



SECURITY DAY

“

IBM QRadar - the best way to protect your assets

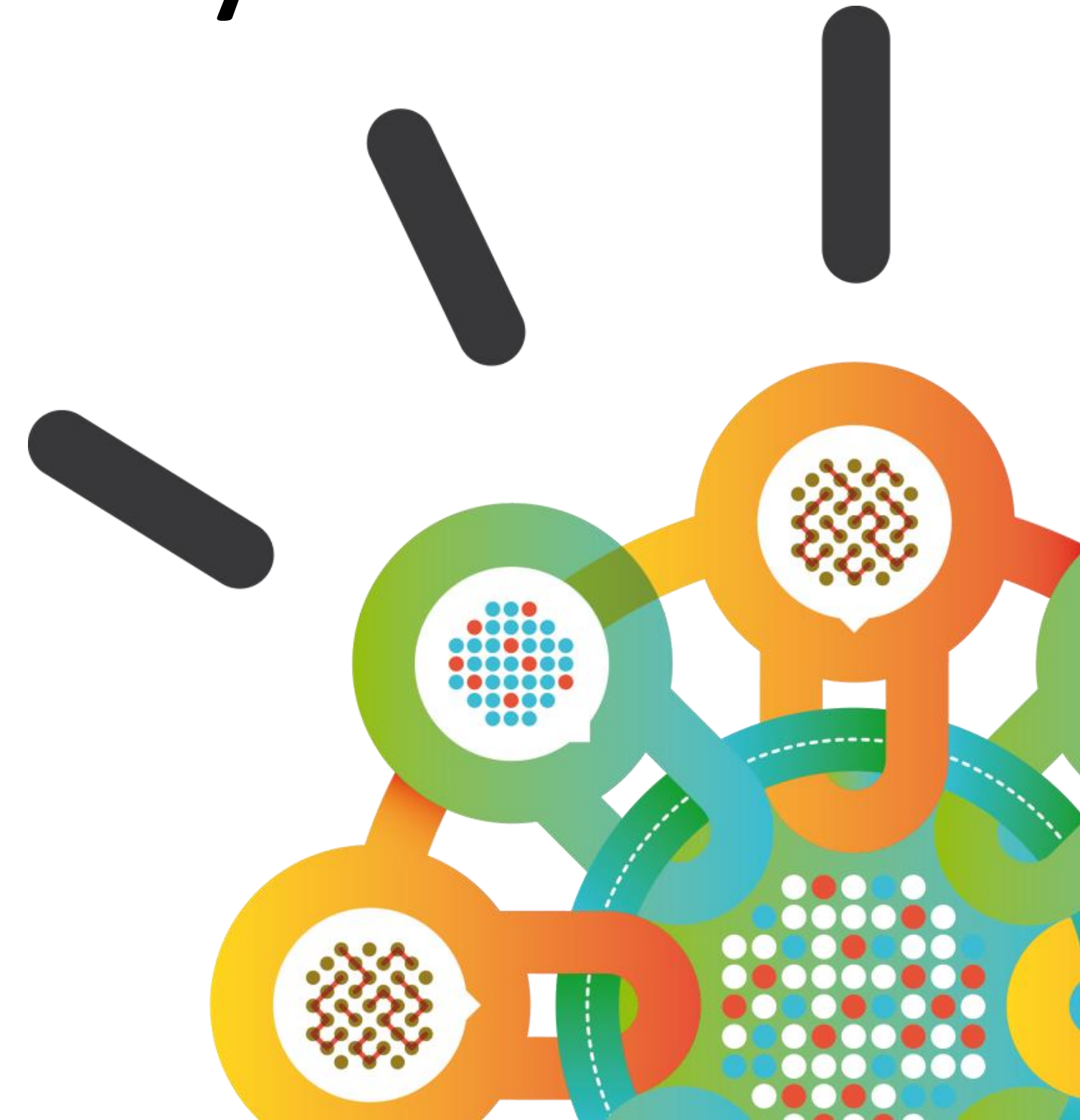
- ANDRZEJ WOJTKOWIAK, IBM



SECURITY DAY

Security Intelligence.
Think Integrated.

IBM QRadar – the best way to protect your assets



2019... it seems that we know that there is a threat



Captain... we have got 3 hours and 56 minutes to hit the iceberg...
Can we make a turn ? ? ?

DoS/DDoS

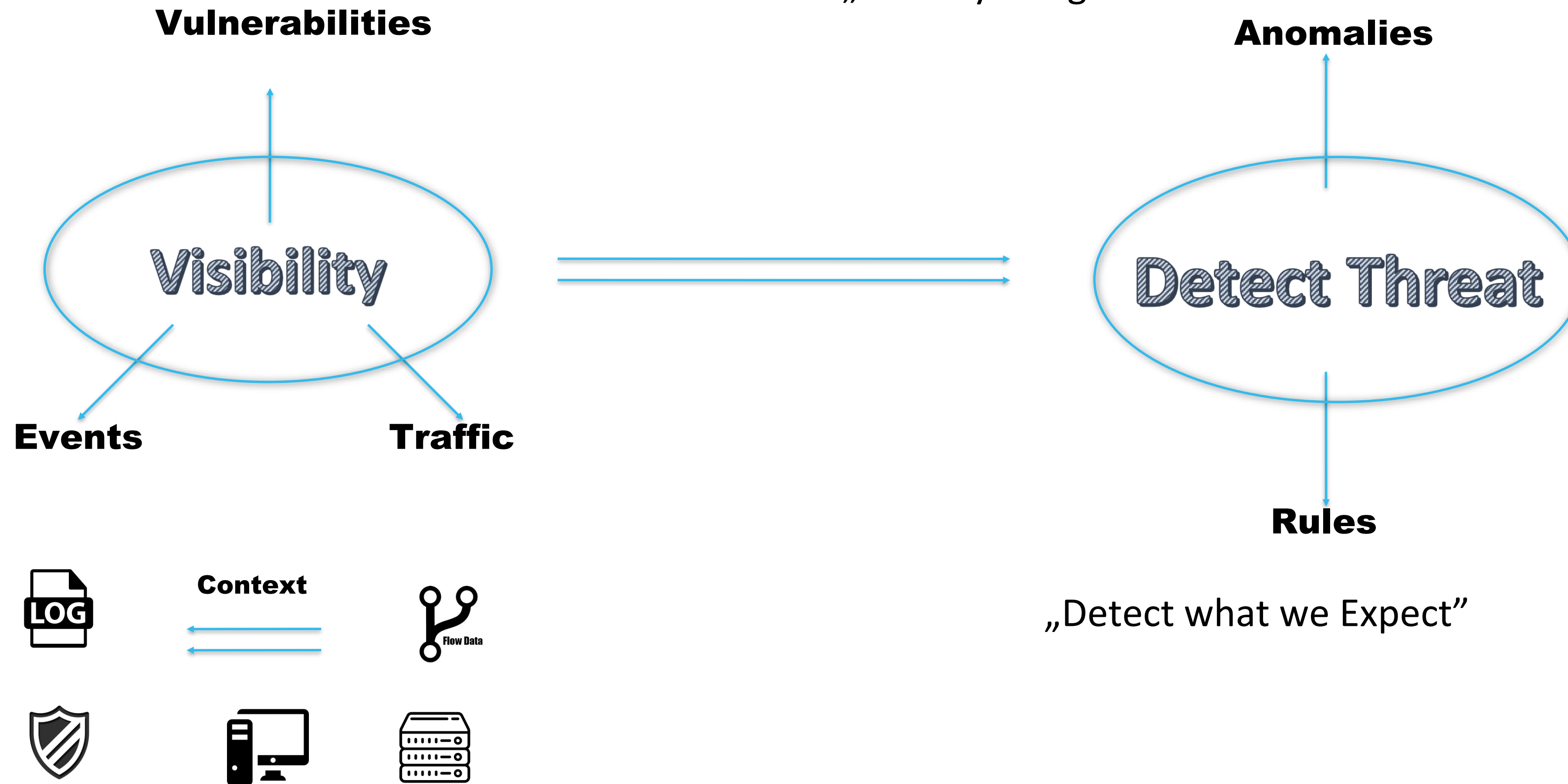
Ransomware

Malware

Human Error & Mistakes

Insiders

How to detect the Threat ?



QRadar is able to continuously monitor infrastructure and inform about security incidents

Simple start with QRadar using out of the box rules

- More than 350 prepared rules
- Create own rules with easy to use Rule Wizard
- Create rules based on Building Blocks which are predefined security objects or event categories

Display: Rules Group: Select a group... Search Rules...

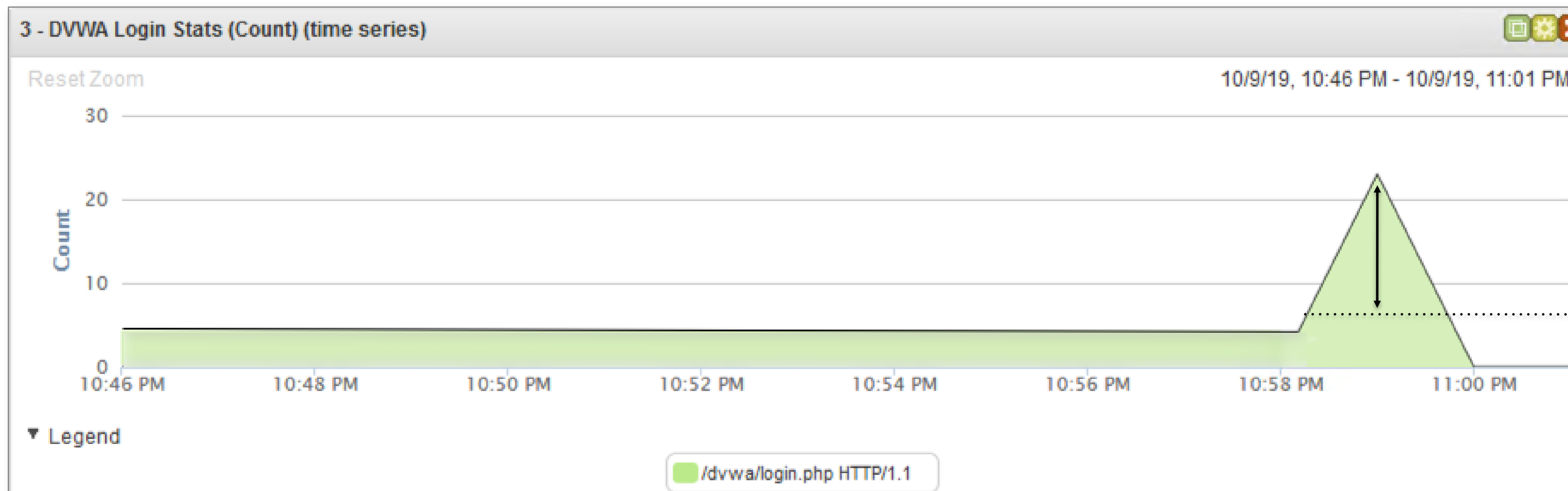
Rule Name	Group	Rule Category	Rule Type	Enabled	Response	Event/Flow Count	Offense Count	Origin	Creation Date	Modification Date
Excessive Database Connections	Anomaly, Recon	Custom Rule	Event	False	Dispatch New Event	0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
Excessive Failed Logins to Compliance IS	Compliance, Recon	Custom Rule	Event	False	Dispatch New Event	0	0	System	11.08.2005, 18:04	24.10.2016, 22:16
Excessive Firewall Accepts Across Multiple Hosts	Anomaly, Recon	Custom Rule	Event	False	Dispatch New Event	0	0	System	30.11.2005, 01:15	24.10.2016, 22:16
Excessive Firewall Denies from Local Host	Recon	Custom Rule	Event	False	Dispatch New Event	0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
Excessive Firewall Denies from Remote Host	Recon	Custom Rule	Event	False	Dispatch New Event	0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
Excessive Firewall Denies from Single Source	Anomaly	Custom Rule	Event	False	Dispatch New Event	0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
Exploit: Exploit Followed by Suspicious Host Activity	Exploit	Custom Rule	Event	False	Dispatch New Event	0	0	System	09.08.2007, 10:49	29.10.2016, 16:29
Exploit: Exploit/Malware Events Across Multiple Destinations	Exploit	Custom Rule	Event	False	Dispatch New Event	0	0	Modified	27.07.2015, 10:48	29.10.2016, 16:29
Exploit: Exploits Followed by Firewall Accepts	Exploit	Custom Rule	Event	False	Dispatch New Event	0	0	System	19.08.2008, 16:33	29.10.2016, 16:29
Exploit: Multiple Vector Attack Source	Exploit	Custom Rule	Event	False	Dispatch New Event	0	0	System	20.08.2008, 12:16	29.10.2016, 16:29
Exploit: Potential VoIP Toll Fraud	Exploit	Custom Rule	Event	False	Dispatch New Event	0	0	System	03.10.2006, 10:27	29.10.2016, 16:29
Exploit: Recon Followed by Exploit	Exploit	Custom Rule	Event	False	Dispatch New Event	0	0	Modified	27.07.2015, 10:50	29.10.2016, 16:29
Exploit: Source Vulnerable to any Exploit	Exploit	Custom Rule	Event	False	Dispatch New Event	0	0	System	02.01.2007, 17:39	29.10.2016, 16:29
Exploit: Source Vulnerable to this Exploit	Exploit	Custom Rule	Event	False	Dispatch New Event	0	0	System	02.01.2007, 17:32	29.10.2016, 16:29
Exploits Events with High Magnitude Become Offenses	Exploit, Intrusion ...	Custom Rule	Event	False		0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
FalsePositive: False Positive Rules and Building Blocks	False Positive	Custom Rule	Common	False		0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
First-Time User Access to Critical Asset	Anomaly, Authenti...	Custom Rule	Event	False	Dispatch New Ev...	0	0	System	27.08.2015, 19:23	24.10.2016, 22:16
Flow Source Stopped Sending Flows	System	Custom Rule	Flow	False	Dispatch New Event	0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
Generated CRE Rule For AD Rule UBA : User Event Frequency An...		Custom Rule	Event	False		0	0	User	11.08.2016, 00:09	08.12.2016, 23:01
Host Port Scan Detected by Remote Host	Recon	Custom Rule	Common	False	Dispatch New Event	0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
Increase Magnitude of High Rate Scans	Recon	Custom Rule	Event	False		0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
Increase Magnitude of Medium Rate Scans	Recon	Custom Rule	Event	False		0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
Large Outbound Transfer High Rate of Transfer	Compliance, Exfilt...	Custom Rule	Flow	False	Dispatch New Event	0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
Large Outbound Transfer Slow Rate of Transfer	Compliance, Exfilt...	Custom Rule	Flow	False	Dispatch New Event	0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
Load Basic Building Blocks	System	Custom Rule	Event	False		0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
Local Flood (TCP)	D/DoS	Custom Rule	Flow	False	Dispatch New Event	0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
Local L2L Database Scanner	Recon	Custom Rule	Common	False	Dispatch New Event	0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53
Local L2L FTP Scanner	Recon	Custom Rule	Common	False	Dispatch New Event	0	0	Modified	29.10.2016, 23:53	29.10.2016, 23:53

- Anomaly
- Asset Reconciliation Exclusion
- Authentication
- Botnet
- Category Definitions
- Compliance
- D/DoS
- Database
- Exfiltration
- Exploit
- False Positive
- Flowshape
- Horizontal Movement
- Host Definitions
- Intrusion Detection
- Log Source Definitions
- Magnitude Adjustment
- Malware
- Network Definition
- Policy
- Port/Protocol Definition
- Post-Intrusion Activity
- Recon
- Response
- Suspicious
- System
- Threats
- User Behavior Analytics
- User Tuning
- VMware Virtual Infrastructure
- Worms
- XForce Premium
 - Enhanced X-Force Rules
 - Legacy Rules
- Other

Rule
 Apply Large Outbound Transfer High Rate of Transfer on flows which are detected by the Local system and when the source bytes is greater than 200000 and when at least 10 flows are seen with the same Source IP, Destination Port, Destination IP in 12 minutes and when the flow context is Local to Remote and when the flow bias is any of the following mostly outbound

Notes
 Detects a single host that is sending more data out of the network than received. This rule detects over 2 MB of data transferred over a 12 minute period.

QRadar - ability to monitor anomalies



Increase in volume of logins to webpage for 500 %

All Offenses > Offense 1 (Summary)

Offense 1 Summary Display Events Anomaly Connections Flows View Attack Path Actions Print Send to Resilient

Magnitude	<div style="width: 75%; background-color: yellow;"></div>			Status		Relevance	3	Severity	5	Credibility	2
Oct 9, 2019	Description	Increased Traffic Volume detected on Web Application based on Anomaly Rule				Offense Type	Event Name				
Oct 9, 2019						Event/Flow count	1 events and 0 flows in 1 categories				
Oct 9, 2019	Source IP(s)	219.138.172.126				Start	Oct 9, 2019, 11:19:00 PM				
Oct 9, 2019	Destination IP(s)	10.10.10.30				Duration	0s				
Oct 9, 2019	Network(s)	other				Assigned to	Unassigned				
Oct 9, 2019	Offense Source Summary										
Oct 9, 2019	Event Name	Increased Traffic Volume detected on Web Application based on Anomaly Rule									
Oct 9, 2019	High Level Category	DOS			Low Level Category	Brute force login					
Oct 9, 2019	Severity	5									
Oct 9, 2019	Offenses	1			Events/Flows	1					

Analyst Custom Searches for QRadar

- XFE Destination IPs
- XFE Source IPs
- Firewall Connections
- Asset/User information from Windows/Linux events

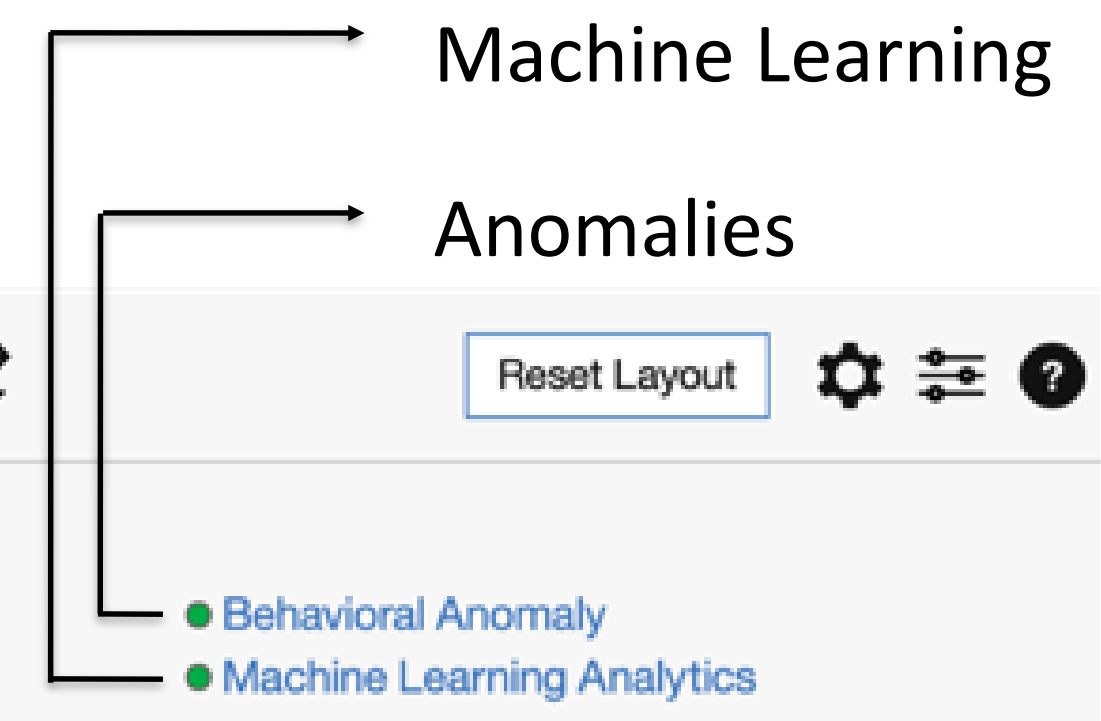
Anomalies & Risk Calculations on User level

Monitored Users

High Risk User

Users Discovered

Users recognized from AD or LDAP



Dashboard Search for User Next Refresh: 00:27 [↻](#) [Reset Layout](#) ⚙️ ☰ ?

Monitored Users

66

High Risk Users

4

6% of monitored users

Users Discovered from Events

16

24% of monitored users

Users Imported from Directory

50

76% of monitored users

Monitored Users

	Recent r...	Risk score ↓	
Ronnie Sharrer 🔔 <small>Chief Happiness Officer from Savannah</small>	210	140K	E 3
Cheryl Sykora <small>Chief Happiness Officer from Savannah</small>	0	49.5K	E 1
Rollin Hand <small>Sales Manager from New York</small>	0	43.1K	E 2
Cindy Carter <small>HR Manager from Savannah</small>	0	40K	E 1
Jack Sprat <small>Compensation Analyst from Savannah</small>	35	18.1K	E 1

Sales Team

	Recent r...	Risk score ↓	
Ronnie Sharrer 🔔 <small>Chief Happiness Officer from Savannah</small>	210	140K	E 3
Rollin Hand <small>Sales Manager from New York</small>	0	43.1K	E 2
Michael Rose <small>Sales Associate from New York</small>	20	17.1K	E 1
Jay Steenberg <small>Sales Associate from New York</small>	45	16.8K	E 1
Wayne Lewis <small>Sales Associate from New York</small>	35	16.6K	E 1

System Score (Last Day)

Average System Risk Score

4:30 PM Mar 20 6:00 AM 12:00 PM 3:30 PM

Risk separately calculated for each and every user

Ability to create separate watchlists - example Sales Team, Administrators, VPN Users etc.

Risk calculated for all monitored infrastructure

Anomalies & Risk Calculations on User level

Dashboard > User Details

Search for User

[Reset Layout](#)
⚙️
🔗
?

Shirley Pollack

Shirley Pollack
[spollack@ibm.com](#)
 Software Engineer
 Software
 Atlanta, Georgia, United States

Overall Risk Score
1.4K ▼
Risk last Interval
0

Active
Dormant ⚠️

spollack
spollack2

Timeline

Mar 9 - Mar 13 📅

● User Events ● Risky Events

Recent Offenses

Offense # 779849 3 days ago

Description: Multiple Login Failures for the Same User preceded by Login Failures Followed By Success from the same Username containing Authcrypt

Categories: Auth Server Session Opened, General Authentication Failed, User Login Failure, Web Service Login Succeeded, Remote Access Login Succeeded, Suspicious Pattern Detected, Login with username/password defaults successful, SSH Login Failed, Misc Login Failed

Event Count: 3.5K **Flow Count:** 0 **Magnitude:** 2/10

Offense # 744740 9 days ago

Description: Multiple Login Failures for the Same User preceded by Login Failures Followed By Success from the same Username containing Login attempt - failed

Risk Category Breakdown (Last Hour)

- User Behavior
- UBA Machine Learning...

Total Activity

6K Mar 9 - Mar 13 📅

Mar 13

12:00 AM - 8:35 PM (20.6 hours)

210
Risk

4
Use Cases

44
Risky Events

17
Log Devices

180
Event IDs

486
URLs

1
Aliases

Count	Use Cases	Risk
40	Detect Insecure Or Non-Standard Protocol	200
2	Abnormal increase in User activity	10
1	Deviation from learned peer group	5
1	Deviation from normal activity patterns	5

Viewing 4 of 4 [View in QRadar](#)

How we detect security incidents

- Huge support for infrastructure

- Over 400 supported systems and applications
- Ability to add own log sources
- Use network traffic to provide context of events
- Analyze both security and non-security events

- Huge number of default rules

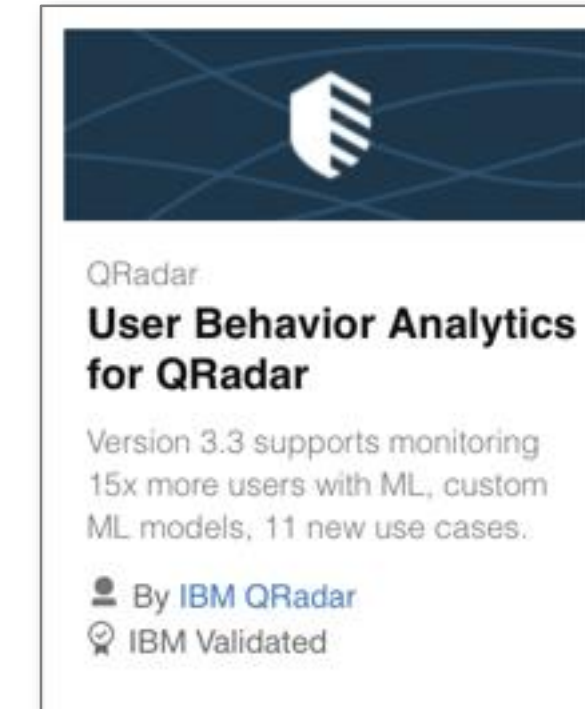
- Over 350 correlation rules available out of the box
- Ability to download over 1200 custom rules from Community Portal (IBM App Exchange)

- Ability to detect anomalies in User Behavior, Applications & Network layers

- Sophisticated algorithms which allows to detect unusual behaviors of our users and infrastructure
- Powerful dashboards which presents risk distribution over time

- Large number of free applications which extends QRadar functionalities

- Around 200 out of the box applications, Content Packs, Custom Rules, Dashboards
- Integration with leading security solutions to assure integration and holistic view
- Powerful functionalities that address security and operational demands



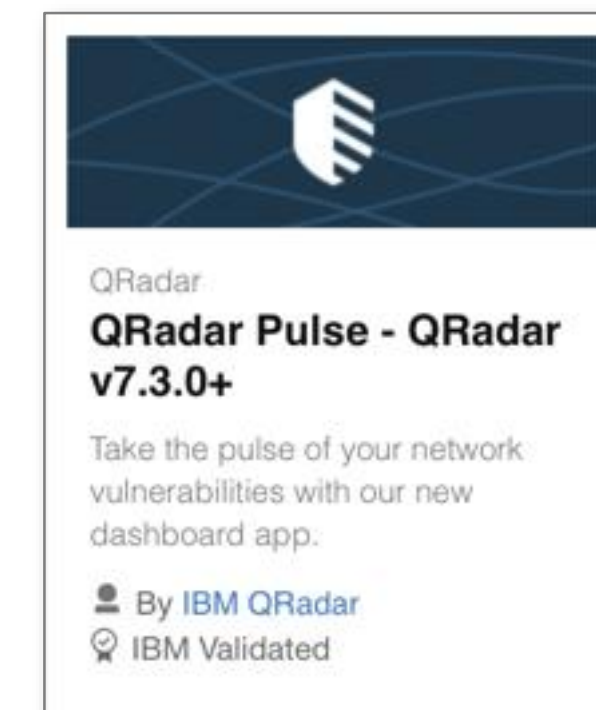
QRadar
User Behavior Analytics for QRadar
 Version 3.3 supports monitoring 15x more users with ML, custom ML models, 11 new use cases.
 By IBM QRadar
 IBM Validated



QRadar
IBM QRadar DNS Analyzer
 Analyze DNS traffic to detect malicious activity within your organization.
 By IBM QRadar
 IBM Validated



QRadar
QRadar Deployment Intelligence
 A powerful monitoring application built to give users a birds-eye-view of QRadar deployment.
 By IBM QRadar
 IBM Validated



QRadar
QRadar Pulse - QRadar v7.3.0+
 Take the pulse of your network vulnerabilities with our new dashboard app.
 By IBM QRadar
 IBM Validated



QRadar
Threat Intelligence
 Stop threats by adding real time threat intelligence feeds to QRadar.
 By IBM QRadar
 IBM Validated

„However, is **DETECTION** enough to really protect Your assets ?”

Detection is only the beginning of the process

Rearm security tools with conclusions from incident
Eliminate potential security gaps
Improve Security Operations Procedures



DETECT

UNDERSTAND

RESPOND

Events
Flows
Vulnerabilities
Rules
Anomalies
Security incidents

Analyze using tools
Identify false-positive
Analyze needs to be reliable
Gain understanding to apply Response Tactics
It needs to be fast and precise to minimize impact

Apply consistent tactics to handle incident
Resolve security incident through it's whole life-cycle
Use automation to enrich investigation
Use automation to perform immediate actions

Watson for Cyber Security performs automated analyze of security incidents

Statistics Reverse Engineering
Social Media Response Plans
Reports Trends

KNOWLEDGE

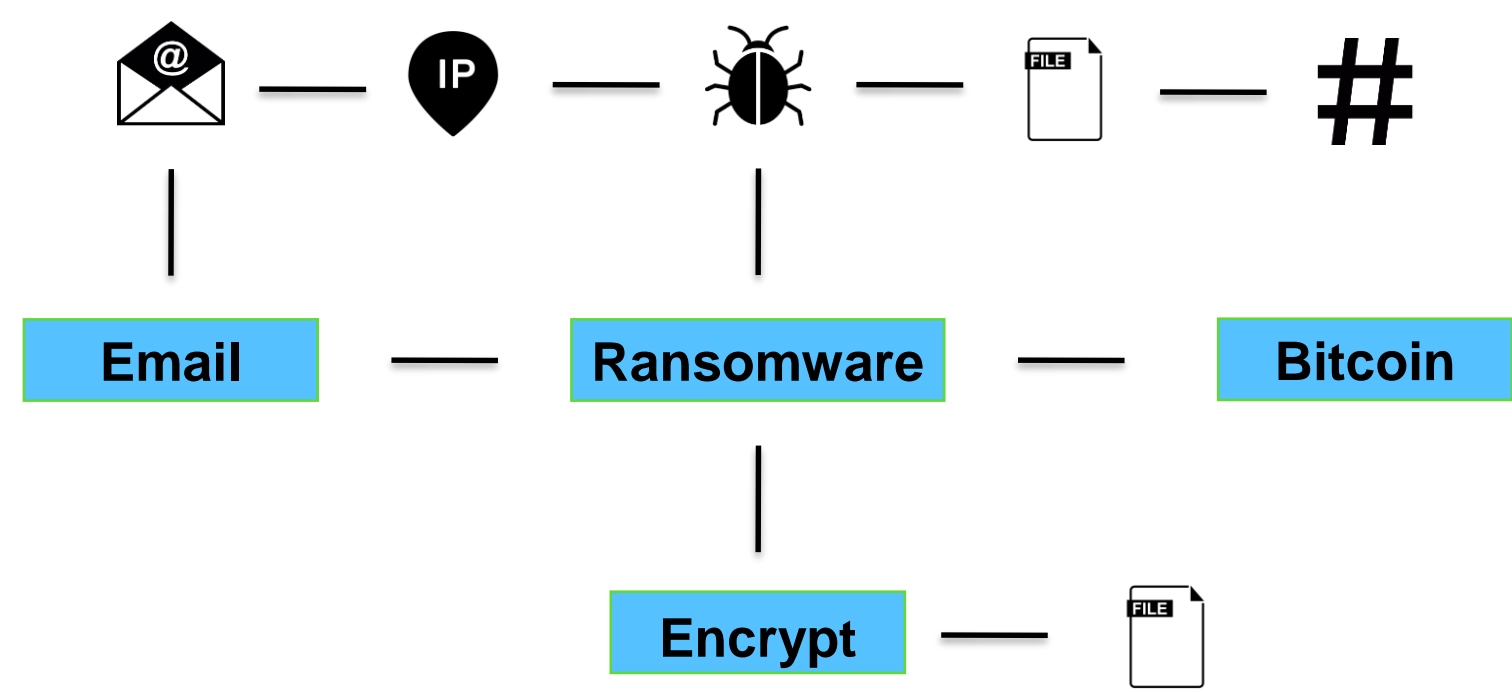


Best Practices Internet & Dark Web
Websites Blogs Forensic Data
R&D Data

Security Incident

Watson For Cyber Security

UNDERSTAND



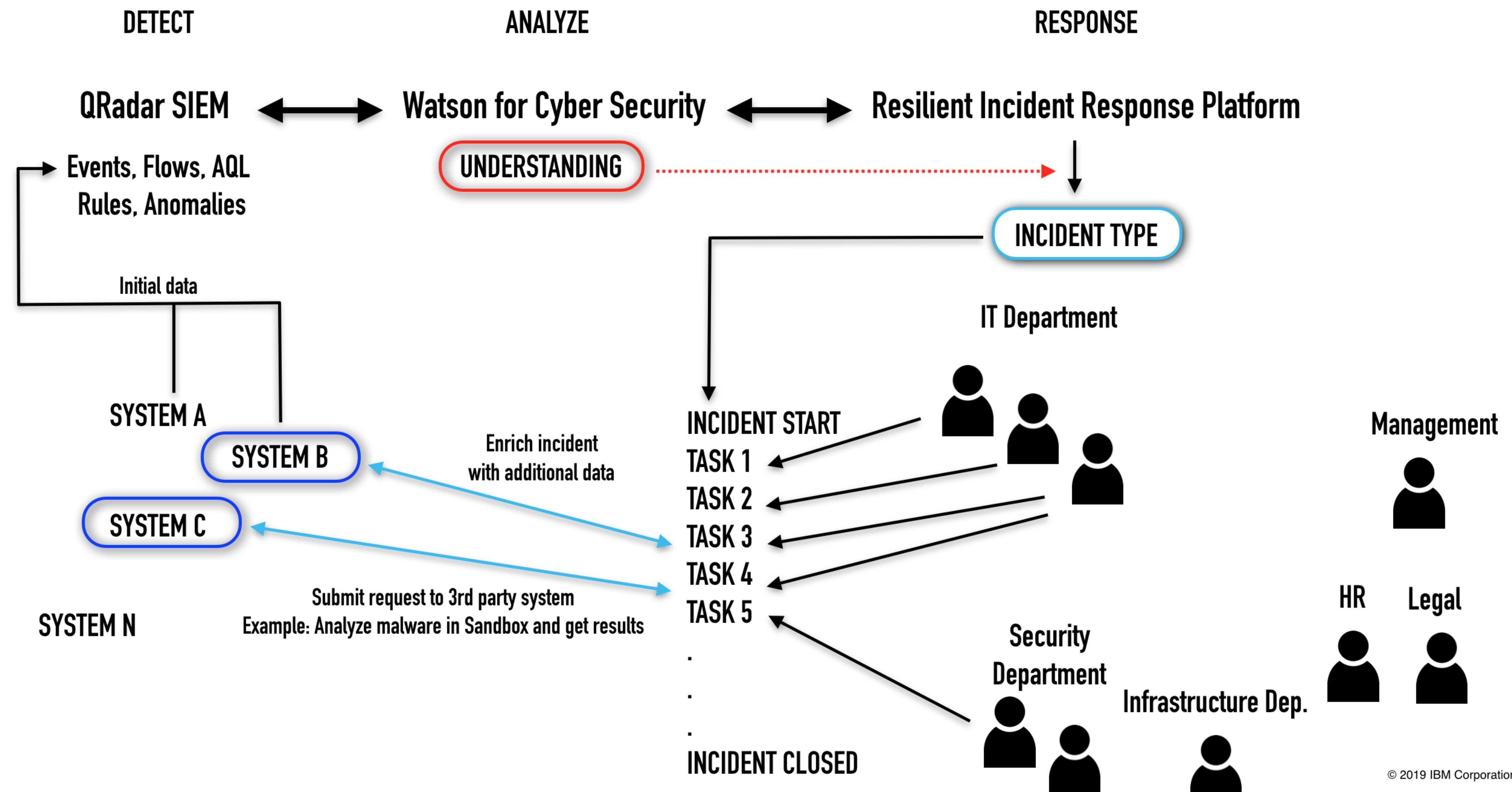
Additional assets which are also in malw

Identified communication

“QRadar Advisor has determined Locky malware family or campaign may be related to the incident and 5 other assets in your networks appear to be affected. QRadar Advisor has also found these additional indicators possibly related to the incident containing 14 Domains, 130 IP Addresses, 7 Geographies, 8 file HASHes”

Locky malware executable file

Resilient Incident Response Platform provides guidance how to resolve incident



Thank You