Temasek Polytechnic
School of Informatics & IT

Introduction to Security Incident Response & Management

Security Incident Investigation in a SOC Environment with IBM QRadar SIEM

(Part A – 1.5 HRS)

Temasek POLYTECHNIC

References

References for Cyber Security Incident Response & Management Concepts:

Relevant NIST/CMU SEI Guides:

- NIST SP 800-61 – Computer Security Incident Handling Guide (both Revisions 1 & 2)
- NIST SP 800-86 – Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-83 – Guide to Malware Incident Prevention and Handling
- RFC 3227 – Guidelines for Evidence Collection and Archiving
- CMU/SEI – Organizational Models for Computer Security Incident Response Teams (CSIRTs)
- CMU/SEI – Handbook for Computer Security Incident Response Teams (CSIRTs)
- CMU/SEI – First Responders to Computer Forensics

References

References for Network Traffic Forensics & IBM Security QRadar SIEM:

- Bejtlich, R. (2013).
  The practice of network security monitoring: Understanding incident detection and response.
  San Francisco, CA: No Starch Press, Inc.
- Davidoff, S., & Ham, J. (2012).
  Network Analysis: Tracking Hackers Through Cyberspace.
  Upper Saddle River, NJ: Prentice Hall.
- Lillard, T.V., Garrison, C. P., Schiller, C. A., & Steele, J. (2010).
  Digital forensics for network, internet, and cloud computing: A forensic evidence guide for moving targets and data.
  Burlington, MA.: Syngress.
- Sanders, C. (2011).
  Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems (2nd Ed.).
  San Francisco, CA.: No Starch Press.
- Relevant IBM SIEM training modules:
  - ***IBM Security Intelligence Fundamentals (BQ600)***
  - ***IBM Security QRadar SIEM Foundations (BQ102)***
  - ***IBM Security QRadar SIEM 7.2 Administration and Configuration (XIS08)***

Disclaimer for Copyright

- All copyrights and other intellectual property rights in the course materials (course notes, lab exercises, etc.) are reserved and shall remain with the original owner(s).

Use of IBM Security QRadar SIEM in a SOC Environment

(Part A) – SOC and SIEM Concepts

A.1 Overview of SOC Operations
A.2 Introduction to IBM Security QRadar SIEM
A.3 Managing Cyber Security Incidents in a SOC
A.4 IBM Security QRadar SIEM Capabilities

A.1 Overview of SOC Operations

What is a SOC?

Source: https://en.wikipedia.org/wiki/Security_operations_center

- A **security operations center (SOC)** is a centralized unit that deals with security issues on an organizational and technical level.
- A SOC within a building or facility is a central location from where staff supervises the site, using data processing technology.
- Typically, a SOC is equipped for access monitoring, and controlling of lighting, alarms, and vehicle barriers.

We are dealing with Information SOC:

- An **information security operations center (ISOC)** is a dedicated site where **enterprise information systems** (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are **monitored, assessed, and defended**.

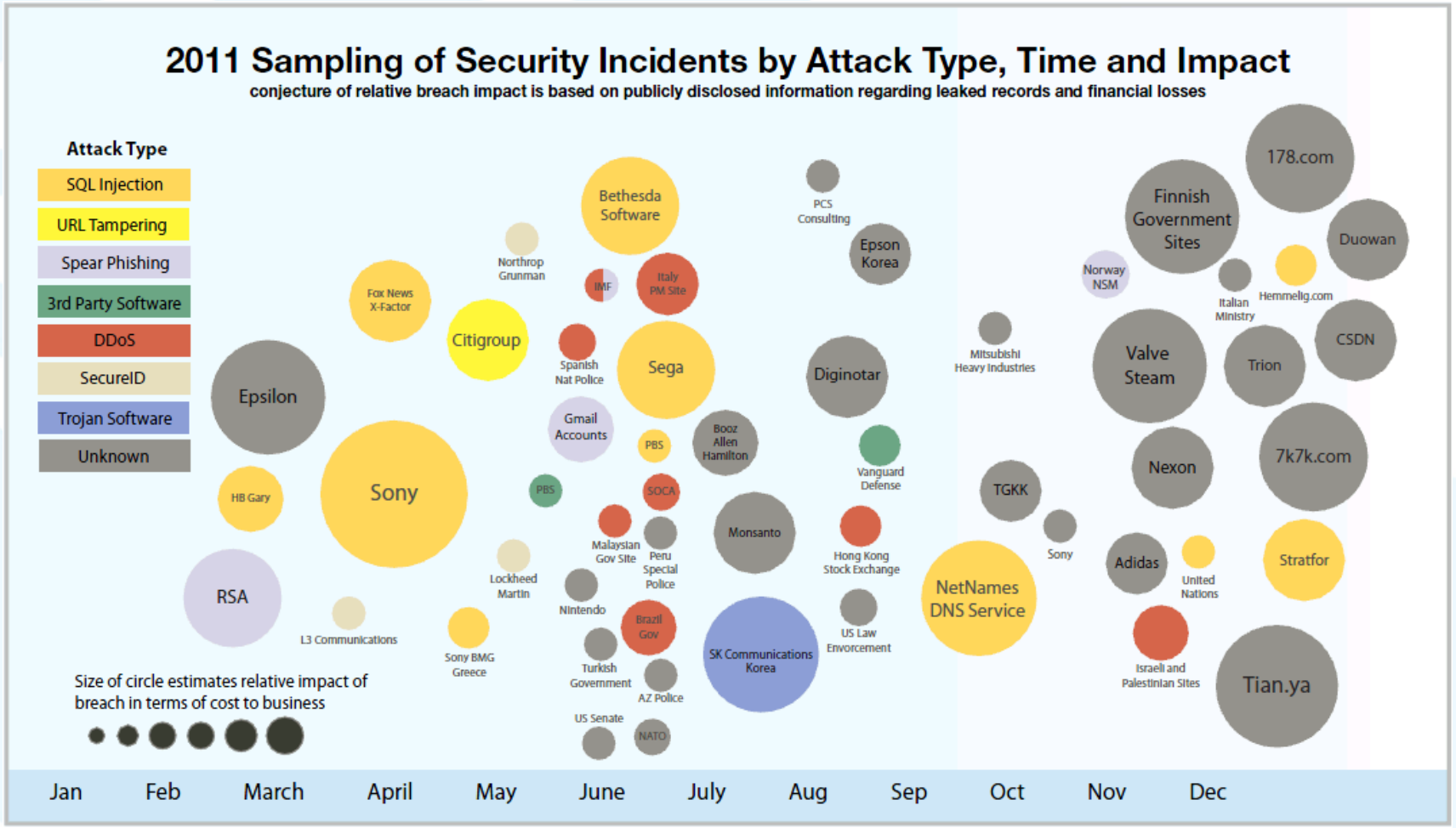
Introductory Youtube Videos on SOC:

- Raytheon – Cyber Security Operations Center (2:11)
- Akamai - Security Operations Center Video – Inside Akamai's SOC (3:45)
- AlienVault – What is a Virtual Security Operations Center (VSOC) (2:54)

Overview of a SOC (from IBM Perspective)

- The IT security landscape is evolving and traditional point solutions such as firewalls and network intrusion prevention systems (NIPS) operating in silos are no longer adequate to protect organisations.
- IBM X-Force report showed that the sophistication of attackers is continuing to increase and evolve into new and often unknown techniques.
- Organisations large and small are continuing to fall victim to structured query language (SQL) injection, URL tampering, spear phising and other techniques, even in the midst of an ample investment in security technologies.
- Today's advanced threats are forcing businesses to move up the security maturity model by building up their own security intelligence through a **Security Operations Centre (SOC)**.
- It is where **enterprise information systems** (web sites, applications, databases, data centres and servers, networks, desktops and other endpoints) are monitored, assessed, and defended from an IT security perspective.

Overview of a SOC (cont.)



(source: "IBM X-Force 2011 Trend and Risk Report", published in Mar 2012)

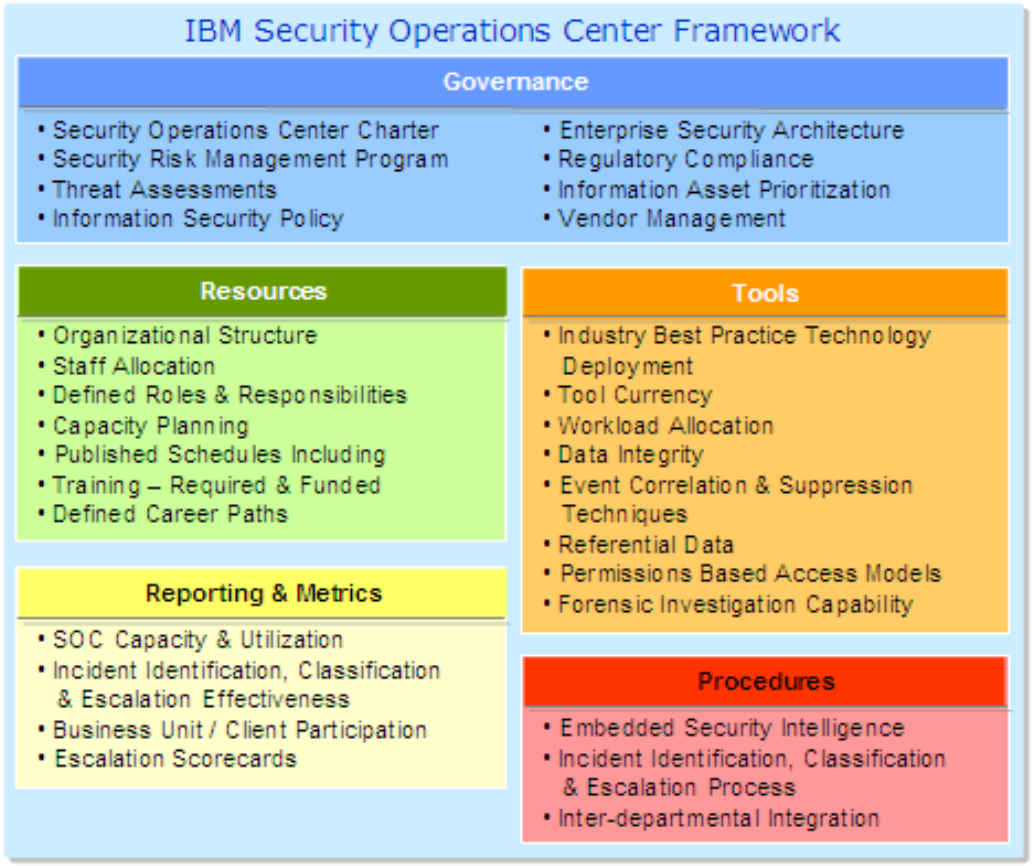
Functions of a SOC

There are a number of **common SOC services** that facilitate IT security monitoring, assessment and defence. They can be divided into the following types of tasks:

- **Monitoring** – 24*7 monitoring of IT security threats by a security analyst. This is typically alerted by security intelligence and alerting by **Security Information and Events Management (SIEM)** technology.
- **Assessment** - All alerts are analysed to eliminate false positives and determine the severity of the threat. Other forms of assessment include analysing vulnerability assessment reports generated by penetration tests or automated vulnerability assessments.
- **Response** – Appropriate countermeasures are determined in line with severity and type of the security incidents. Countermeasures could include fine tuning of firewall rules, network intrusion prevention systems (NIPS) and server security configuration.
- **Forensics** – Post-threat analysis is conducted to determine root cause of a security incident and future countermeasures to mitigate risks of a repeat incident.

SOC Framework

As a typical SOC framework, IBM has identified various function blocks which include **Governance, Resources, Reporting & Metrics, Tools, and Procedures** as shown in the figure below.



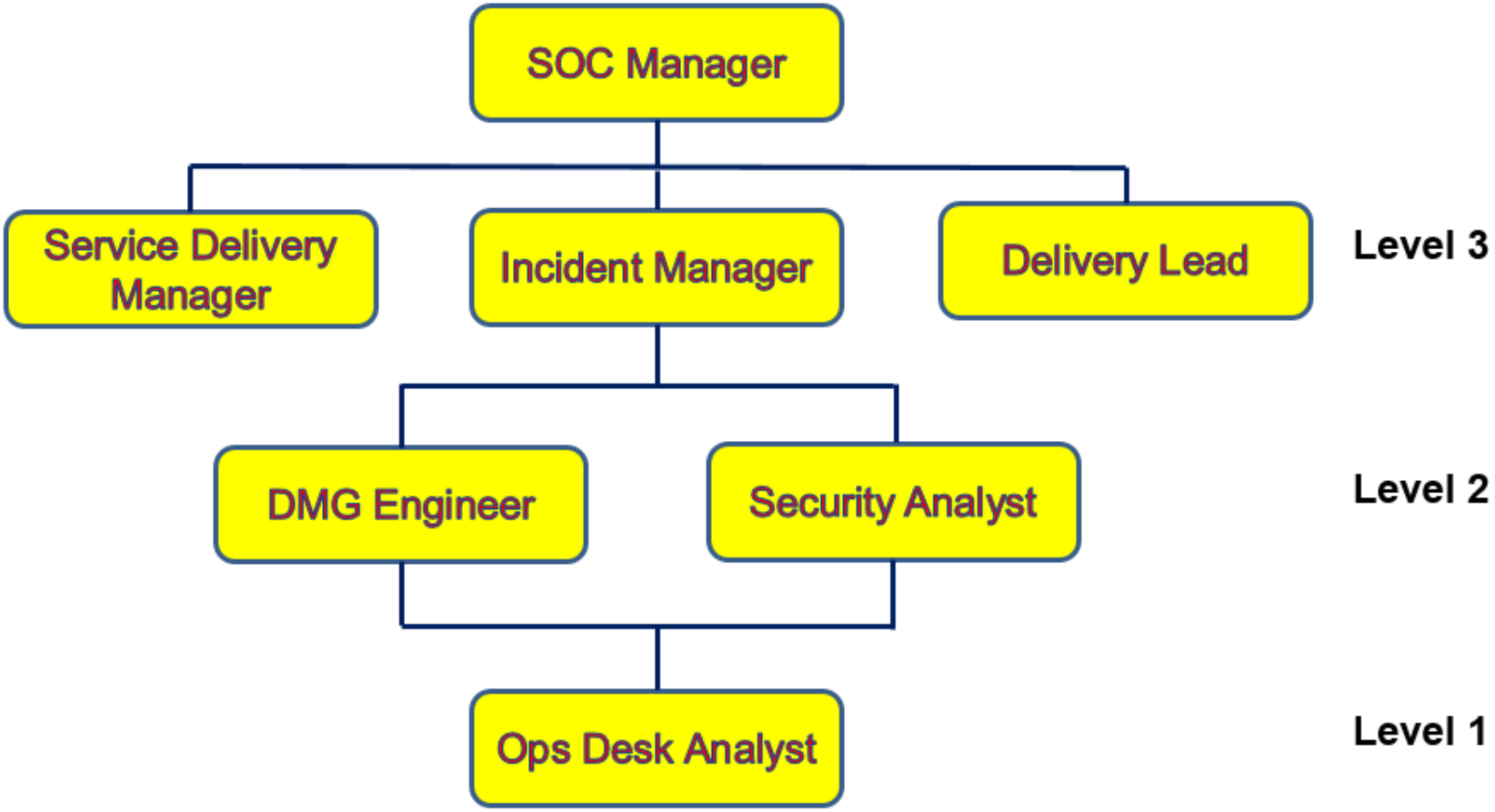
SOC Processes & Procedures

- Apart from key technologies deployed in the SOC data centre, the heart of the SOC is where the security team works as a SOC is 80% people and process and 20% technology.
- IBM has identified and developed **14 processes and 36 procedures** that typically need to be implemented in all SOCs.
- The extent of deployment differs between SOCs but the overall structure is required to ensure that a SOC has the necessary base processes to allow it to mature as more services are added on.
- Details of the processes and procedures are shown in the following figure.

SOC Processes & Procedures (cont.)

SOC Key Job Roles & Responsibilities

The job roles and their hierarchy are depicted in the following figure



SOC Key Job Roles & Responsibilities

SOC staff **roles and responsibilities** differ between SOCs based on services provided and how the SOC evolves. However, the following **key roles** are expected.

- **SOC Manager** – Provides overall leadership within a SOC ensuring the teams meet all internal and external Service Level Agreements/Objectives (SLA/SLO)
- **Service Delivery Manager** - Scope of work includes understanding client requirements, the identification of risks, threats, vulnerabilities, potential anomalous flows and interactions, and the design of integration and security architectures for security into customer service management systems
- **Incident Manager** - Responsible for taking incoming customer escalations and responding to them in a timely manner
- **Delivery Lead** – Leads a team of security professionals to proactively detect malicious behaviour and enact countermeasures
- **Device Management (DMG) Engineer** – Responsible for multiple assigned technical tasks including research, analysis, troubleshooting, product installation, system integration, and complex root cause analysis of managed security solutions
- **Security Analyst** - **Monitors client security systems and events** to detect and investigate threats, and work regularly with client teams to enhance current solutions to **improve client security posture**
- **Operations (Ops) Desk Analyst** – Responsible for providing direct **help-desk support** to end users, logs and tracks security incidents as reported by users via **phone calls/emails** or detected by SIEM tools, and updates status reports to relevant SOC staff. For more experienced staff, s/he may also help out in the security analyst tasks

A.2 Introduction to IBM Security QRadar SIEM

What is a SIEM?

Source: https://en.wikipedia.org/wiki/Security_information_and_event_management

- In the field of computer security, **security information and event management (SIEM)** software products and services combine **security information management (SIM) and security event management (SEM)**.
- The segment of security management that deals with real-time monitoring, correlation of events, notifications and console views is commonly known as ***security event management*** **(SEM)**.
- The second area provides long-term storage as well as analysis and reporting of log data, and is known as ***security information management*** **(SIM)**.
- The acronyms *SEM*, *SIM* and *SIEM* have been sometimes used interchangeably.
- They provide real-time analysis of security alerts generated by network hardware and applications.
- Vendors sell SIEM as software, as appliances or as managed services; these products are also used to log security data and generate reports for **compliance** purposes.
- Organizations are turning to big data platforms, such as Apache Hadoop, to complement SIEM capabilities by extending **data storage capacity** and **analytic flexibility**.
- The need for voice-centric visibility or **vSIEM (**voice security information and event management) provides a recent example of this evolution.

Introductory Youtube Videos on Use of IBM Security QRadar SIEM in a SOC:

- The Next Era for Security – IBM QRadar Security Intelligence Platform (2:48)
- A Look Inside IBM Security QRadar (4:57)

What is a SIEM? (cont.)

Source: https://en.wikipedia.org/wiki/Security_information_and_event_management

- The term ***security information event management*** **(SIEM)** is coined by Mark Nicolett and Amrit Williams of Gartner in 2005.
- It should have the following basic functions:
  - the product capabilities of gathering, analyzing and presenting information from network and security devices
  - identity and access-management applications
  - vulnerability management and policy compliance tools
  - operating-system, database and application logs
  - external threat data/intelligence feeds
- A key focus is to monitor and help manage user and service privileges, directory services and other system-configuration changes; as well as providing log auditing and review and incident response.

See also: AlienVault – SIEM for Beginners

https://www.alienvault.com/docs/whitepapers/SIEM-for-Beginners.pdf

SIEM Capabilities

Source: https://en.wikipedia.org/wiki/Security_information_and_event_management

- **Data aggregation**: Log management aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.
- **Correlation**: looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information. Correlation is typically a function of the Security Event Management portion of a full SIEM solution.
- **Alerting**: the automated analysis of correlated events and production of alerts, to notify recipients of immediate issues. Alerting can be to a dashboard, or sent via third party channels such as email.
- **Dashboards**: Tools can take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern.
- **Compliance**: Applications can be employed to automate the gathering of compliance data, producing reports that adapt to existing security, governance and auditing processes
- **Retention**: employing long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements. Long term log data retention is critical in forensic investigations as it is unlikely that discovery of a network breach will be at the time of the breach occurring.
- **Forensic analysis**: The ability to search across logs on different nodes and time periods based on specific criteria. This mitigates having to aggregate log information in your head or having to search through thousands and thousands of logs.

Magic Quadrant for SIEM

Source: Gartner (December 2018)

Best Practices: Intelligent Detection

Best practices: Intelligent detection

1 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 Detect deviations to identify malicious activity

- Establish baseline behaviors
- Monitor and investigate anomalies
- Monitor network flows

3 React in real-time to exploits

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

Best practices: Intelligent detection

What is Security Intelligence?

What is Security Intelligence?

Security Intelligence

--noun

The real-time collection, normalization and analytics of the data generated by users, applications, and infrastructure that impacts the IT security and risk posture of an enterprise

Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation

IBM Security QRadar SIEM

IBM Training

IBM Security QRadar SIEM

Web-based command console for Security Intelligence

- Delivers actionable insight focusing security teams on high-probability incidents
  Employs rules-based correlation of events, flows, assets, topologies, and vulnerabilities
- Detects and tracks malicious activity over extended time periods, helping uncover advanced threats often missed by other solutions
  Consolidates "big data" security incidents within purpose-built, federated database repository
- Provides anomaly detection to complement existing perimeter defenses
  Calculates identity and application baseline profiles to assess abnormal conditions

Optimized threat analysis

Daily volume of events, flows, incidents

2,000,000,000

automatically analyzed to find

20 – 25

potential offenses to investigate

IBM Security QRadar SIEM

IBM Security QRadar Vulnerability Manager

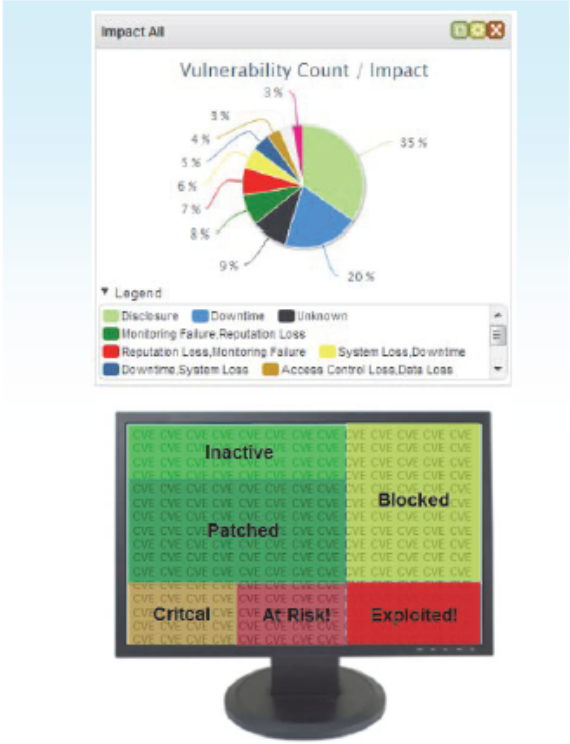
IBM Training

IBM Security QRadar Vulnerability Manager

Scan, assess, and remediate vulnerabilities

QRadar® Vulnerability Manager

- Contains an embedded, well proven, scalable, analyst recognized, PCI-certified scanner
- Detects 70,000+ vulnerabilities
- Tracks National Vulnerability Database (CVE)
- Is present in all QRadar log and flow collectors and processors
- Integrates with IBM Security Endpoint Manager (BigFix) to reveal which vulnerabilities will be patched and when
- Leverages QRadar Risk Manager to report which vulnerabilities are blocked by your IPS and FW
- Uses QFlow report if a vulnerable application is active
- Presents a prioritized list of vulnerabilities you should deal with as soon as possible



IBM Security QRadar Vulnerability Manager

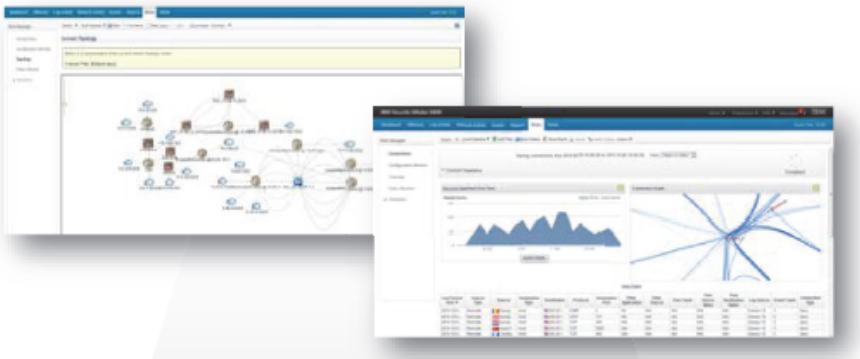
IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager

Scan, assess, and remediate risks

QRadar® Vulnerability Manager

- Network topology model based on security device configurations enables visualization of actual and potential network traffic patterns
- Policy engine correlates network topology, asset vulnerabilities and configuration, and actual network traffic to quantify and prioritize risk, enabling risk-prioritized remediation and compliance checking, alerting, and reporting
- Centralizes network security device configuration data and discovers configuration errors; monitors firewall rule activity
- Models threat propagation and simulates network topology changes



Asset risk quantification

Remediation prioritization

Network topology

Policy and compliance monitoring

Threat simulations

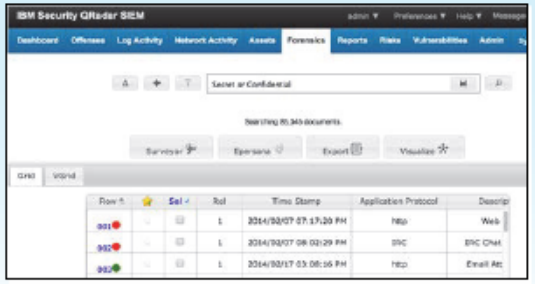
IBM Security QRadar Incident Forensics

IBM Security QRadar Incident Forensics

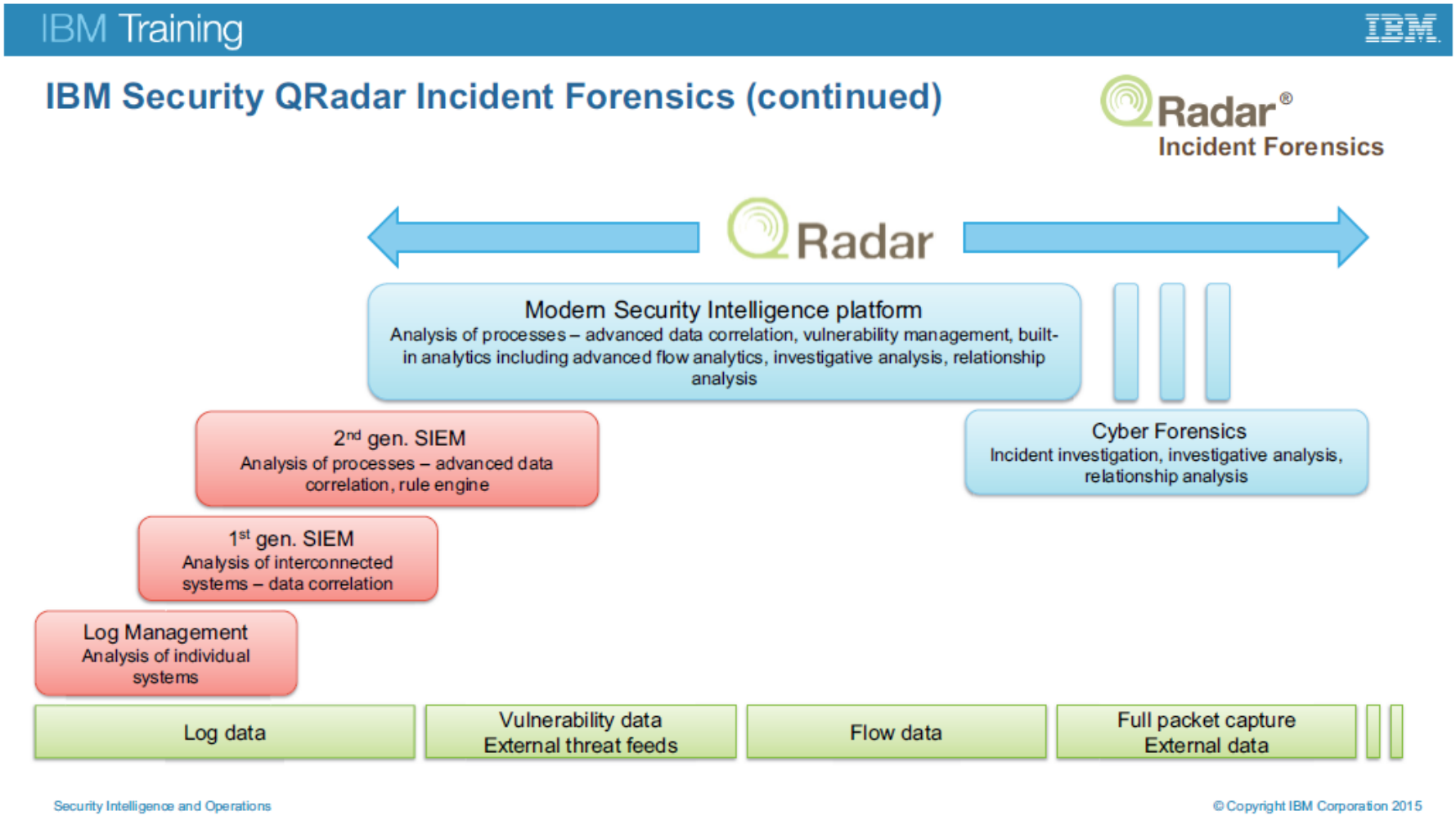
Intuitive investigation of security incidents

QRadar® Incident Forensics

- Reduces incident investigation periods from days or hours to minutes
  Employs Internet search engine technology to close security team skill gaps
- Compiles evidence against malicious entities breaching secure systems and deleting or stealing sensitive data
  Creates rich "digital impression" visualizations of related content
- Helps determine root cause of successful breaches to prevent or reduce recurrences
  Adds full packet captures to complement SIEM security data collection and analytics

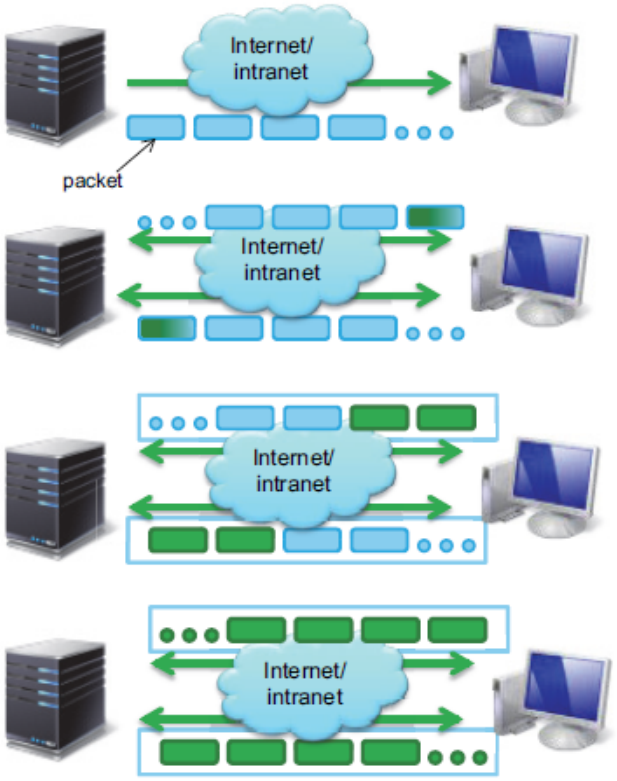


IBM Security QRadar Incident Forensics (cont.)



IBM Security QRadar Incident Forensics (continued)

From NetFlow to QFlow to QRadar Incident Forensics



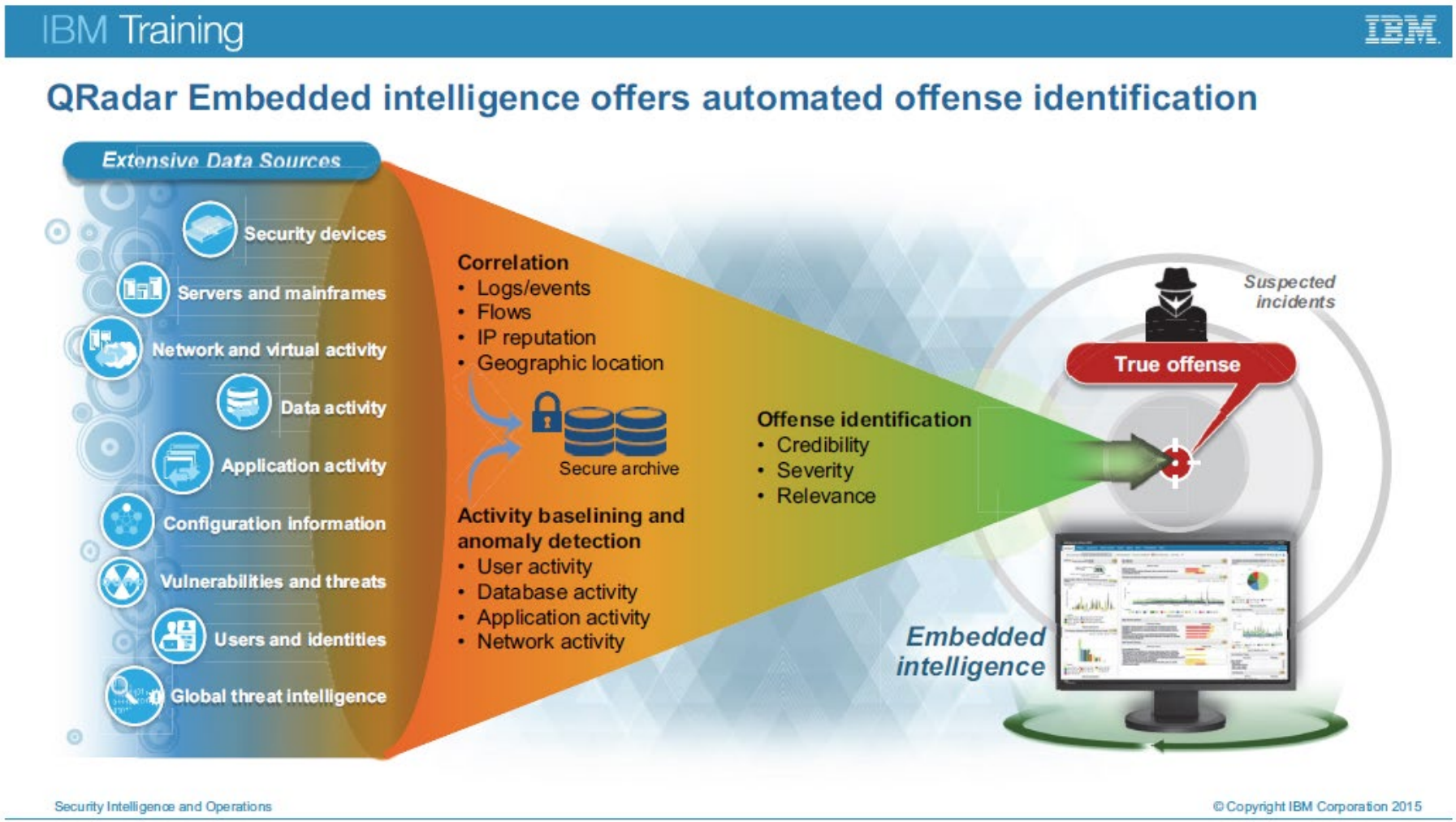
Netflow: packet oriented, identifies unidirectional sequences sharing source and destination IPs, ports, and type of service

QFlow: packet oriented, identifies bidirectional 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.

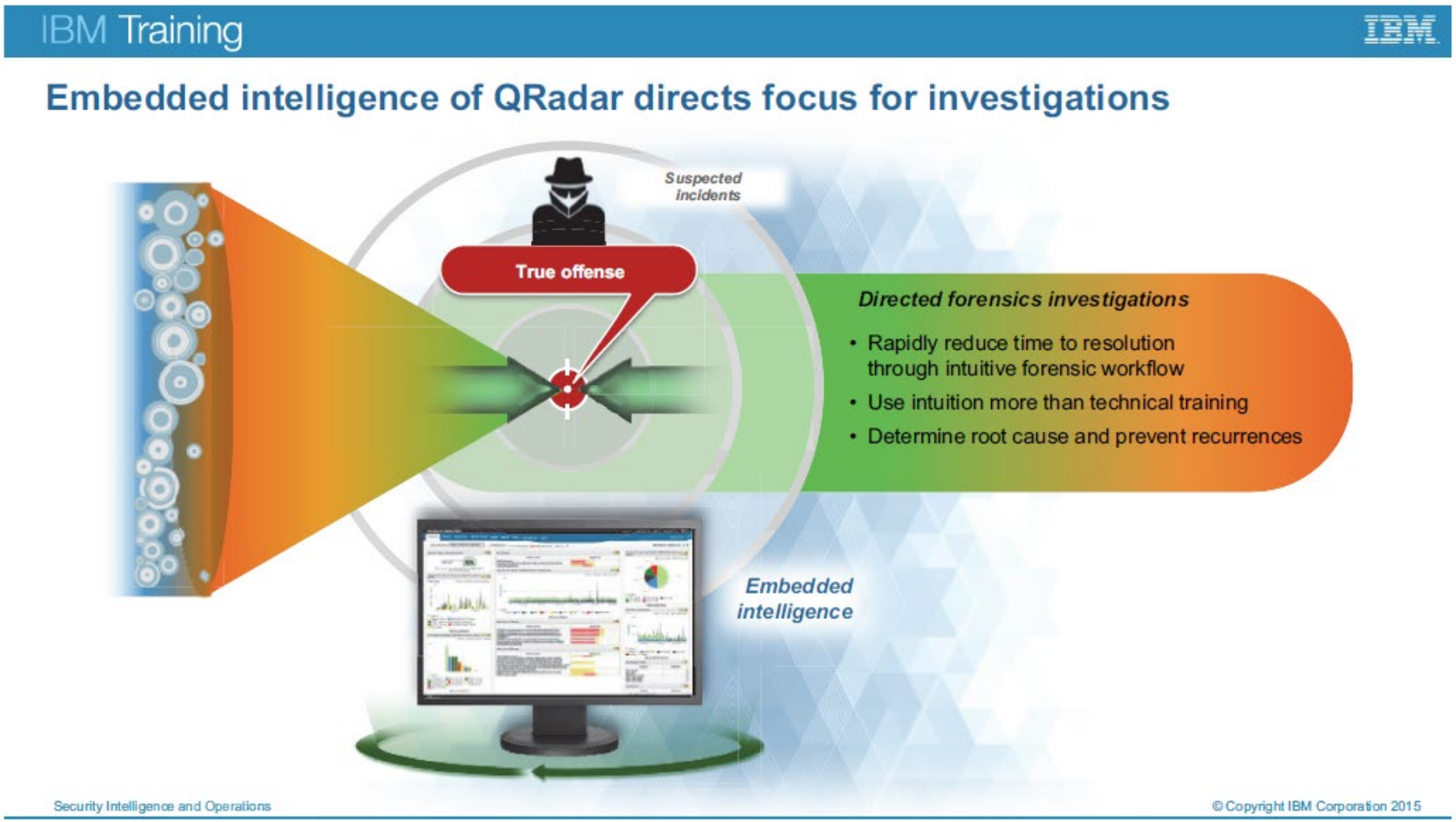
QRadar Incident Forensics: session oriented, captures all packets in a flow indexing the metadata and payload to enable fast search-driven data exploration

QRadar Embedded Intelligence



QRadar Embedded intelligence offers automated offense identification

QRadar Embedded Intelligence (cont.)



Embedded intelligence of QRadar directs focus for investigations

Benefits of IBM Security Intelligence approach

Benefits of IBM Security Intelligence approach

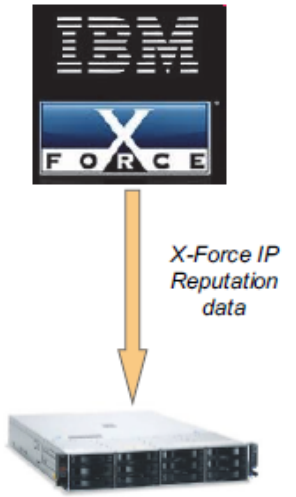
- Holistic IT security management and integration with infrastructure and processes
  - Use tools and solutions that know how to communicate with each other
  - Integrate with centralized vulnerability management
- Pro-active IT security management
  Detect and counteract the threat before the actual exploit
- Network flow analysis and forensics
  Collect data that no attacker can obfuscate (network flow) and store application data for more detailed forensic investigations
- Risk assessment support through network topology awareness in combination with vulnerability information
  - Investigate potential risks due to network topology and vulnerabilities
  - Focus on the "important and valuable" assets that need protection and do not flood the Security Intelligence system with useless data

Benefits of IBM Security Intelligence approach

IBM Security X-Force Threat Intelligence

IBM Security X-Force Threat Intelligence

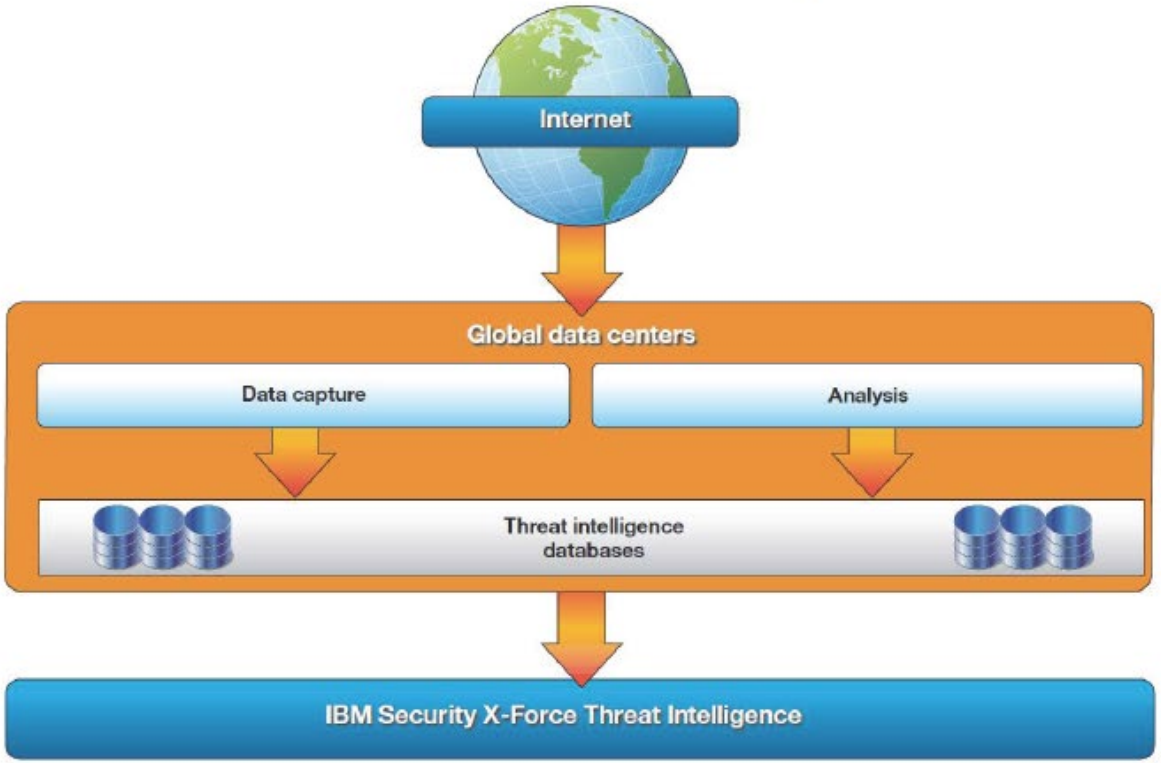
- Purpose
  To further enrich the threat detection capabilities in QRadar using the IBM X-Force Threat Intelligence data on a subscription basis
- X-Force Threat Intelligence
  X-Force represents the IBM security threat research team that collects and maintains comprehensive Internet threat and reputation data such as spam servers, botnet command and control servers, malware distribution points, anonymous proxies, and dynamic and dialup network address ranges
- Integration with QRadar
  - X-Force Threat Intelligence data is constantly updated and maintained, with updates being pushed out continuously to subscribing QRadar appliances
  - Any QRadar event and flow activity involving X-Force Threat Intelligence addresses is automatically flagged in offenses, rules, and reports; this data can be used to identify new threats or validate threats detected through existing QRadar means
- Ordering
  Each appliance in a deployment needs to subscribe this service



The Value of IBM X-Force R&D Team

IBM Training

The value of the IBM X-Force research and development team



Security Intelligence functional components

The value of the IBM X-Force research and development team

X-Force Threat Intelligence - Vulnerability Coverage Use Cases

X-Force Threat Intelligence - vulnerability coverage use cases

Security issue	Insight provided
A series of attempted logins from a dynamic range of IP addresses	Malicious attacker
An anonymous proxy connection to a business partner portal	Suspicious behavior
A connection from a non-mail server with a known spam host	Spam contamination
A connection between an internal endpoint and a known botnet command and control server	Botnet infection
Communication between an endpoint and a known malware distribution site	Malware attack

X-Force Threat Intelligence - vulnerability coverage use cases

Summary

SOC and SIEM Concepts

A.1 Overview of SOC Operations

- What is a SOC?
- Overview of a SOC
- Functions of a SOC
- SOC Framework
- SOC Processes & Procedures
- SOC Key Job Roles & Responsibilities

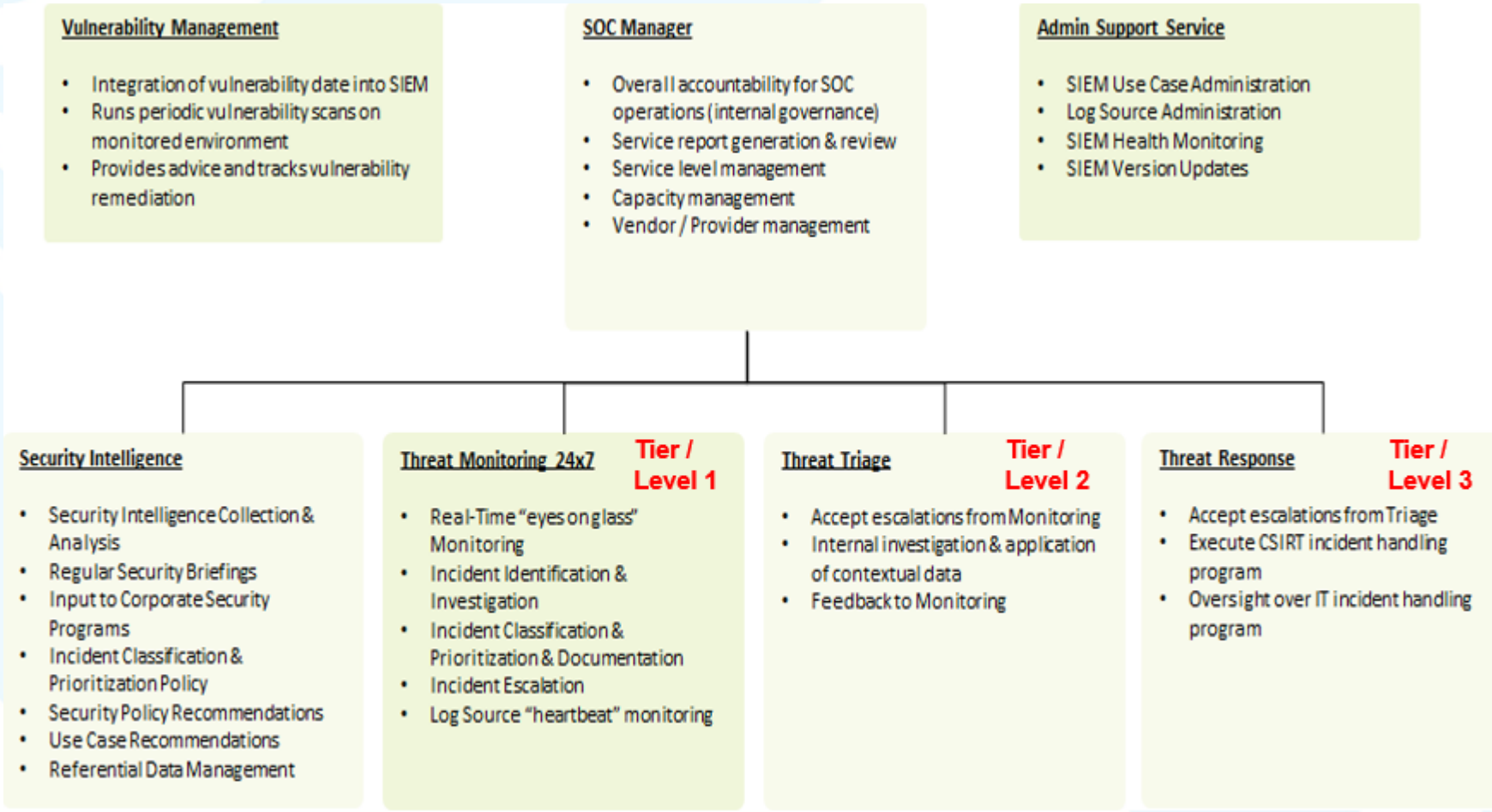
A.2 Introduction to IBM Security QRadar SIEM

- What is SIEM?
- SIEM Capabilities
- What is Security Intelligence?
- IBM Security QRadar SIEM
- IBM Security QRadar Vulnerability Manager
- IBM Security QRadar Risk Manager
- IBM Security QRadar Incident Forensics
- IBM Security X-Force Threat Intelligence

A.3 Managing Cyber Security Incidents in a SOC

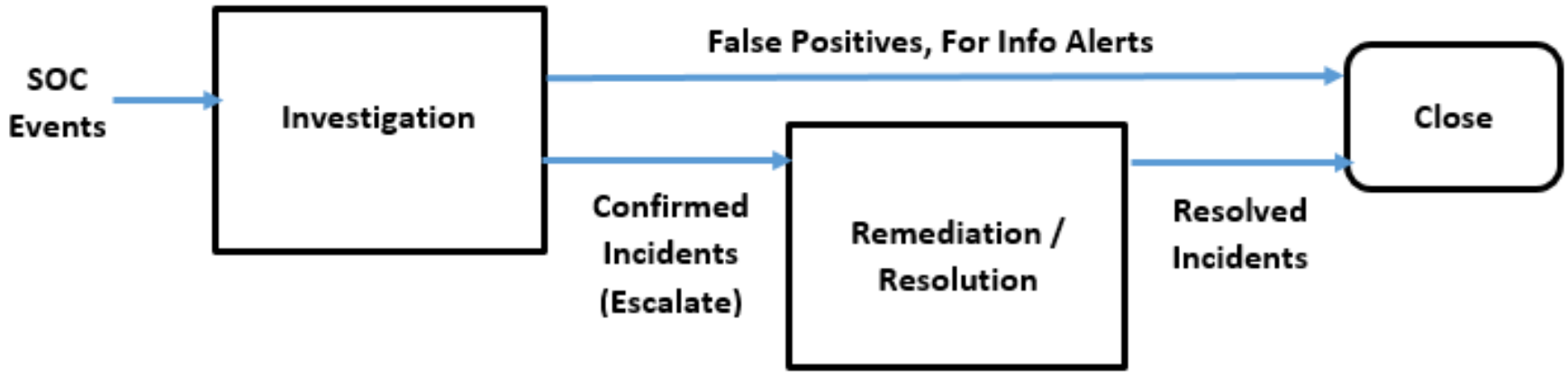
Typical SOC Setup in Temasek Polytechnic

Organization Chart:



Typical SOC Incident Escalation Workflow

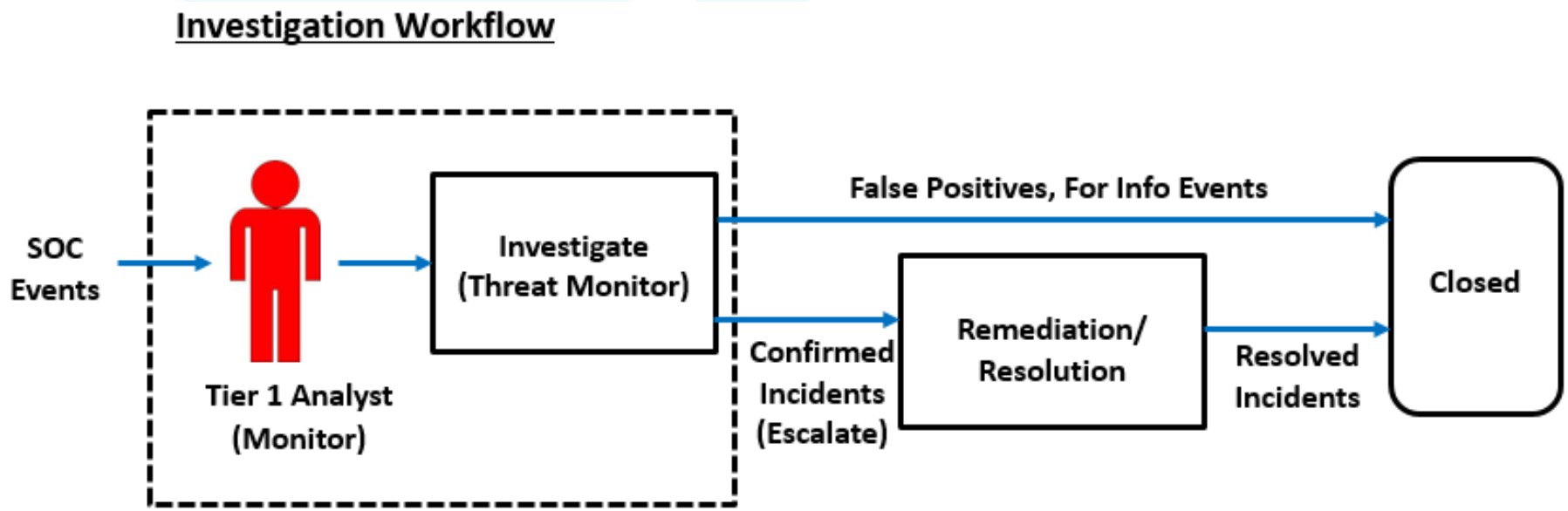
SOC High-Level Workflow



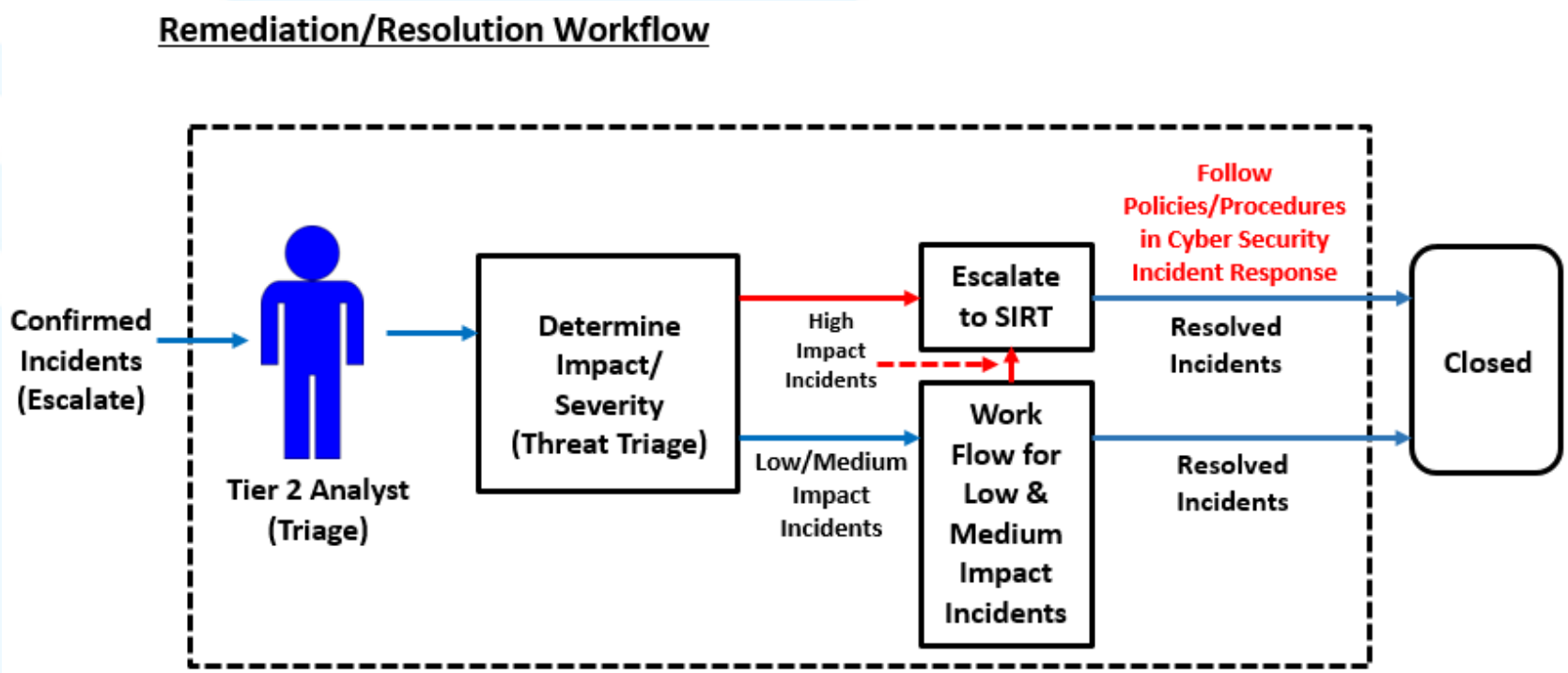
Example Service Level Objectives / Service Level Agreements (SLOs/SLAs)

Impact / Severity	SLO / SLA
High	15 mins
Medium	1 hour
Low	48 hours

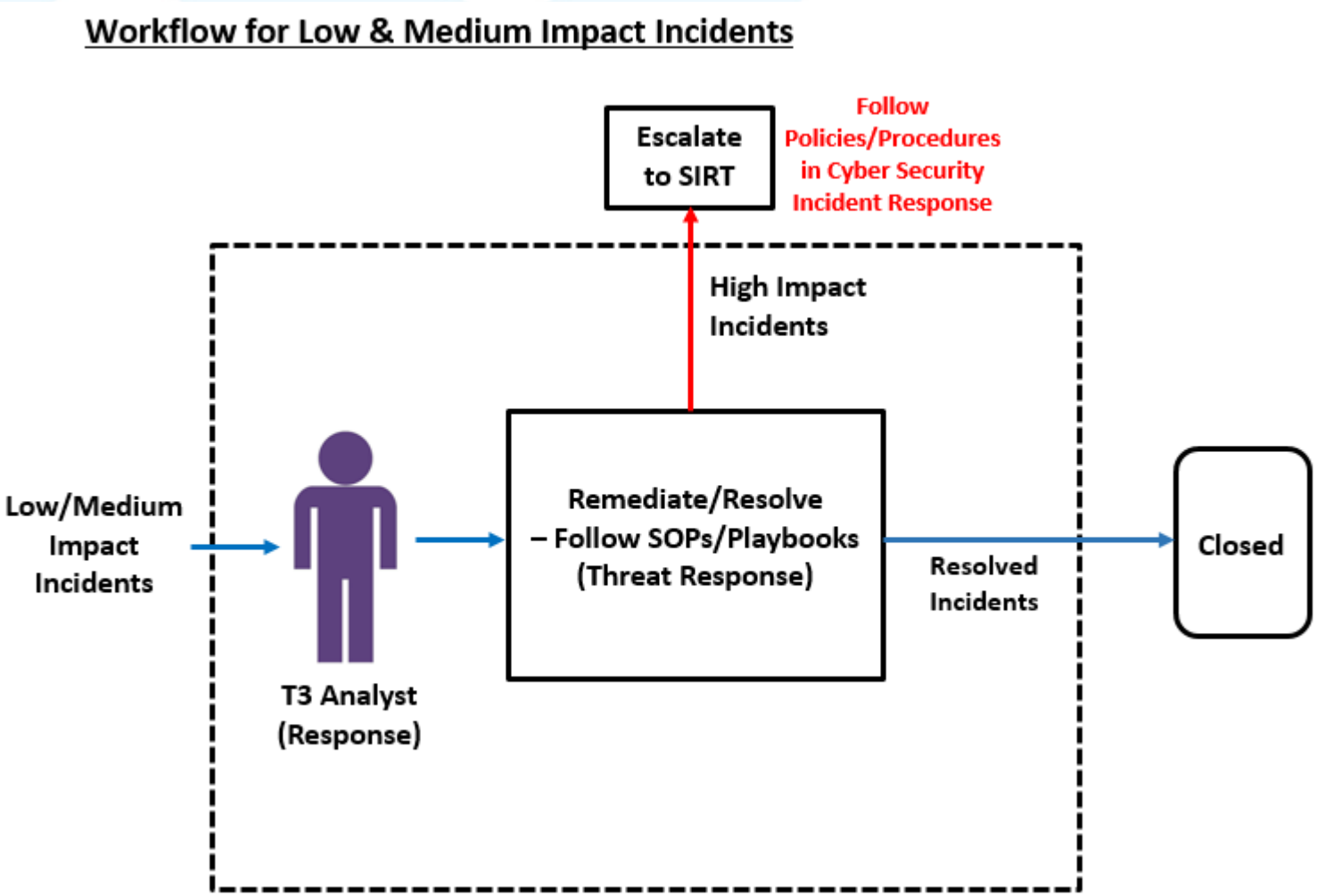
Typical SOC Incident Escalation Workflow



Typical SOC Incident Escalation Workflow (cont.)



Typical SOC Incident Escalation Workflow (cont.)



A.4 IBM Security QRadar SIEM Capabilities

IBM Security QRadar SIEM Capabilities

First, let's discuss the powerful **IBM Security QRadar SIEM capabilities** that are essential to carry out effective **investigations of network offenses**.

- IBM Security QRadar SIEM provides deep visibility into network, user, and application activity.
- It provides collection, normalization, correlation, and secure storage of events, flows, assets, and vulnerabilities.
- QRadar SIEM classifies suspected attacks and policy breaches as **offenses**.
- You will learn how to perform the following tasks:
  - Describe how QRadar SIEM collects data to detect suspicious activities
  - Navigate and customize the QRadar SIEM dashboard
  - Investigate suspected attacks and policy breaches
  - Search, filter, group, and analyze security data
  - Use QRadar SIEM to create customized reports

Reference: IBM Security Qradar SIEM Foundations (BQ102)

Purposes of QRadar SIEM

The IBM Security QRadar SIEM licensed program performs these tasks

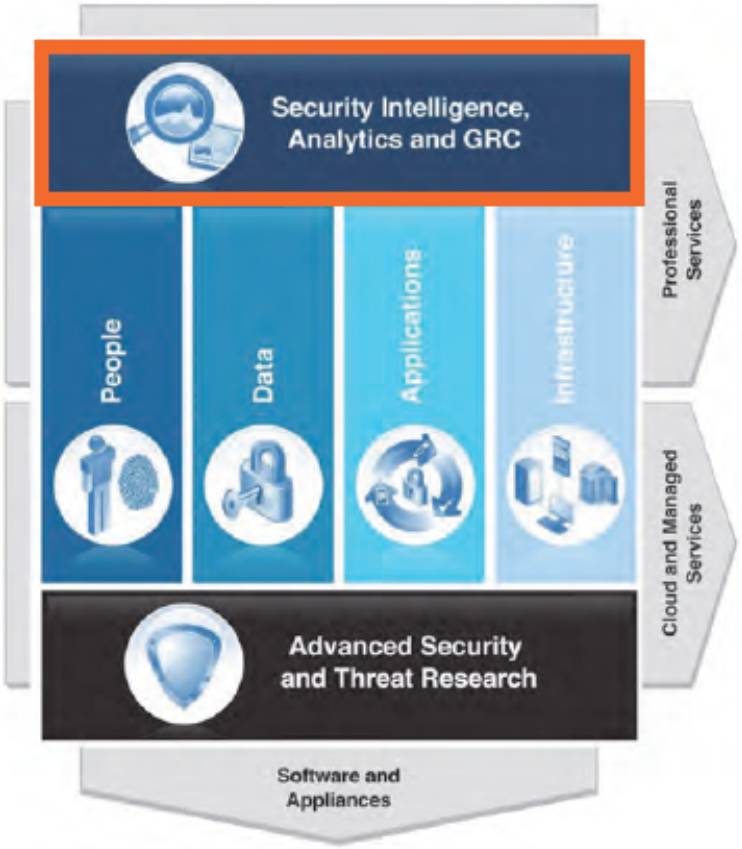
- Alerts to suspicious activities and policy breaches in the IT environment
- Provides deep visibility into network, user, and application activity
- Puts security-relevant data from various sources in context with each other
- Provides reporting templates to meet operational and compliance requirements
- Provides reliable, tamper-proof log storage for forensic investigations and evidentiary use

"Our most formidable challenge is getting companies to detect that they have been compromised."

Kimberly K. Peretti,
Senior Counsel,
US Dept. of Justice (DoJ)

Purposes of QRadar SIEM

QRadar SIEM and the IBM Security Framework



In the IBM Security Framework, QRadar SIEM offers these capabilities

- Security Intelligence, Analytics and Governance, Risk Management, and Compliance (GRC)
- Insight into all domains of the IBM Security Framework

QRadar SIEM and the IBM Security Framework

Identifying suspected attacks and policy breaches

QRadar SIEM helps answer the following key questions

- What is being attacked?
- What is the security impact?
- Who is attacking?
- Where should the investigation be focused?
- When are the attacks taking place?
- How is the attack penetrating the system?
- Is the suspected attack or policy breach real or a false alarm?

Providing context

To enable security analysts to perform investigations, QRadar SIEM correlates information such as these examples

- Point in time
- Offending users
- Origins
- Targets
- Vulnerabilities
- Asset information
- Known threats

Providing context

Key QRadar SIEM capabilities

- Ability to process security-relevant data from a wide variety of sources, such as these examples
  - Firewalls
  - User directories
  - Proxies
  - Applications
  - Routers
- Collection, normalization, correlation, and secure storage of raw events, network flows, vulnerabilities, assets, and threat intelligence data
- Layer 7 payload capture up to a configurable number of bytes from unencrypted traffic

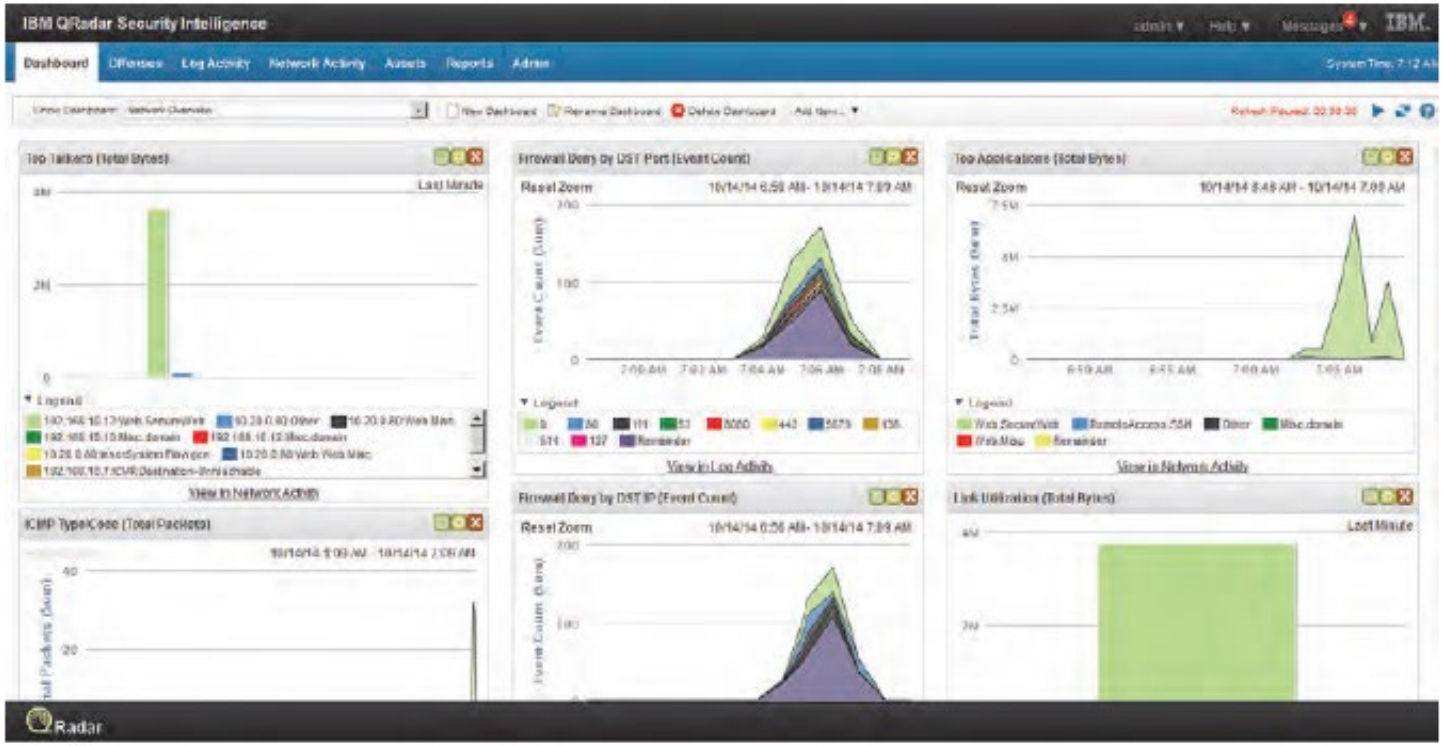
Key QRadar SIEM capabilities

Key QRadar SIEM capabilities (cont.)

- Comprehensive search capabilities
- Monitor host and network behavior changes that could indicate an attack or policy breach such as these examples
  - Off hours or excessive usage of an application or network activity patterns inconsistent with historical profiles
  - Prioritization of suspected attacks and policy breaches
- Notification by email, SNMP, and others
- Many generic reporting templates included
- Scalable architecture to support large deployments
- Single user interface

Key QRadar SIEM capabilities (continued)

QRadar SIEM Console



The console provides one integrated user interface for all tasks

Collecting and Processing Events & Flows

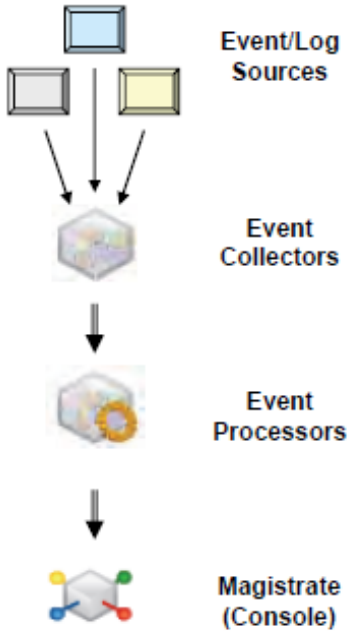
Normalizing raw events

- An *event* is a record from a device that describes an action on a network or host
- QRadar SIEM normalizes the varied information found in raw events
  - Normalizing means to map information to common field names, for example
    - SRC_IP, Source, IP, and others are normalized to **Source IP**
    - user_name, username, login, and others are normalized to **User**
  - Normalized events are mapped to high-level and low-level categories to facilitate further processing
- After raw events are normalized, it is easy to search, report, and cross-correlate these normalized events

Event collection and processing

- *Log Sources* typically send syslog messages, but they can use other protocols also
- *Event Collectors* receive raw events as log messages from a wide variety of external log sources

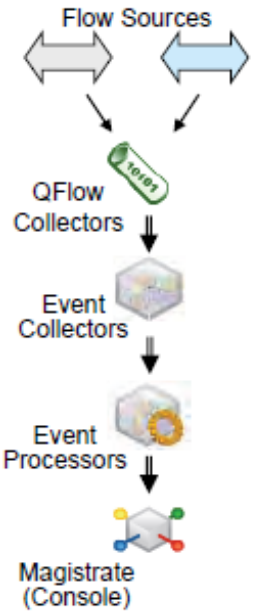
  Device Support Modules (DSMs) in the event collectors parse and normalize raw events; raw log messages remain intact
- *Event Processors* receive the normalized events and raw events to analyze and store them
- *Data Nodes* (not pictured) provide additional storage for event and flow data
- *Magistrate* correlates data from event processors and creates offenses



Event collection and processing

Event collection and processing (cont.)

- A *flow* is a communication session between two hosts
- QFlow Collectors read packets from the wire or receive flows from other devices

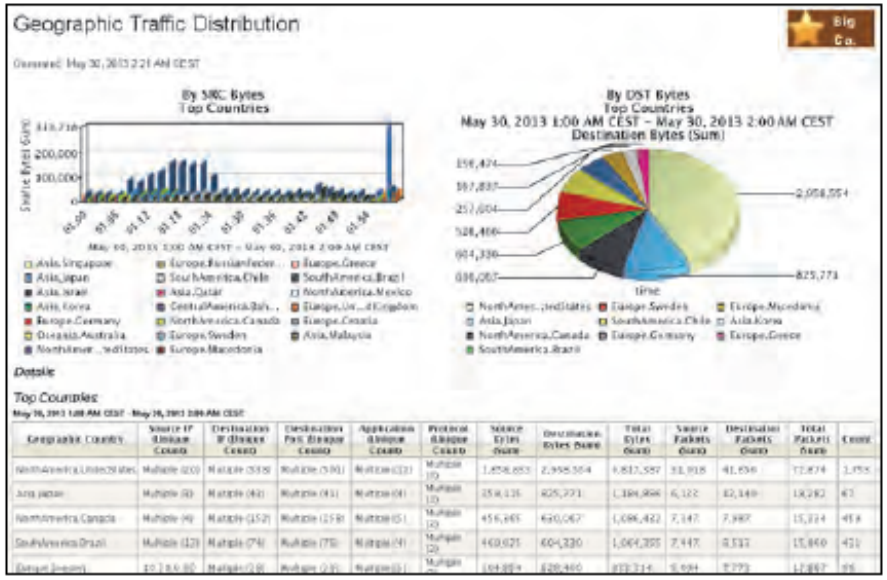


- QFlow Collectors convert all gathered network data to flow records similar normalized events; they include such details as when, who, how much, protocols, and options.

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes	Source Packets	Destination Packets	ICMP Type/Code
	Oct 14, 2014, 7:00:13 AM	192.168....	61190	202.12.27.33	53	udp_ip	Misc.domain	101 (C)	0	1	0	N/A
	Oct 14, 2014, 6:59:59 AM	192.168....	64334	192.168.10.10	22	tcp_ip	RemoteAccess.SSH	380 (C)	3,376 (C)	4	4	N/A
	Oct 14, 2014, 7:00:53 AM	0.0.0.0	546	0.0.0.0	547	udp_ip	Other	612 (C)	0	4	0	N/A
	Oct 14, 2014, 6:59:59 AM	192.168....	64334	192.168.10.10	22	tcp_ip	RemoteAccess.SSH	3,816	64,432	48	52	N/A
	Oct 14, 2014, 6:59:59 AM	192.168....	64334	192.168.10.10	22	tcp_ip	RemoteAccess.SSH	4,132	65,256	51	54	N/A
	Oct 14, 2014, 7:00:00 AM	192.168....	61190	192.203.230.10	53	udp_ip	Misc.domain	101 (C)	0	1	0	N/A
	Oct 14, 2014, 7:00:53 AM	0.0.0.0	546	0.0.0.0	547	udp_ip	Other	459 (C)	0	3	0	N/A
	Oct 14, 2014, 7:00:24 AM	192.168....	64348	192.168.10.10	443	tcp_ip	Web.SecureWeb	3,559	24,010	19	23	N/A
	Oct 14, 2014, 7:00:05 AM	192.168....	61709	192.168.10.1	53	udp_ip	Misc.domain	101 (C)	0	1	0	N/A
	Oct 14, 2014, 6:59:59 AM	192.168....	61897	192.168.99.1	53	udp_ip	Misc.domain	78	0	1	0	N/A
	Oct 14, 2014, 7:00:01 AM	192.168....	64335	192.168.10.10	443	tcp_ip	Web.SecureWeb	192	297	3	4	N/A
	Oct 14, 2014, 7:00:05 AM	192.168....	N/A	192.168.10.12	N/A	icmp_ip	ICMPDestinationUnreachable	120 (C)	0	1	0	Port Unreac...

Flow collection and processing

Reporting



- All collected information is available for reports
- Thousands of report templates are available
- With the report wizard, you can create new templates and change existing templates

Collecting and Processing Vulnerability Data

Asset profiles

QRadar SIEM maintains asset profiles for systems in the network; the profiles track host details, such as these examples

- IP addresses
- Services listening on open ports
- Vulnerabilities

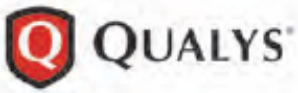
Id	IP Address	Asset Name	Aggregate CVSS Score	Vulnerabilities	Services
1030	10.111.219.138	10.111.219.138	0.0	0	0
1013	10.117.220.204	10.117.220.204	0.0	0	0
1014	10.117.220.205	10.117.220.205	0.0	0	0
1012	10.117.254.16	10.117.254.16	0.0	0	0
1011	10.117.254.36	10.117.254.36	0.0	0	0
1010	10.117.254.66	10.117.254.66	0.0	0	0
1009	10.15.20.140	10.15.20.140	0.0	0	0
1015	10.2.100.66	10.2.100.66	0.0	0	0
1018	10.20.0.80	10.20.0.80	0.0	0	0
1007	128.245.120.152	128.245.120.152	0.0	0	0
1019	172.16.254.2	chkpt1	0.0	0	0

Asset profiles

Active scanners

For vulnerability assessment (VA) and maintaining asset profiles, QRadar SIEM integrates with many active scanners

- You can schedule Nessus, Nmap, and IBM Security QRadar Vulnerability Manager scanner directly in QRadar SIEM
- For other scanners, you schedule only the collection of scan results in QRadar SIEM but not the scan itself

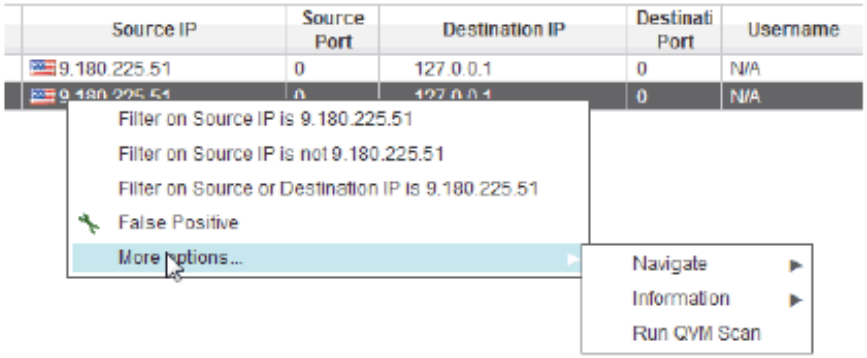


QRadar Vulnerability Manager scanner

You can add the separate product IBM Security QRadar Vulnerability Manager licensed program with QRadar SIEM

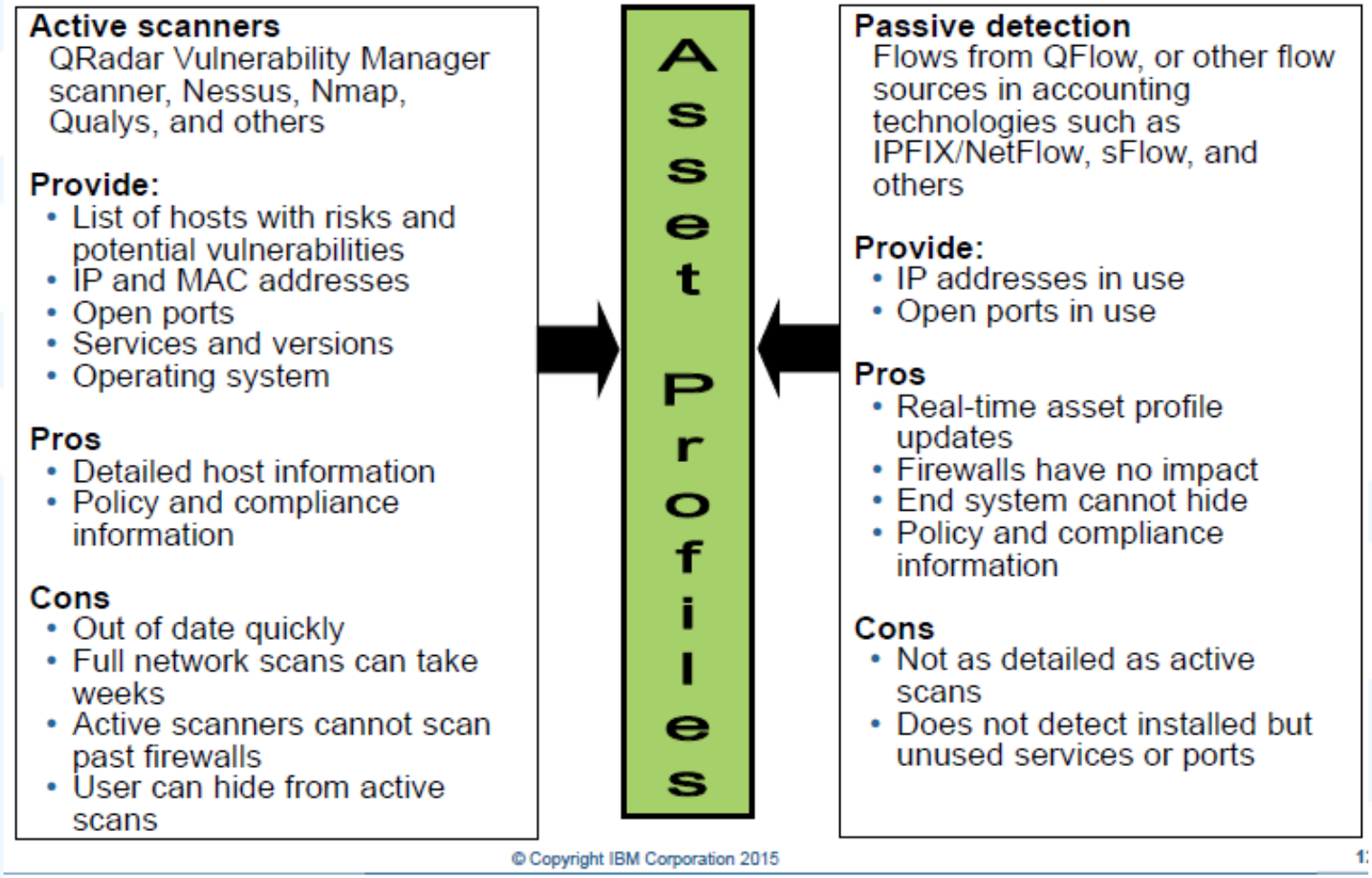
It provides these benefits

- Active scanner present on all QRadar event and flow collectors and processors
- Detects 70,000+ vulnerabilities



- Processes results from IBM-hosted scanner to see a view from outside your firewall
- Tracks *Common Vulnerabilities and Exposures* (CVE)
- Third-party vulnerability data feeds

Gathering asset information



Gathering asset information

Using the QRadar SIEM Dashboard

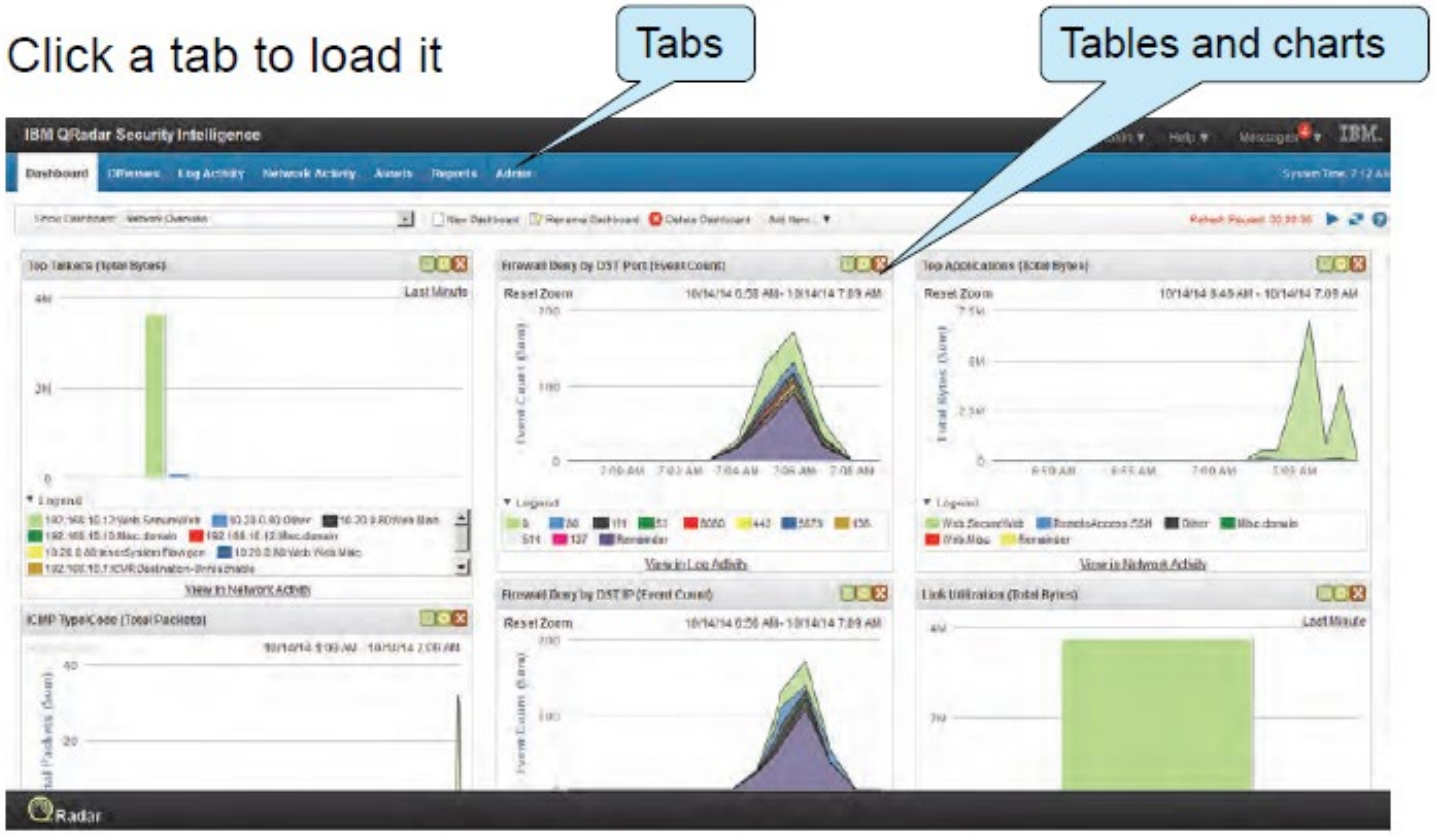
- Navigating the Dashboard tab
- Customizing a Dashboard

Navigating the Dashboard tab

Dashboard overview

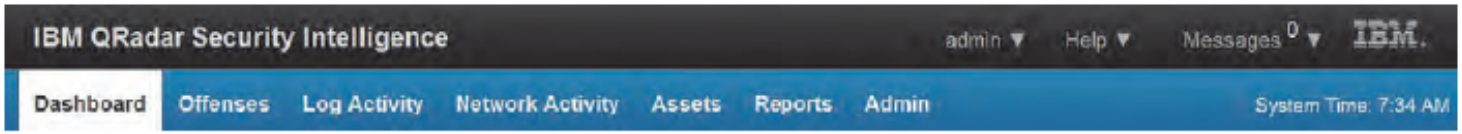
- QRadar SIEM shows the **Dashboard** tab when you log in
- You can create multiple dashboards
- Each dashboard can contain items that provide summary and detailed information
- Seven default dashboards are available
- You can create custom dashboards to focus on your security or operations responsibilities
- Each dashboard is associated with a user; changes that you make to a dashboard do not affect the dashboards of other users

Default dashboard



Default dashboard

QRadar SIEM tabs

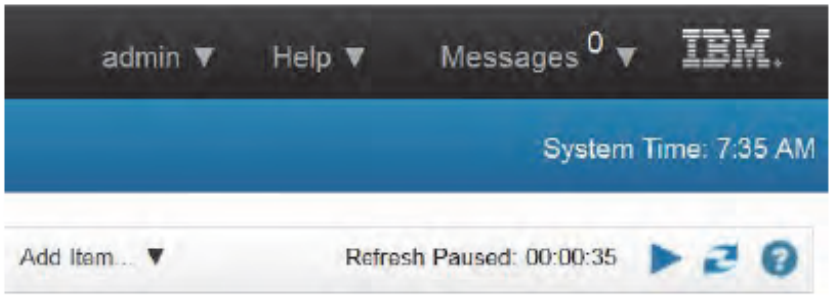


Use tabs to navigate the primary QRadar SIEM functions

- **Dashboard**: The initial summary view
- **Offenses**: Displays offenses; list of prioritized incidents
- **Log Activity**: Query and display events
- **Network Activity**: Query and display flows
- **Assets**: Query and display information about systems in your network
- **Reports**: Create templates and generate reports
- **Admin**: Administrative system management

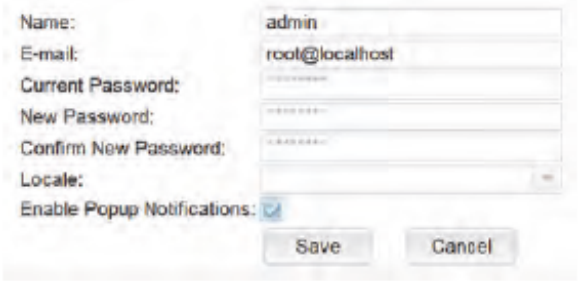
QRadar SIEM tabs

Other menu options



The dashboard has the following additional menu options

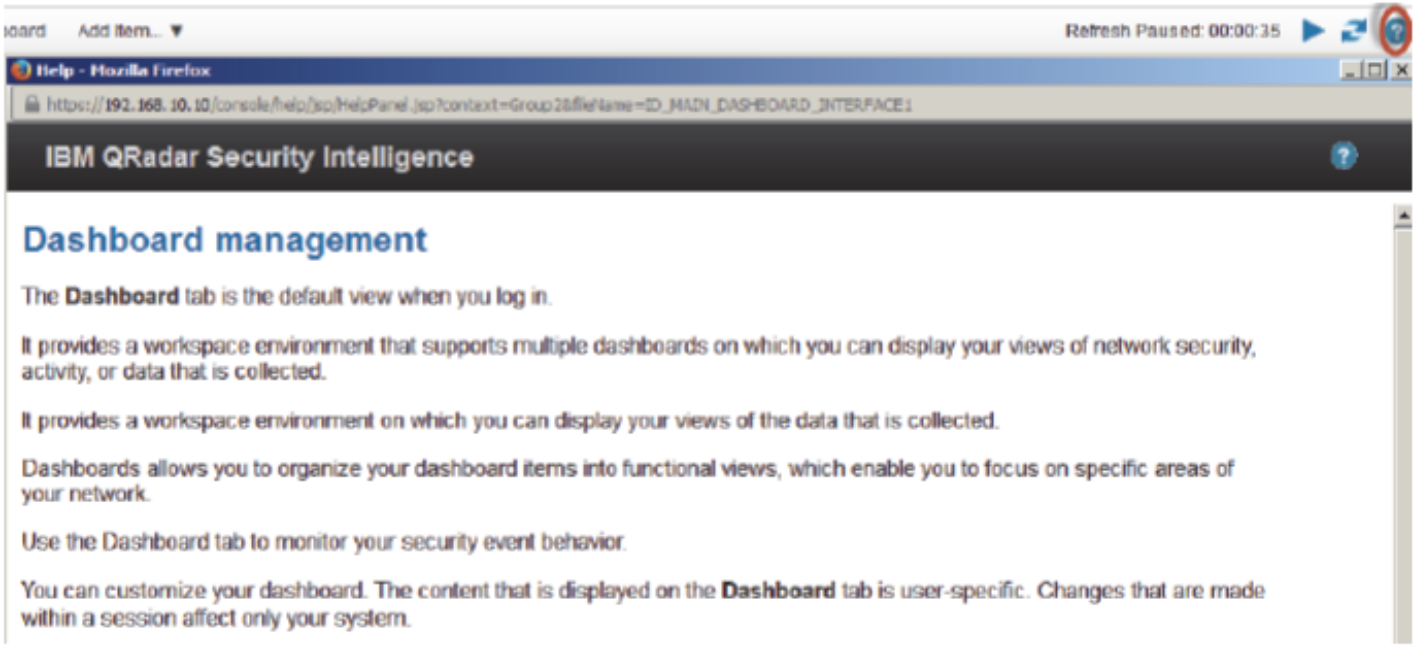
- **User Preferences**
- **Help**
- **Log out**



Other menu options

Context-sensitive help

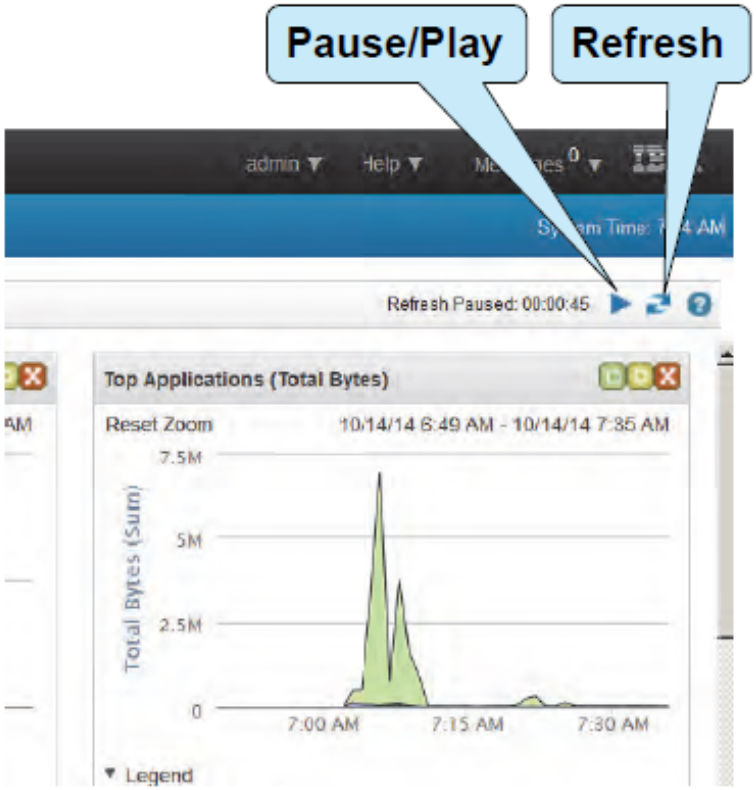
Click the question mark in any window to access help for the current page



Context-sensitive help

Dashboard refresh

- In the displayed dashboard, events and flows refresh every minute unless you click **Pause**
- Use the **Refresh** button to manually refresh the displayed data



Dashboard refresh

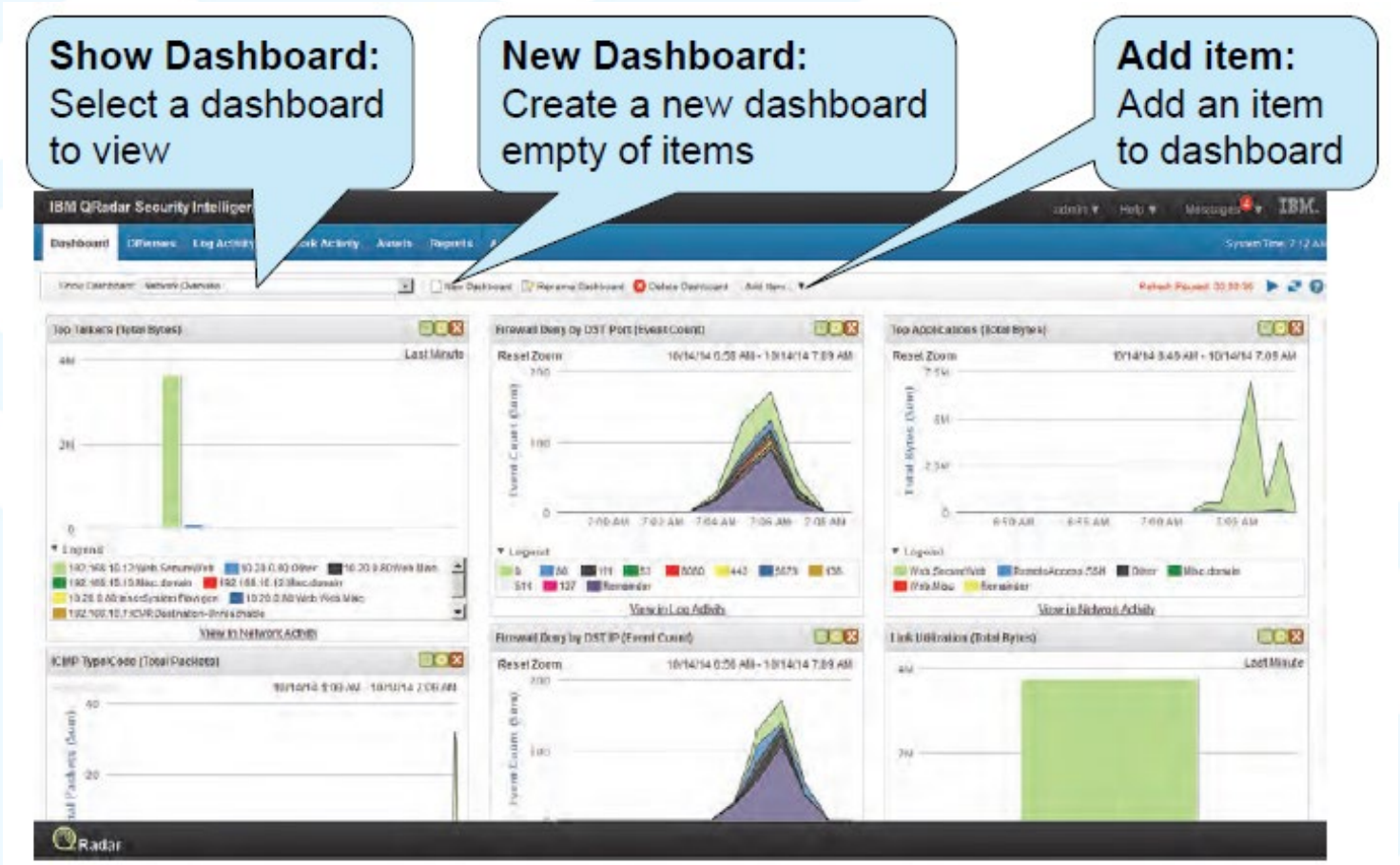
Customizing a Dashboard

Dashboard variety

- QRadar SIEM includes the following default dashboards
  - Application Overview
  - Compliance Overview
  - Network Overview
  - System Monitoring
  - Threat and Security Monitoring
  - Virtual Cloud Infrastructure
  - Vulnerability Management
- Use multiple dashboards to better organize data; for example, a single user can have the following dashboards to show log and network activity of these systems
  - Databases
  - Critical Applications

Dashboard variety

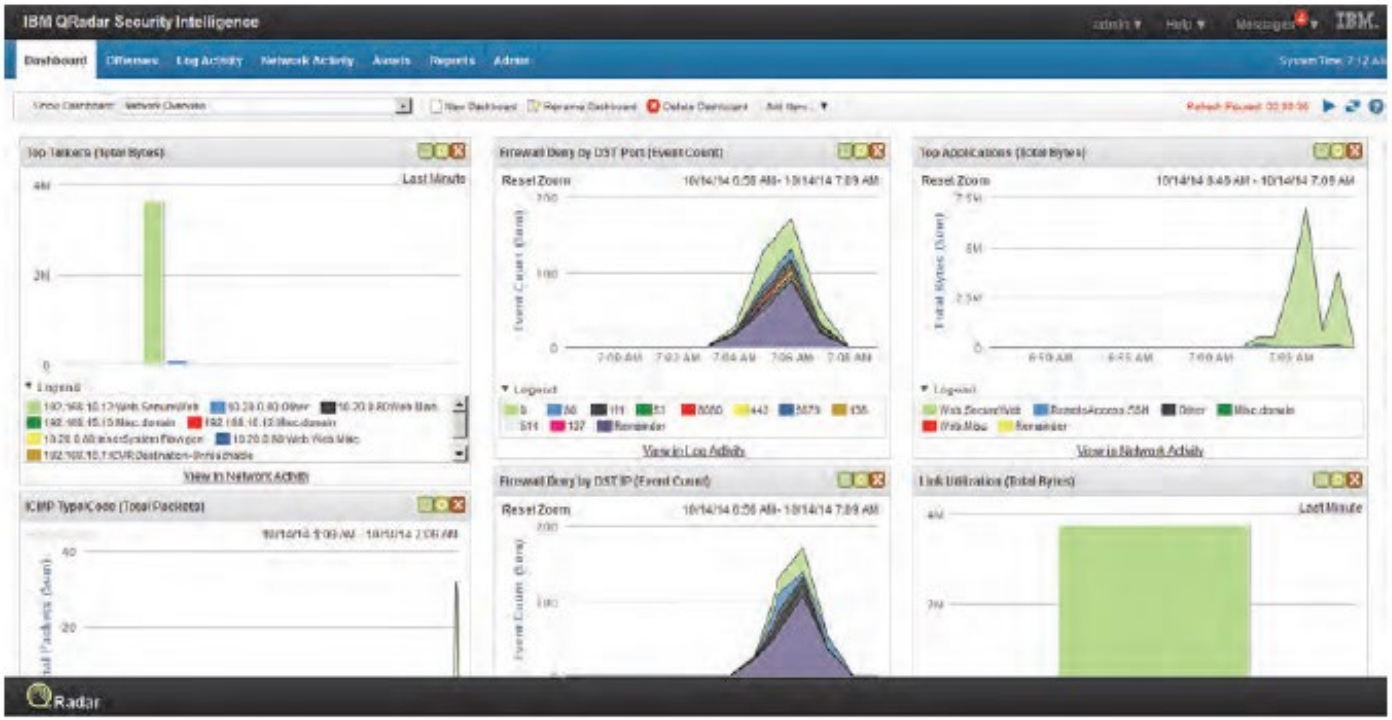
Creating a custom dashboard



Creating a custom dashboard

Number of items on dashboard

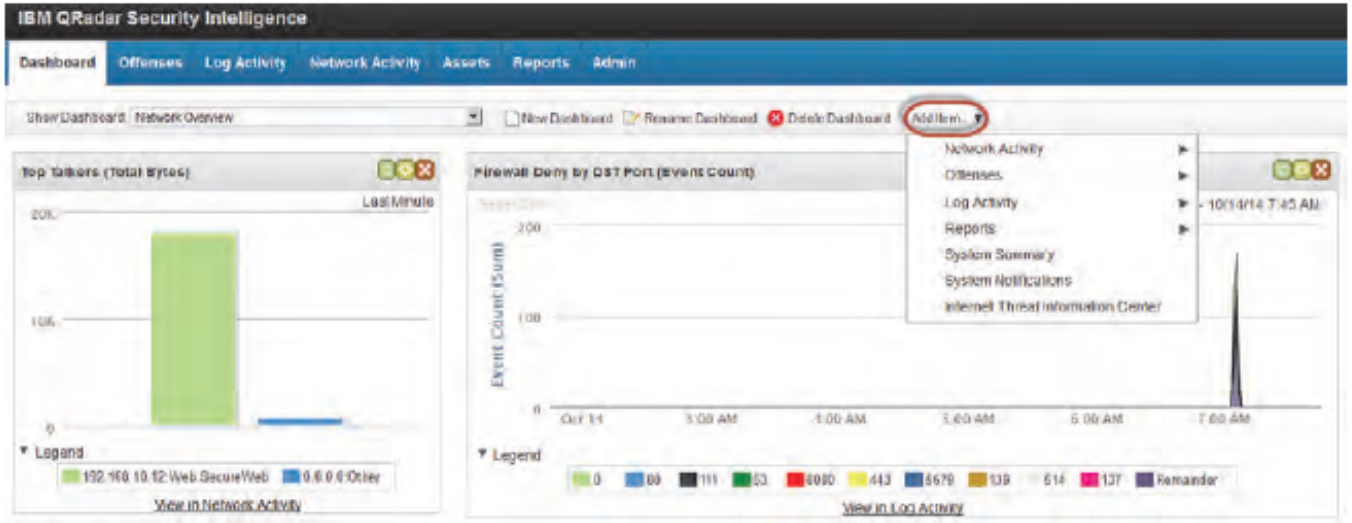
Include no more than 15 items on each dashboard



Items

Managing dashboard items

Click **Add Item** to place additional objects on the dashboard
Click the green icon to detach the object from the interface to the desktop
Click the yellow icon to modify the settings of an object
Click the red icon to delete an object from the dashboard



Summary

SOC and SIEM Concepts

A.3 Managing Cyber Security Incidents in a SOC

Typical SOC Setup in Temasek Polytechnic

- SOC Manager
- Threat Monitoring (Tier 1)
- Threat Triage (Tier 2)
- Threat Response (Tier 3)
- Security Intelligence
- Vulnerability Management
- Administration Support Service

Typical SOC Incident Escalation Workflow

- Service Level Objectives/Service Level Agreements (SLOs/SLAs) for High/Medium/Low Impact Incidents
- Tier 1 Analyst (Threat Monitoring & Incident escalation)
- Tier 2 Analyst (Threat Triage – Determine impact/severity level)
- Tier 3 Analyst (Threat Response – Incident resolution/remediation)
- Follow SOC SOPs/Playbooks
- Escalate to corporate SIRT for high impact security incidents

Summary (Cont.)

SOC and SIEM Concepts

A.4 IBM Security QRadar SIEM Capabilities

- QRadar SIEM Purpose
- Collecting and Processing Events & Flows
- Collecting and Processing Vulnerability Data
- Using the QRadar SIEM Dashboard
  - Navigating the Dashboard tab
  - Customizing a Dashboard

Hands-on Demo / Lab Exercises

Hands-on Demo / Lab Exercises

Hands-on Demo / Lab Exercises:

- Navigating IBM QRadar SIEM dashboard and tabs
- Video – A Look Inside IBM Security QRadar (4:57)