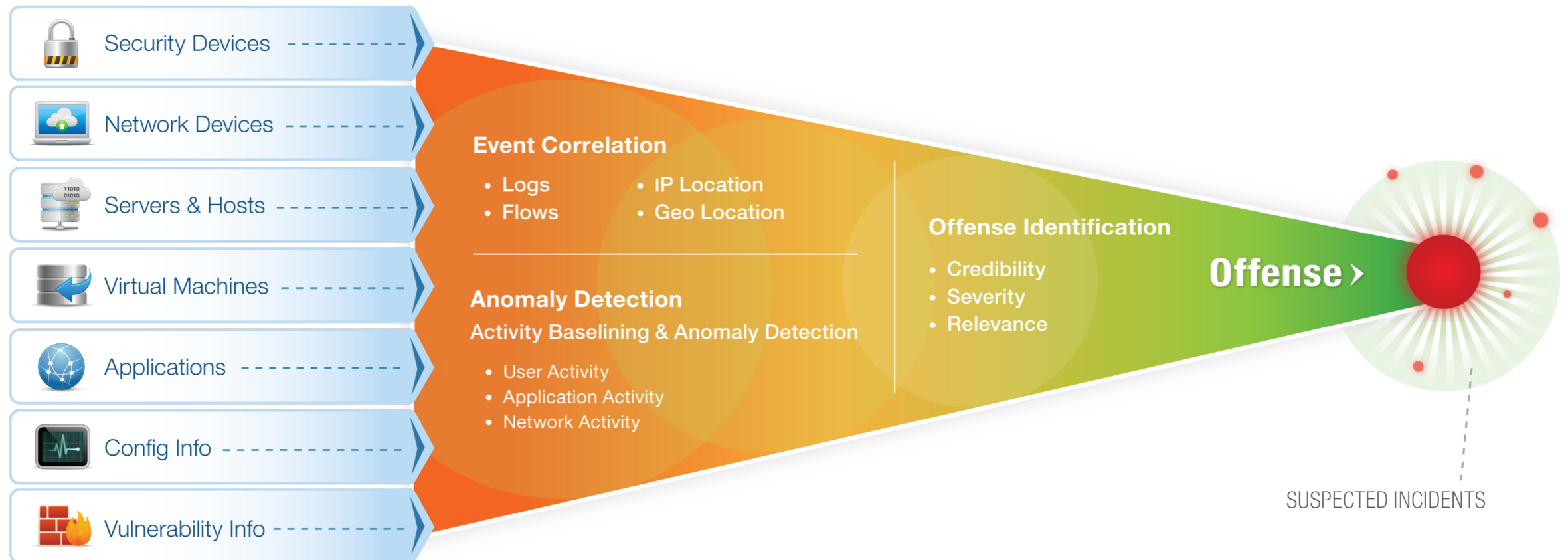
This is the role of SIEM



QRadar SIEM and MODULES

Log Management	 	<ul style="list-style-type: none"> • Full log management • Simple migration from LM to full SIEM by change in license
SIEM	 	<ul style="list-style-type: none"> • Correlation of log, flow, vulnerability & identity data • Automatic asset profiler • Full incident management
Risk & Vulnerability Management	  	<ul style="list-style-type: none"> • Simulate potential attacks • Full network scanner • Monitoring of network configuration
Network and Application Visibility	   	<ul style="list-style-type: none"> • Full network analyze up to 7 Layer • Build network characteristics and identify anomalies • Ability to analyze traffic in virtual environment
Network Forensic	 	<ul style="list-style-type: none"> • Full forensic based on packet capture • Precise proof, who did what, when and how!
Scalability		<ul style="list-style-type: none"> • Event Processors & Flow Processors • Network characteristics analysis • High Availability & Disaster Recovery • Full scalability

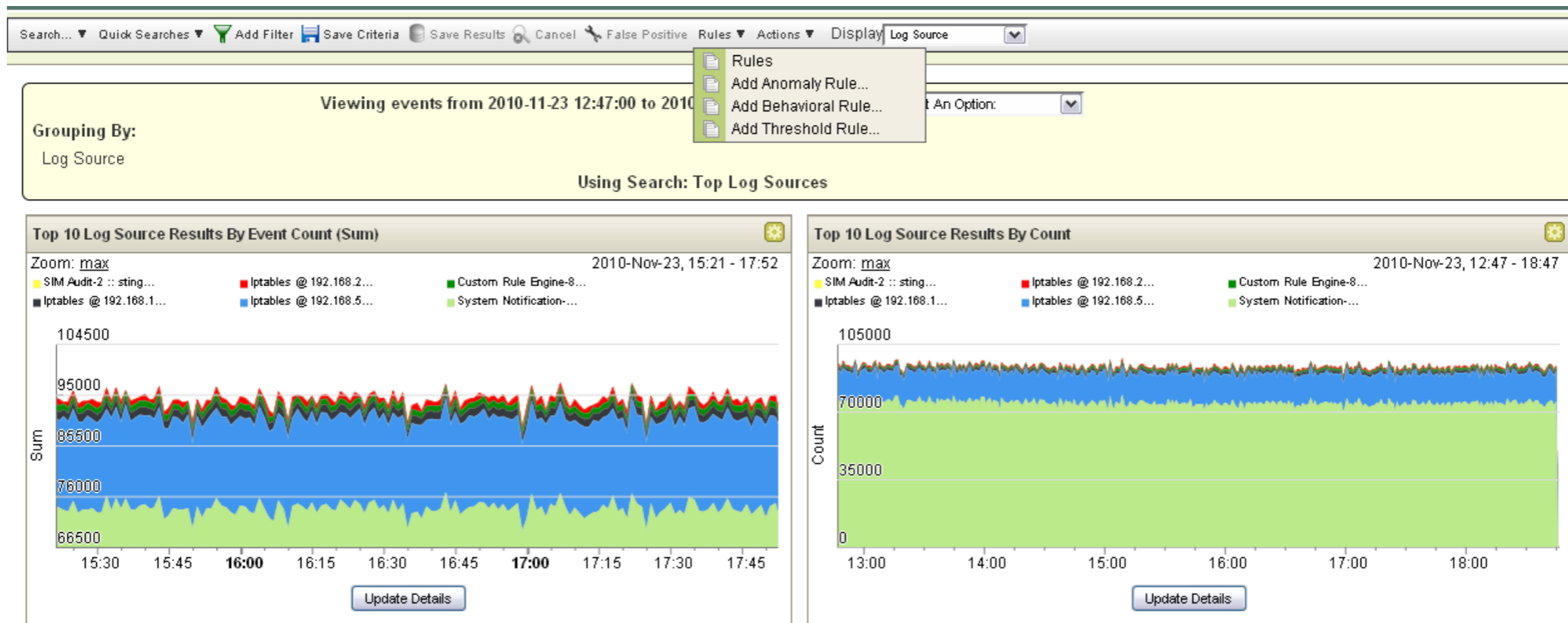
How IBM QRadar works ?



- Analyze of Event & Flows to understand typical threats as well as threats that won't leave evidence in logs
- Provide anomaly detection mechanism to detect unusual situations
- Provide prioritization of the incidents

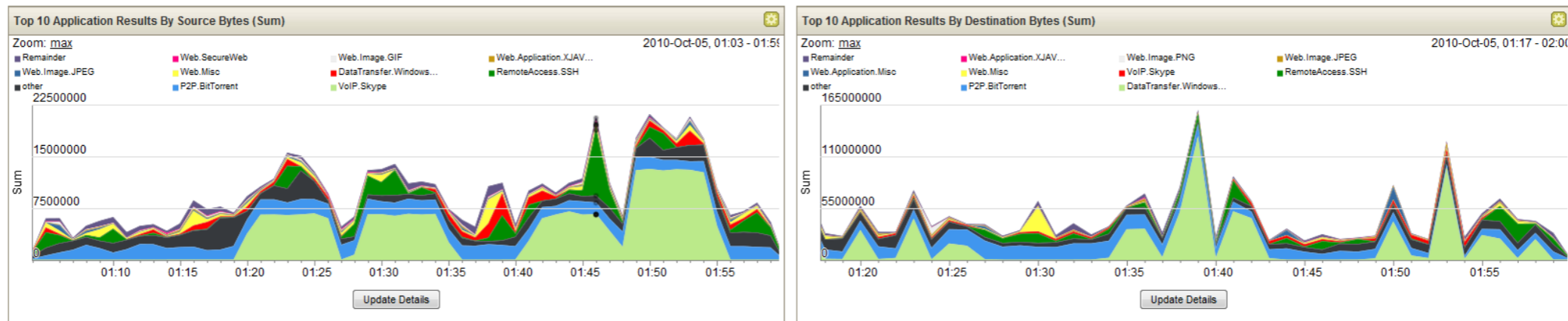
Flows for Application Visibility

- Flow collection from native infrastructure (NetFlow, SFlow, JFlow)
- Layer 7 data collection and payload analysis
- Full pivoting, drill down and data mining on flow sources for advanced detection and forensic examination
- Visibility and alerting according to rule/policy, threshold, behavior or anomaly conditions across network and log activity



Flows for Network Intelligence

- Detection symptoms of 0Day attack
- Policy monitoring and rogue server detection
- Visibility into all attacker communication
- Passive flow monitoring builds asset profiles & auto-classifies hosts
- Network visibility and problem solving (not just security related)



(Hide Charts)

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)	Total Bytes (Sum)	Source Packets (Sum)	Destination Packets (Sum)	Total Packets (Sum)	Count
DataTransfer.Window	Multiple (24)	Multiple (7)	Multiple (13)	Multiple (2)	Multiple (7)	16 319 315	531 531 708	547 851 023	178 629	390 655	569 284	123
P2P.BitTorrent	Multiple (20)	Multiple (5)	Multiple (85)	Multiple (60)	Multiple (3)	44 216 868	191 621 654	235 838 522	127 854	161 966	289 820	546
other	Multiple (259)	Multiple (9)	Multiple (3 063)	Multiple (2 877)	Multiple (10)	37 349 699	168 802 101	206 151 800	93 672	228 533	322 205	6 810
VoIP.Skype	Multiple (5)	Multiple (4)	Multiple (40)	Multiple (40)	other	131 172 458	46 819 290	177 991 748	195 570	76 007	271 577	171
RemoteAccess.SSH	Multiple (10)	Multiple (5)	Multiple (7)	22	Multiple (4)	37 885 116	111 228 020	149 113 136	101 404	261 727	363 131	122
Web.Misc	Multiple (16)	Multiple (5)	Multiple (295)	80	other	10 726 080	20 635 741	31 361 821	33 634	23 904	57 538	2 401
Web.Application.Misc	Multiple (9)	Multiple (4)	Multiple (31)	80	other	654 743	23 125 267	23 780 010	8 193	15 674	23 867	89
Web.Image.JPEG	Multiple (13)	Multiple (4)	Multiple (60)	80	other	2 418 857	18 538 204	20 957 061	15 449	14 150	29 599	586
Web.Web.Misc	Multiple (16)	Multiple (4)	Multiple (152)	80	other	255 544	0 427 264	0 282 800	4 484	6 920	11 404	764

Displaying 1 to 40 of 64 items (Elapsed time: 0:00:00.106)

Page: 1 Go < 1 | 2

Flows for Asset Discovery

Port	Risk / Severity	Last Seen	First Seen
514	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)
7676	1	2009-09-29 21:30:12 (Passive)	2009-09-28 02:30:11 (Passive)
7777	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)
7778	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)
8009	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)

Automatic Asset Discovery

QRadar creates host profiles as network activity is seen to/from

Passive Asset Profiling

QRadar identifies services and ports on hosts by watching network activity

Server Discovery

QRadar identifies and classifies server infrastructure based on these asset profiles

Correlation on new assets & services

Rules can fire when new assets and services come online

Server Discovery

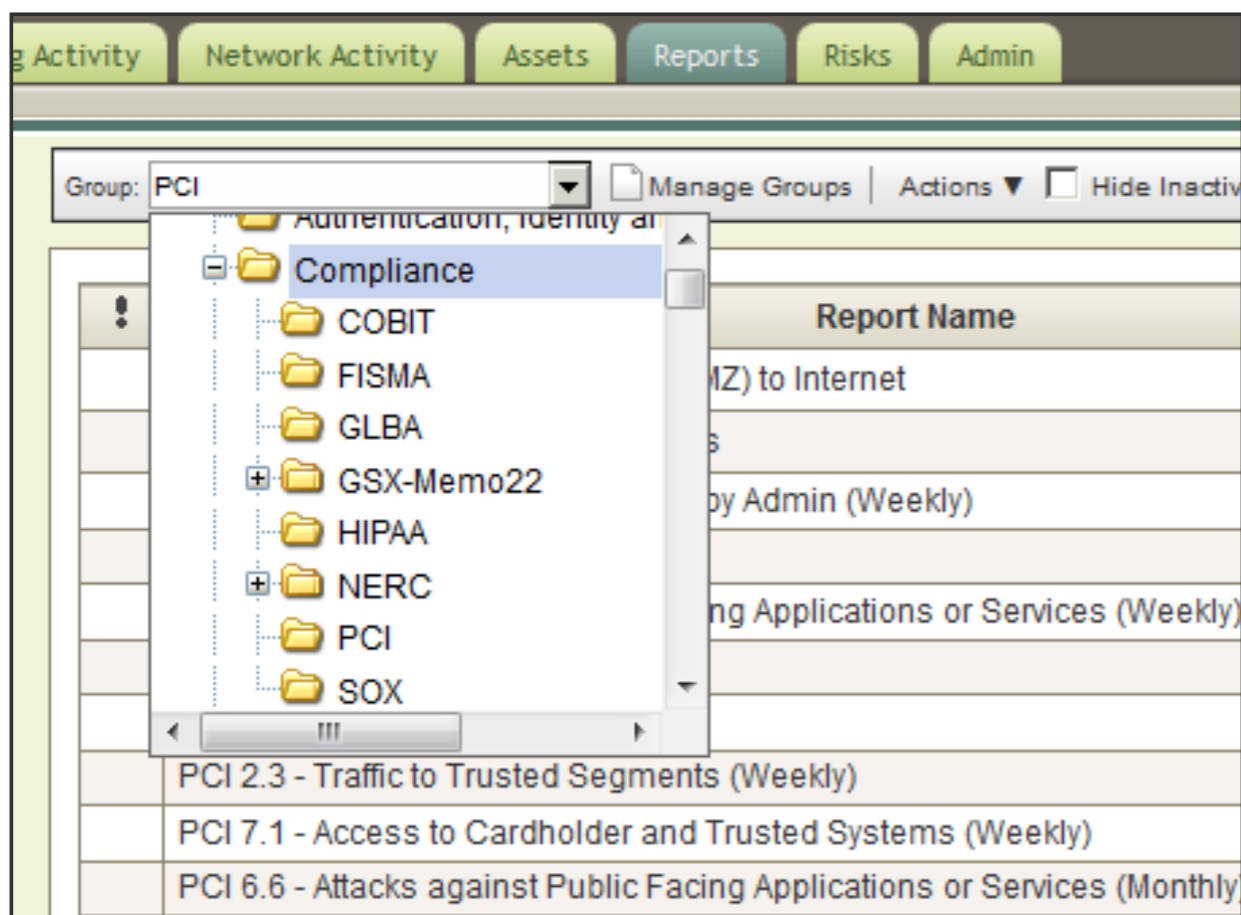
To discover servers (assets) in your deployment based on standard server ports, select the desired role in the Server Type drop-down list box and click 'Discover Servers'.

Server Type:	Database Servers ▼ <input checked="" type="radio"/> All <input type="radio"/> Assigned <input type="radio"/> Unassigned
Ports:	1433, 1434, 3306, 66, 1521, 1525, 1526, 1527, 1528, 1529, 1571, 1575, 1630, 1748, 1754, 1808, 1809, 2481, 2482, 2484, 3872, 3891, 3938 Edit Ports
Server Type Definition:	Edit this BB to define typical database servers. This BB is used in conjunction with the Default-BB-FalsePositive: Database Server False Positive Categories and Default-BB-FalsePositive: Database Server False Positive Events building blocks. Edit Definition
Network:	Select an object... ▼

Matching Servers:

Approve	Name	IP	Network ▲
<input type="checkbox"/>		10.101.139.151	Asia.Bridges.all
<input type="checkbox"/>	Patient Records DB	10.101.139.156	Asia.Bridges.all
<input type="checkbox"/>		10.101.144.76	Asia.Holloway.all
<input type="checkbox"/>		10.102.150.115	Business.Staff
<input checked="" type="checkbox"/>	CRM Database	10.101.145.198	IT.NetServers
<input type="checkbox"/>		10.101.145.237	IT.NetServers
<input type="checkbox"/>	CRM	10.101.3.32	IT.Server.main
<input type="checkbox"/>		10.101.146.10	IT.other

Compliance Rules and Reports



Out-of-the-box templates for specific regulations and best practices: COBIT, SOX, GLBA, NERC, FISMA, PCI, HIPAA, UK GCSx

Easily modified to include new definitions

Extensible to include new

regulations and best practices

Can leverage existing correlation

rules

Rule Name ▲	Group	Rule Cate
Compliance: Auditing Services Changed on Com...	Compliance	Custom Rul
Compliance: Compliance Events Become Offens...	Compliance	Custom Rul
Compliance: Configuration Change Made to Devi...	Compliance	Custom Rul
Compliance: Excessive Failed Logins to Compli...	Compliance	Custom Rul
Compliance: Multiple Failed Logins to a Complia...	Compliance	Custom Rul
Compliance: Sensitive Data in Transit	Compliance	Custom Rul
Compliance: Traffic from DMZ to Internal Network	Compliance	Custom Rul
Compliance: Traffic from Untrusted Network to Tr...	Compliance	Custom Rul

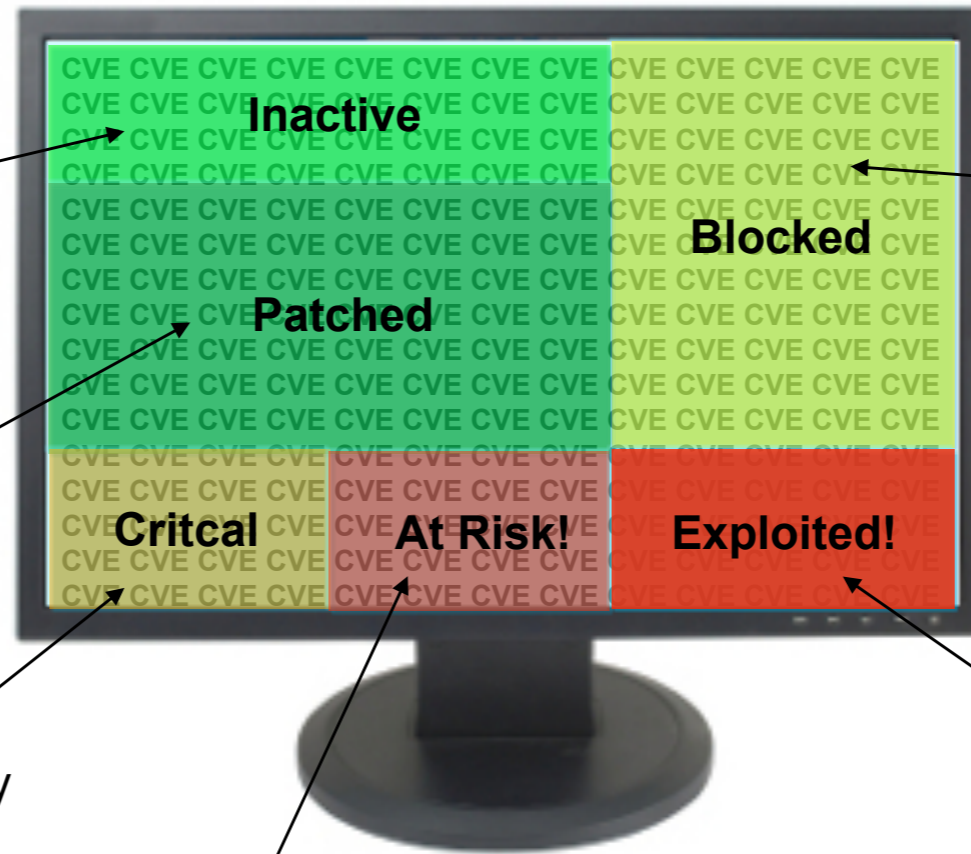
MODULES - QVM

Vulnerability management to detect and prioritize weaknesses
based on the context of Your infrastructure

Inactive: Flow analytics sense application activity

Patched: Endpoint management indicates which vulnerabilities will be patched

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



Blocked: Risk Management shows which vulnerabilities are blocked by firewalls and IPSs

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

At Risk: X-Force Threat and SIEM security incident data, coupled with network traffic flow information, provide visibility to assets communicating with potential threats

MODULES - QRM

QRadar Risk Manager enhances Security Intelligence by adding network topology visualization and path analysis, network device optimization and configuration monitoring, and improved compliance monitoring/reporting to QRadar SIEM

- Collects firewall, switch, router and IPS/IDS configuration data to assess vulnerabilities and facilitate analysis and reporting
- Discovers firewall configuration errors and helps remove ineffective rules to improve performance
- Depicts network topology views and helps visualize current and alternative network traffic patterns
- Identifies active attack paths and assets at risk of exploit, helping mitigate risks and prioritize remediation activities
- Analyzes policy compliance for network traffic, topology and vulnerability exposures
- Improves forensic analyses to determine offense root cause; models potential threat propagation
- Performs rule change simulation and impact analysis

MODULES - QRM

Device		Interfaces	
IP / Context	10.0.250.1 / N/A	Hostname	external
Current Interfaces	9	Adapter	Generic XML
Current Rules	22	Type	FIREWALL
Current NAT Rules	0	Vendor	Vyatta
Current Log Source(s)	CheckPoint @ external-fw.acme.com (Auto-Mapped)		
Config Obtained On	Wed Oct 06 09:52:25 MDT 2010		

Status	Config Date/Time	List	Ent
	2010-10-06 09:...	ALLOW_ONLY_ESTABLISHED	1
	2010-10-06 09:...	ALLOW_ONLY_ESTABLISHED	Default
	Multiple(2)	DENY_ALL	Multiple
	2010-10-06 09:...	DMZ_TO_WORLD	1
	2010-10-06 09:...	DMZ_TO_WORLD	2
	2010-10-06 09:...	DMZ_TO_WORLD	3
	2010-10-06 09:...	DMZ_TO_WORLD	4
	2010-10-06 09:...	DMZ_TO_WORLD	5
	2010-10-06 09:...	DMZ_TO_WORLD	Default
	2010-10-06 09:...	INSIDE_OUT	1
	2010-10-06 09:...	INSIDE_OUT	2
	2010-10-06 09:...	INSIDE_OUT	3

Container Details - Device Rules

This chart displays rule data for a set of devices.

Limit Rules To Top:

Type:

- Most Used Accept Rules
- Most Used Deny Rules
- Unused Rules
- Least Used Accept Rules
- Least Used Deny Rules
- Shadowed Rules

Date/Time Range:

- Current Configuration
- Interval
- Specific Range

Interval:

Start Time: at :

End Time: at :

Timezone:

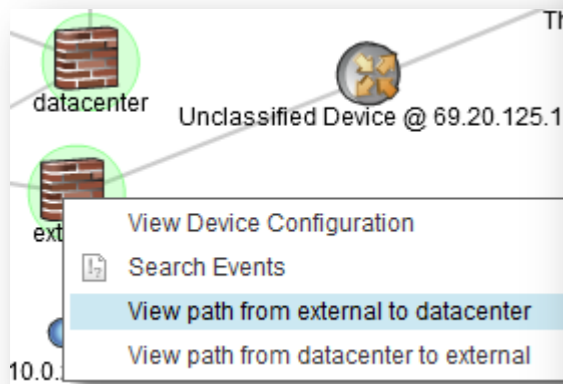
Targeted Data Selection

Format:

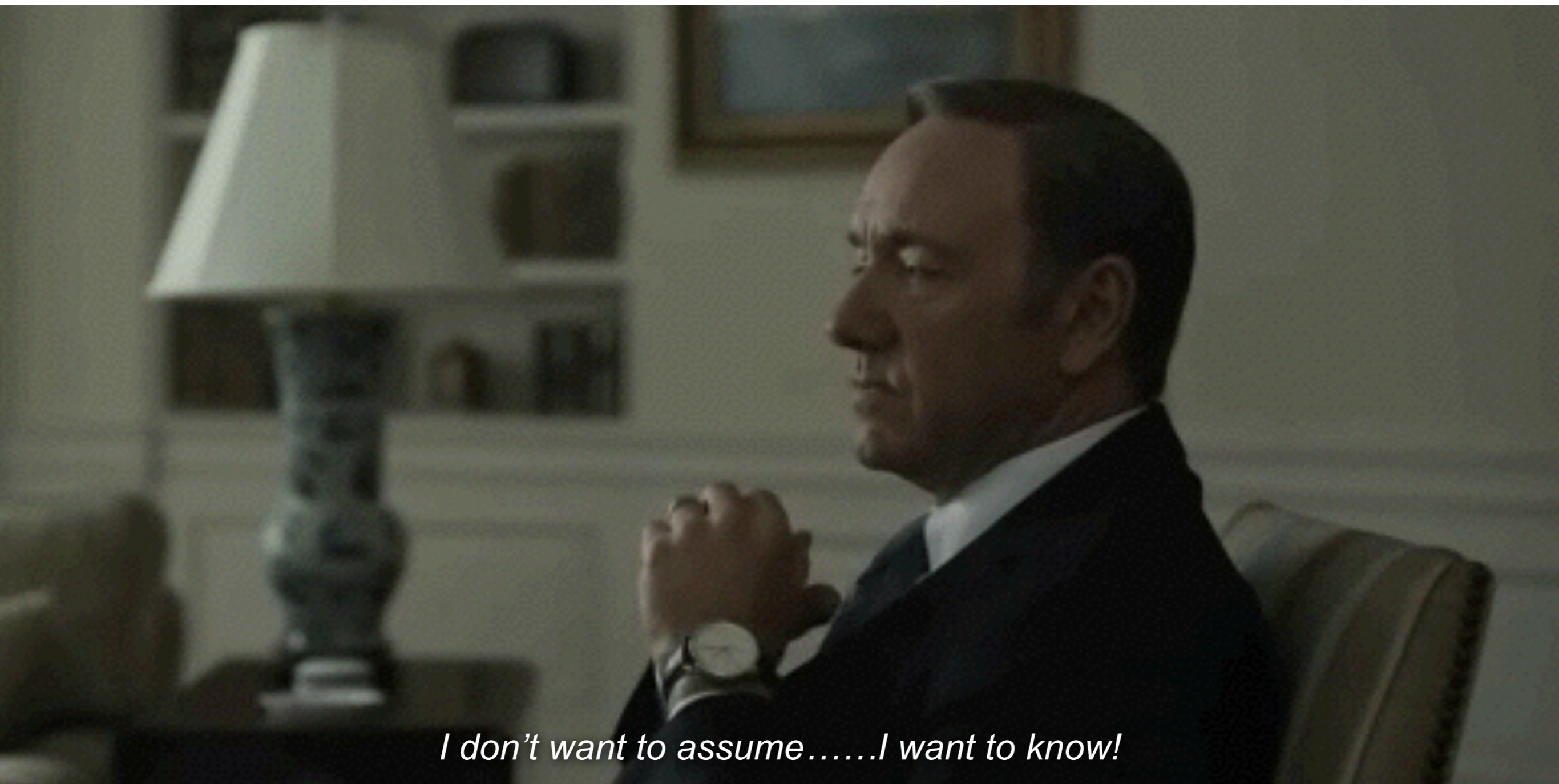
- One aggregate report for specified devices
- One report per device

Devices:

- All Devices
- Adapter:
- Specific Devices



10.0.120.0/24



I don't want to assume.....I want to know!

Frank Underwood, *House of Cards*

MODULES - QIF

Security Intelligence Platform

QRadar Security Intelligence Console

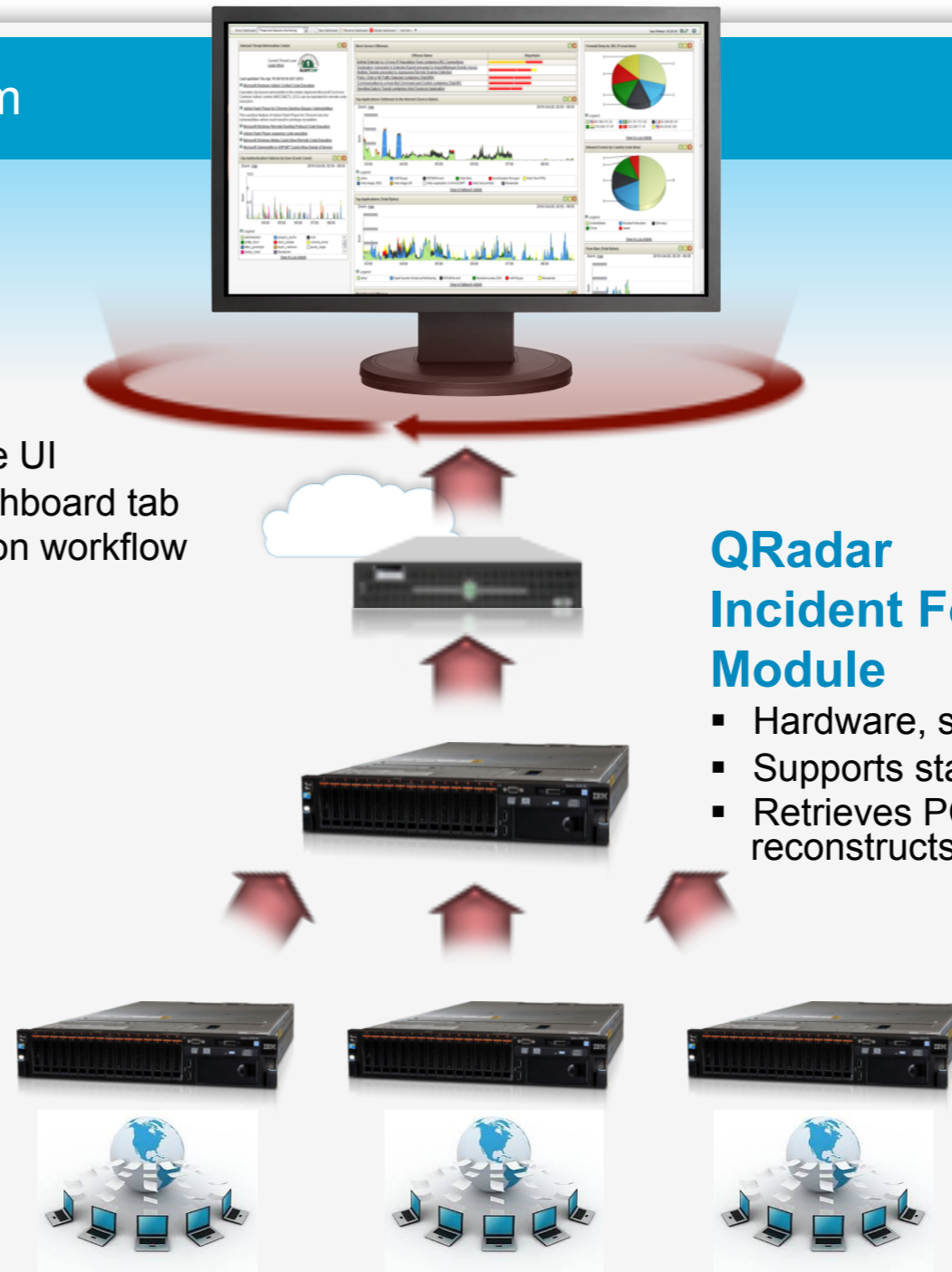
- Seamlessly integrated, single UI
- Includes new 'Forensics' dashboard tab
- Supports incident investigation workflow

QRadar Packet Capture Appliances

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

QRadar Incident Forensics Module

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



MODULES - QIF

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%		
HTTP User-Agent (custom):	Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; AppleWebKit/533.4 (KHTML, like Gecko; iframe_loaded=false&post_form_id=14d949fea3ccd51f54ad9b4a8ae0816c 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
<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; iframe_loaded=false&post_form_id=14d949fea3ccd51f54ad9b4a8ae0816c 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; iframe_loaded=false&post_form_id=14d949fea3ccd51f54ad9b4a8ae0816c 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; iframe_loaded=false&post_form_id=14d949fea3ccd51f54ad9b4a8ae0816c HTTP/1.1 Host: www.facebook.com Connection: keep-alive</pre>	<pre>HTTP/1.1 200 OK Cache-Control: private Expires: Sat, 01 Jan 2000 00:00:00 GMT P3P: CP="DSP LAU" Pragma: no-cache Set-Cookie: act=del; .\z....S...?..9...S]...f.<...9..9..P...wK...W.6...C...4geIf..8... </pre>

To full visualization of extended relationships and embedded content

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

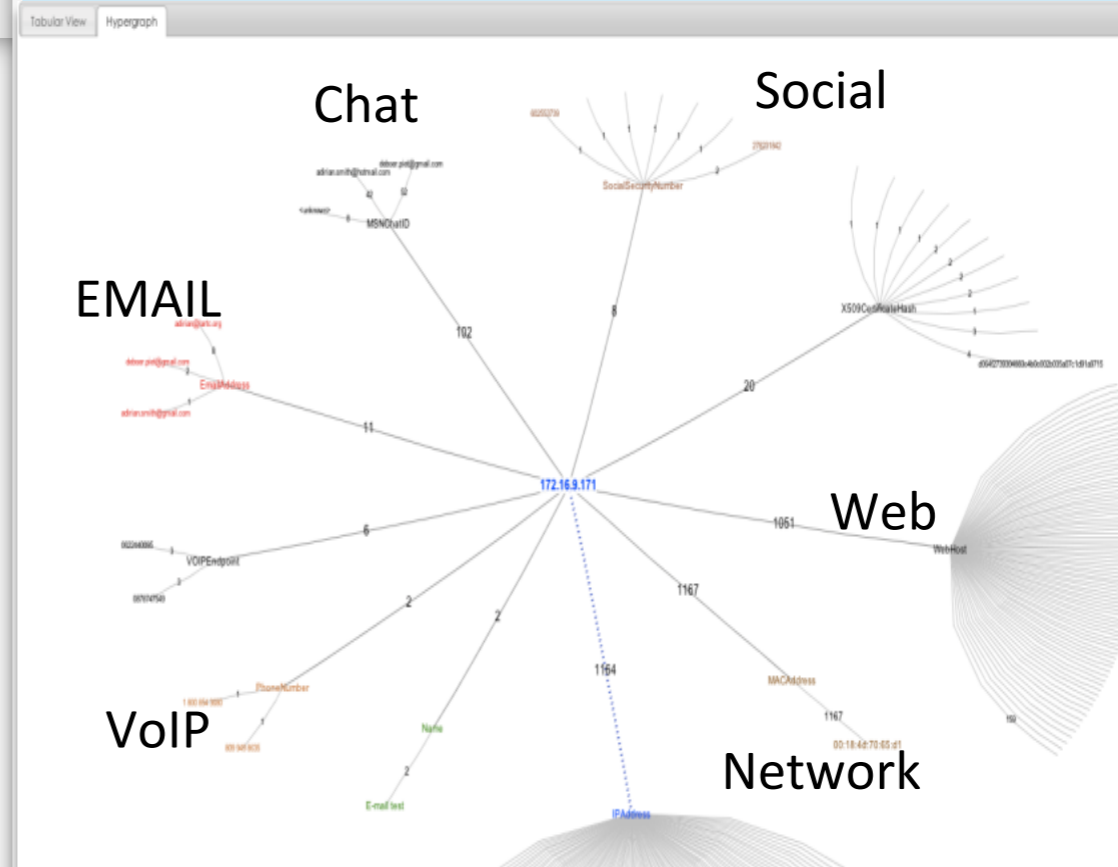
The screenshot shows the IEX website interface. At the top, there are navigation tabs for 'Home', 'Beleggingsfondsen', 'Turbo's', 'Speeders', 'Opties & Futures', and 'Productrecensies'. The main content area features a section titled '10 van Tak: Serieuze zaken' with several articles and a 'Nieuws' section. On the right side, there is a 'Markt vandaag' section with a line chart showing market performance and a table of market indices including Euro/Dol, FRANKF-, LONDEN-F, NY-DJ-In, NY-Nasda, and Goud St.

MODULES - QIF

From standard asset identity information

Attacker Summary		Details	
Magnitude	<div style="width: 100%; height: 10px; background-color: red;"></div>	User	dwight.spencer
Description	10.100.50.21	Asset Name	
Vulnerabilities	0	MAC	
Location	Server Network.Server Network	Asset Weight	0

To rich visualizations of digital impressions showing extended relationships



MODULES - XForce Threat Intelligence

Integrating X-Force Threat Intelligence with the analytics of QRadar allows for more intelligent and accurate security enforcement

The screenshot displays the IBM Security QRadar SIEM interface. At the top, there's a navigation bar with tabs for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, and Admin. The main area is divided into several panels:

- Default-IDS / IPS-All: Top Alarm Signatures (Event Count):** A line chart showing event counts over time.
- Most Severe Offenses:** A table listing offenses with their names and magnitudes. Examples include "Internal Connection to Possible Malware Host preceded by Local DNS Scanner containing Misc.DNS".
- Flow Bias (Total Bytes):** A line chart showing total bytes over time.
- Rule Wizard - Rule Test Stack Editor:** A pop-up window for configuring rules. It lists various tests like "when the local network is one of the following networks" and "when the destination IP is one of the following IP addresses".
- Rule Wizard - Google Chrome:** A browser window showing the "Select a location" step, with a tree view of categories like HostileNets, Bogon, Watchlists, and XForce_Premium.

Selection of categories of malicious IPs

Real-time Security Overview with XF Threat Intelligence Correlation

Ability to set rules leveraging X-Force Threat Intelligence

MODULES - XForce Threat Intelligence

Security Issue	Insight provided
Series of attempted logins from a dynamic range of IP addresses	Malicious attacker
Anonymous proxy connection	Suspicious behavior
A connection from a non mail server with a known spam host	SPAM contamination
Connection between an internal endpoint and a known Botnet C&C	Botnet Infection
Communication between an endpoint and a known malware distribution site	Malware attack

Examples of usage - Malware activity

Offense 2849

Summary Attackers Targets Categories Annotations Networks Events **Flows** Rules Actions Print ?

Magnitude		Relevance	0	View flows for this offense	3
Description	Malware - External - Communication with BOT Control Channel containing Potential Botnet connection - QRadar Classify Flow		Event count	6 events in 1 categories	
Attacker/Src	10.103.6.6 (dhcp-workstation-103.6.6.acme.org)		Start	2009-09-29 11:21:01	
Target(s)/Dest	Remote (5)		Duration	0s	
Network(s)	other		Assigned to	Not assigned	
Notes	Botnet Scenario This offense captures Botnet command channel activity from an internal host. The botnet node communicates with IRC servers running on non-standard ports (port 80/http), which would typically bypass many detection techniques. This sc...				

Potential Botnet Detected?
This is as far as traditional SIEM can go.

First Packet Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Application	ICMP Type/Code	Source Flags	Destination Flags	Source QoS	Destination QoS	Flow Source
11:19	tcp_ip	10.103.6.6	48667	62.64.54.11	80	IRC	N/A	S,P,A	F,S,P,A	Best Effort	Class 1	qradar
11:19	tcp_ip	10.103.6.6	50296	192.168.224.13	80	IRC	N/A	S,P,A	S,A	Best Effort	Class 1	qradar
11:19	tcp_ip	10.103.6.6	51451	62.181.209.20	80	IRC	N/A	S,P,A	F,S,P,A	Best Effort	Class 1	qradar
11:19	tcp_ip	10.103.6.6	47961	62.211.73.232	80	IRC	N/A	F,S,P,A	F,S,P,A	Best Effort	Class 1	qradar

IRC on port 80?
QFlow enables detection of a covert channel.

Source Payload 108 packets, 8850 bytes	<p>UTF Hex Base64</p> <pre>NICK IamaZombie USER IamaZombNICK IamaZombie USER IamaZombNICK IamaZombie USER IamaZombPROCTIL NAMESX PROCTIL NAMESX PROCTIL NAMESX NOTICE Defender :VERSION xchaNOTICE Defender :VERSION x JOIN #botnet_command_channel JOIN #botnet_command_channel</pre>
Destination Payload 70 packets, 5996 bytes	<p>UTF Hex Base64</p> <pre>:Lexington.KY.US.AccessIRC.Net:Lexington.KY.US.AccessIRC.Net:</pre>

Examples of usage - Complex Threat

Offense 3063			
Summary Attackers Targets Categories Annotations Networks Events			
Magnitude		Relevance	3
Description	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	Event count	1428 events in 3 cate
Attacker/Src	202.153.48.66	Start	2009-09-29 16:05:01
Target(s)/Dest	Local (717)	Duration	1m 32s
Network(s)	Multiple (3)	Assigned to	Not assigned
Notes	Vulnerability Correlation Use Case Illustrates a scenario involving correlation of vulnerability data with I China (202.153.48.66) sweeps a subnet using the Conficker worm exploit (CVE 2008-4250). The first s		

Sounds Nasty...
But how do we know this?

The evidence is a single click away.

Network Scan
Detected by QFlow



Buffer Overflow
Exploit attempt seen by Snort

	Event Name	Source IP	Destination IP	Destination Port	Log Source	Low Level Category
<input type="checkbox"/>	Network Sweep - QRadar Classify Flow	202.153.48.66	Multiple (716)	445	Flow Classification E	Network Sweep
<input type="checkbox"/>	NETBIOS-DG SMB v4 srvsvc NetrpPathConon	202.153.48.66	Multiple (8)	445	Snort @ 10.1.1.5	Buffer Overflow

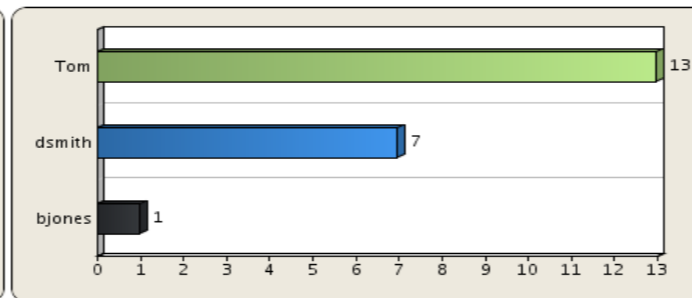
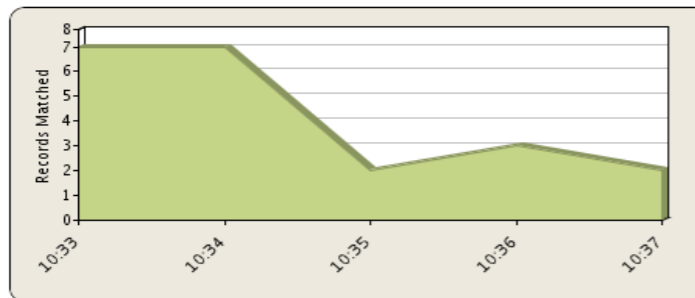
Port	Service	OSVDB ID	Name	Description	Risk / Severity
445	unknown	49243	Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution	Microsoft Windows Server Service contains a flaw that may allow a malicious user to remotely execute arbitrary code. The issue is triggered when a crafted RPC request is handled. It is possible that the flaw may allow remote code execution resulting in a loss of integrity.	3

Targeted Host Vulnerable
Detected by Nessus

Examples of usage - User Activity Monitoring

Magnitude	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>			Relevance	3	Severity	5	Credibility	3
Description	Single Host preceded by Login Failures Followed By Success preceded by Login failure to a disabled account. preceded by Authentication: Repeated Login Failures		Event count	36 events in 6 categories					
Attacker/Src	10.103.7.88 (dhcp-workstation-103-7-88.acme.org)		Start	2009-09-29 10:33:34					
Target(s)/Dest	10.101.3.10 (Windows AD Server)		Duration	4m 51s					
Network(s)	IT.Server.main		Assigned to	Not assigned					
Notes	Windows Authentication Use Case Demo data to demonstrate event-only Windows Authentication use case, including login failures, login attempt to disabled account, etc. This attack is comprised of: - Event(s): Multiple authentication attempts from ...								

Authentication Failures
Perhaps a user who forgot their password?



(Hide Charts)

Brute Force Password Attack

Numerous failed login attempts against different user accounts.

Username	Source IP (Unique Count)	Destination IP (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Category (Unique Count)	Event Count (Sum)	Count
Tom	10.103.7.88	10.101.3.10	Multiple (4)	WindowsAuthSe...	Multiple (4)	19	13
dsmith	10.103.7.88	10.101.3.10	Multiple (4)	WindowsAuthSe...	Multiple (3)	7	7
bjones	10.103.7.88	10.101.3.10	Logon Failure - ...	WindowsAuthSe...	Host Login Failed	1	1

Event Name	Log Source	Source IP	Destination IP
Host Login Succeeded - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Host Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Host Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Remote Access Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Remote Access Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Suspicious Pattern Detected - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Suspicious Pattern Detected - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10

Host Compromised

All this followed by a successful login.
Automatically detected, no custom tuning required.

QRadar Architecture

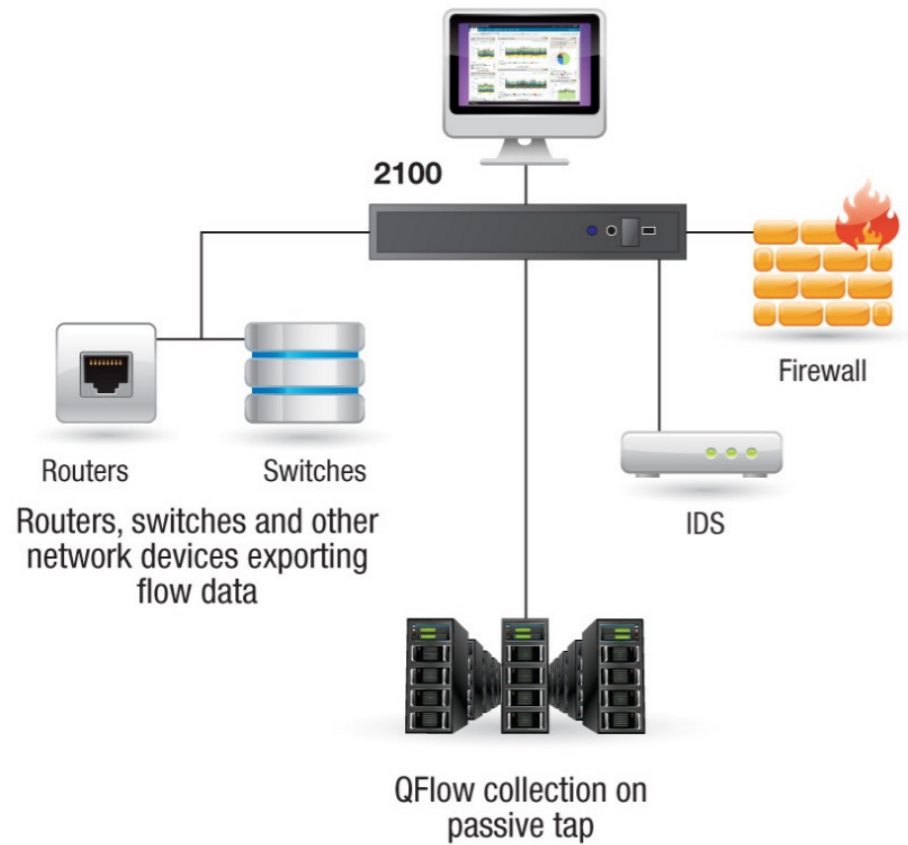
All In On Appliance

EPS max 15 000
FPM max 300 000

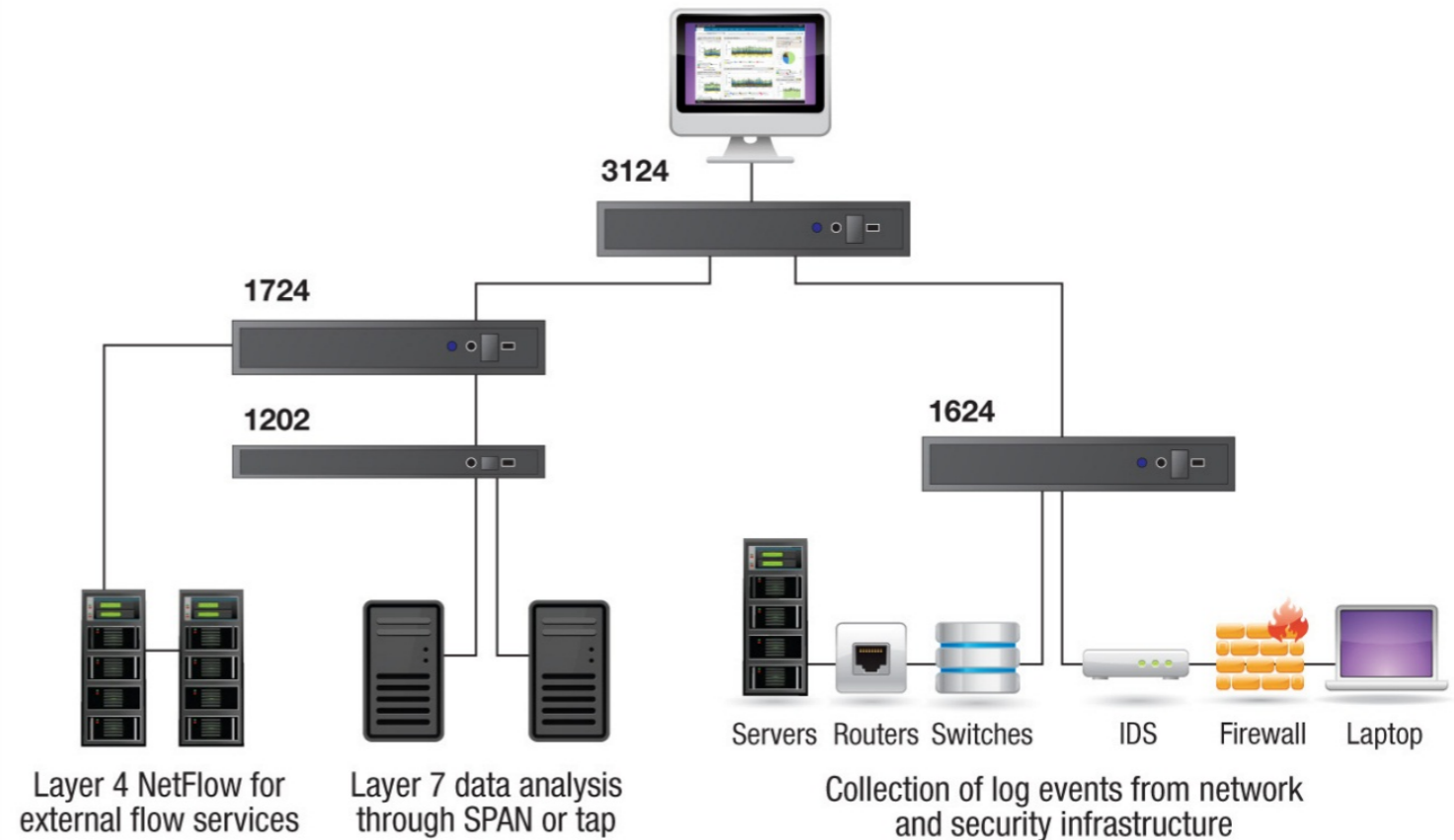
Distributed

EPS max 40 000 per box
FPM max 1 200 000 per box

Sample IBM Security QRadar SIEM 2100 all-in-one deployment
QRadar web console



Sample IBM Security QRadar SIEM 3124 distributed deployment
QRadar web console



Gartner MQ 2014

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (June 2014)

Many are trying but we are still the Leaders....

Gartner MQ 2015

Figure 1. Magic Quadrant for Security Information and Event Management



Live Demo



That's all Folks!