

IBM QRadar

Module 1: Introduction to Security Intelligence & Event Management

1. [Introduction to Security Intelligence & Event Management](#)
2. [Security technologies implemented in the IT Industry](#)
3. [SIEM Evolution](#)
4. [Introduction to SIEM](#)
5. [Benefits of SIEM](#)
6. [Introduction to IBM QRadar & Log Manager](#)
7. [Strengths](#)
8. [Log Management](#)

1. Security Intelligence & Event Management

SIEM systems collect, store, investigate, support mitigation and report on security data for incident response, forensics, and regulatory compliance.

Security and risk management leaders increasingly seek security information and event management solutions with capabilities that support early attack detection, investigation and response. Users should balance advanced SIEM capabilities with the resources needed to run and tune the solution. Several companies have developed SIEM software products to detect network attacks and anomalies in an IT system.

Gartner reports are the most relevant reports about this subject which analyze the SIEM tools available in the market provided by the top 14 leading SIEM vendors. According to these reports, the products can be classified into four groups based on two main features, the ability to execute and the completeness of vision.



2. Security technologies implemented in the IT Industry

The following technologies are implemented in building out a security infrastructure. Enterprise implements these in the aftermath of a major security data breach. Building infrastructure with all the security technologies provide the most robust risk.

- Advanced threat detection
- Network and desktop forensics
- Network and data leakage protection
- Behavioural-based analysis
- Security/threat intelligence feeds
- Threat forecasting and modelling
- Artificial Intelligence & Deep Learning
- Zero-Trust
- Firewall & Antivirus

3. SIEM Evolution

Before 2005, there used to be quite a debate over Security Information Management (SIM) and Security Event Management (SEM). This debate was ended for once and all by Amrit Williams and Mark Nicollet of Gartner when they defined SIEM – Security Information Event Management in 2005

SIEM solutions were introduced somewhere around 2000 in the form of either a SIM solution or an SEM solution. The systems during this initial phase from 2000 to 2005 provided basic log aggregation across different system types along with basic event correlation techniques.

- The initial systems were designed based on IP Addresses, instead of users. With the dynamic allotment of IP Addresses and rapid increase in the number of mobile devices, correlating a device by its IP Address is

effectively useless for a business as a single IP Address gets allotted to multiple devices in a day.

- Traditional systems used rule-based methods to establish a correlation between various security events. Hence, updating hundreds of rules in real-time does not only consume time but also results in the improper utilisation of resources.
- Since a rule-based event correlation system is in place, they tend to generate a large number of false-positive events.
- Overwhelmed by the number of false positives thus generated, true positive events might be ignored by the analysts. Moreover, a rule-based approach is a backwards-looking approach i.e. a situation occurs and then rules to prevent the same situation from happening again are created.

Analysts identify three generations of SIEM security capabilities and technologies:

- The first generation of SIEMs, introduced in 2005, combine log management and event management systems, which were previously separate. They are limited in the scale of data they can process and in the sophistication of alerts and visualizations they generate.
- The second generation of SIEMs was better equipped to handle big data—large volumes of historical logs. Such SIEMs can correlate historical log data with real-time events and data from threat intelligence feeds.
- The third generation of SIEMs, proposed by Gartner in 2017, combines traditional SIEM capabilities with two new technologies. These are user and entity Behavior analytics (UEBA), which uses machine learning to establish behavioural baselines of users or IT systems, and identifies anomalies. This includes security automation, orchestration and response (SOAR) which can help analysts quickly investigate incidents and activate security tools to automatically respond to an incident.

Along with the addition of traditional information security techniques, SIEMs have gone onto including advanced techniques such as **User Behaviour Analytics and Deep Packet Inspection**. **User Behaviour Analytics, or UBA**, focuses on analysing user-oriented user data and user credentials. The algorithms used in UBA are based on machine learning and hence work on the predictive model. Machine learning algorithms have increased the efficiency of SIEMs by replacing rule-based algorithms. Many vendors have developed UBA tools to complement traditional SIEM systems while vendors developing new SIEM tools are including SIEM as an inbuilt tool. **Deep Packet Inspection is an application of UBA by analysing data at the packet level for the articulation of user behaviour**. This articulation is not only limited to a single computer but includes mobile phones and tablets as well. **Packet Inspection is the primary use case for deep learning in security**.

SIEM solutions have moved on from using a rule-based approach and are now using artificial intelligence to reach the highest level of security. As a business owner or someone looking after an organization's security, you must take note that a SIEM system is as good as people managing it. Even though present-day SIEMs are AI-based, they still need human interaction for implementation, monitoring and taking proper action against the generated alerts.

4. Introduction to SIEM

Cyber-attacks are consistently increasing, and as a result, so is the resulting damage. While attackers can target any organization as they wish, no organization remains immune to cyber-attacks. Over time, attackers have continued to evolve their tactics, techniques, and procedures (TTPs). To defend against these attacks, an organization implements a flurry of measures such as firewalls, intrusion detection/prevention system (IDS/IPS), network access control, proxy server, load balancer, anti-virus/anti-malware tool, and whatnot. We will provide you with an introduction to SIEM, which can be a very strong detective security control.

SIEM technology aggregates event data produced by security devices, network infrastructure, host and endpoint systems, applications, and cloud services. The primary data source is log data, but SIEM technology can also process other forms of data, such as network telemetry (i.e., flows and packets). Event data is combined with contextual information about users, assets, threats, and vulnerabilities. The data may be normalized, so that events, data, and contextual information from disparate sources can be analyzed for specific purposes, such as network security event monitoring, user activity monitoring, and compliance reporting. The technology provides real-time analysis of events for security monitoring, query and long-range analytics for historical analysis, and other support for incident investigation and management, and reporting — e.g., for compliance requirements.

A SIEM system provides a single interface for viewing and correlating data gathered from different security controls and network infrastructure components, so you have a more holistic picture of what's happening on your network than any single security control can provide on its own. When correctly implemented, a SIEM tool can help you detect and mitigate threats on your network that otherwise you might have missed, owing to the sheer volume of log and event data generated by your systems.

Modern SIEM tools combine the capabilities of what used to be two separate product categories a few years ago: security information management (SIM) and security event management (SEM).

A few years back, SIM tools helped organizations collect and manage security-related log data from firewalls, antivirus software, intrusion detection and prevention systems, network routers, DNS servers, authentication systems, application software, databases, and other sources. Enterprises typically used those tools to ensure and demonstrate their compliance with regulatory and industry requirements. SEM systems provided real-time analysis and visualization of security events and alerts, such as authentication failures or audit and intrusion events, generated by security and other systems.

A SIEM product combines these capabilities and gives organizations a way to automate the collection, correlation, storage, and analysis of log and alert data gathered from internal systems. There is no meaningful distinction between SEM, SIM, and SIEM anymore, says Daniel

Kennedy, an analyst with 451 Research. “Everything is SIEM. Nobody draws the distinction between SEM and SIEM anymore,” he says.

SIM tool - four components - data collection, data analysis, event management and reporting

NIST - Identify, Protect, Detect, respond and Recover

SOAR - security orchestration, automation and response solution.

5. Benefits of SIEM

Organizations can benefit from a SIEM implementation in multiple ways

- **Spotting threats more quickly**

The logs generated by your security controls and network hardware and software are key to helping you figure out what’s going on in your network from a security perspective.

Log data can tell you whether someone is attacking you or has already gained access to your systems, has escalated privileges or is moving laterally across your network. Logs can reveal credential misuse, suspicious scanning activities, and all sorts of other malicious and anomalous behavior on your network.

- **Using rules**

Unfortunately, the sheer volume of log data generated by enterprise security and network infrastructure systems makes it extremely hard for security administrators to extract much actionable information from it. A SIEM tool can help address that problem by giving organizations a way to collect security-relevant data from across the network and applying rules for reducing the data to a smaller and far more manageable volume of actionable security alerts.

Security administrators can set up rules to ensure that their SIEM system generates alerts on significant, or potentially significant, events that might merit further investigation. They can use rules to categorize threats and prioritize them. Such rules can help ensure that SIEM systems filter out a lot of the noise generated by log data and focus only on the events that matter.

- **Two rule examples**

For example, a security administrator could set up a rule that instructs the SIEM system to look for and alert on buffer overflow events on your network. Similarly, your administrator could set up rules for **alerting on any ping sweeps or vulnerability- and port-scanning activity on your network or any abnormally large number of failed login messages. Scans and failed logins** are

often signing that threat actors are probing your network for potential vulnerabilities and soft spots.

- **SIEM is not a surrogate for security controls**

As powerful as a SIEM system can be, it's not a stand-in for conventional security controls, such as firewalls, antivirus software, It means - While a Security Information and Event Management (SIEM) system is highly effective, it cannot replace traditional security measures like firewalls and antivirus software. SIEM systems excel in collecting, analyzing, and correlating security data to identify anomalies and potential threats. However, they do not directly prevent or mitigate attacks like firewalls and antivirus software do. Both SIEM systems and conventional controls are essential for a robust cyber security strategy.

Intrusion detection systems, and access control and identity management technologies. So how does a SIEM complement these controls?

A SIEM ties together all the log and alert data generated by these control systems and winnows them down so you can spot threats more quickly. A SIEM tool's value lies in its ability to assess log data from one source and correlate it with data from other systems to identify real threats while weeding out false positives. For example, it can take alerts from your IDS or intrusion prevention system and correlate them with vulnerability data from your endpoint systems to verify if a network intrusion resulted in your systems getting breached.

“SIEM is very much about the collection of logs, the correlation of logs based on rule sets and automated alerting that allows for incident response,” Kennedy says.

- **Speedy incident response**

Equally importantly, a SIEM tool can help organizations defuse or respond to threats more quickly. SIEM systems give incident handlers a way to drill down into incidents quickly and to pull up information on everything that happened before, during, and after an incident.

They can show where an attacker might have **gained entry, when and how, and what the attacker did, so that it becomes easier to shut down the attacker.** Almost all modern SIEM tools either include or support dashboards for visualizing and assessing threats and capabilities for automatically **shutting them down.**

- **Better forensic analysis**

The system logs and alert data stored by SIEM systems are useful from a forensic analysis standpoint, especially after a security incident or breach. Security administrators can query the

data in a SIEM system and drill down into the sequence of events that might have caused an alert. The insights gained from such analysis can be used to implement new security controls or fine-tune existing ones.

Forensics analysis of log data sometimes helps organizations discover deeply hidden threats within their networks that their alerting systems might have missed. Analysts can mine the aggregated data gathered from their security systems and network components and search for patterns or other markers of low and slow attacks. They can navigate through SIEM data using specific queries and criteria to verify if a specific security incident did or did not occur.

For example, the log data in a SIEM system can help a security analyst verify if a particular user or system acted in a suspicious or malicious manner.

- Meeting compliance requirements

A SIEM system can help make compliance reporting easier for organizations that have to meet regulatory requirements. In fact, many organizations justify their SIEM purchases on compliance grounds, but then use the technology for threat management and incident response purposes as well, says Kennedy.

While 69.5% of enterprises with a SIEM capability use it to satisfy a compliance requirement, almost 90% would have rolled out the

SIEM system without a compliance requirement at all, according to research by Kennedy's firm, 451 Research.

SIEM products enable centralized logging and audit of security-relevant data and help organizations meet log review and log retention requirements.

They allow logs from multiple systems across your network to be stored in a central server and in a single common format. This makes it easier for administrators to build compliance reports that include relevant data from across all the organization's security controls and network infrastructure.

Many SIEM products support log management, analysis, and reporting for specific regulations such as HIPAA, Sarbanes-Oxley, the Federal Information Security Management Act (FISMA), and the PCI data security standard.

SIEM helps to focus on certain areas that can be used to detect threats like below:

Insider Threats help to Uncover suspicious user activity that may indicate compromised credentials or an insider threat. An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors,

or business associates, who have inside information concerning the organization's security practices, data, and computer systems.

Advanced Threats Piece together several seemingly low-risk events to find the one extremely high-risk cyberattack underway. An advanced persistent threat is a stealthy threat actor, typically a nation-state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.

Securing the cloud Exposes hidden risks in hybrid multi-cloud environments and containerized workloads. Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, services, and the associated infrastructure of cloud computing.

Data exfiltration Correlate exfiltration events, such as insertion of USBs, use of personal email services, unauthorized cloud storage, or excessive printing. Data exfiltration occurs when malware and/or a malicious actor carries out an unauthorized data transfer from a computer. It is also commonly called data extrusion or data exportation. Data exfiltration is also considered a form of data theft.

OT and IoT security Centralize monitoring for OT and IoT solutions to identify abnormal activity and potential threats.

6. Introduction to IBM QRadar & Log Manager

IBM Security provides a range of security technologies and services and is headquartered in Cambridge, Massachusetts. The QRadar Security Intelligence Platform is primarily built around the QRadar SIEM solution and composed of several other separately priced components:

- **IBM QRadar SIEM**

QRadar SIEM consolidates log source event data from thousands of device endpoints and applications distributed throughout a network. It performs immediate normalization and correlation activities on raw data to distinguish real threats from false positives. As an option, this software **incorporates IBM X-Force Threat Intelligence, which supplies a list of potentially malicious IP addresses including malware hosts, spam sources, and other threats.** QRadar SIEM can also correlate system vulnerabilities with event and network data, helping to prioritize security incidents.

IBM QRadar SIEM provides the following capabilities:

- Provides near real-time visibility for threat detection and prioritization, delivering surveillance throughout the entire IT infrastructure
- Reduces and prioritizes alerts to focus investigations on an actionable list of suspected incidents
- Enables more effective threat management while producing detailed data access and user activity reports
- Delivers security intelligence in cloud environments • Produces detailed data access and user activity reports to help manage compliance
- Offers multi-tenancy and a master console to help Managed Service Providers provide security intelligence solutions in a cost-effective manner

- **IBM QRadar Vulnerability Manager**

QRadar Vulnerability Manager proactively discovers network device and application security vulnerabilities, adds context, and supports the prioritization of remediation and mitigation activities. It is fully integrated with the QRadar Security Intelligence Platform and enriches the results of both scheduled and dynamic vulnerability scans with network asset information, security configurations, flow data, logs, and threat intelligence to manage vulnerabilities and achieve compliance. QRadar Vulnerability Manager helps you develop an optimized plan for addressing security exposures. Unlike stand-alone tools, the solution integrates vulnerability information to help security teams gain the visibility they need to work more efficiently and reduce costs. It is part of the QRadar SIEM architecture. It can be quickly activated with a licensing key and requires no new hardware or software appliances.

- **IBM QRadar Network Insights**

IBM® QRadar® Network Insights provides in-depth visibility into network communications on a real-time basis to extend the capabilities of your IBM QRadar deployment. Through the deep analysis of network activity and application content, QRadar Network Insights empowers QRadar Sense Analytics to detect threat activity that would otherwise go unnoticed.

QRadar Network Insights provides in-depth analysis of both network metadata and application content to detect suspicious activity that is hidden among normal traffic and extract content to provide QRadar with visibility into network threat activity. The intelligence that is provided by QRadar Network Insights integrates seamlessly with traditional data sources and threat intelligence to extend QRadar detection, analysis, and threat detection capabilities.

- **QRadar Risk Manager**

QRadar Risk Manager provides three key areas of value that build on top of the QRadar SIEM value proposition:

- Network topology visualization and path analysis
- Network device optimization and configuration monitoring
- Improved compliance monitoring and reporting

A key area to emphasize is the ability of the product to risk-prioritize vulnerable machines based on network reachability, and to provide detailed device configuration information that can be used to quickly shut down network paths that attackers may use to exploit vulnerabilities. This is key, as many vulnerabilities either cannot be rapidly remediated due to change windows or technological limitations, or remediation might not be available because many vulnerabilities never have patches available

- **IBM QRadar User Behavior Analytics (UBA)**

IBM® QRadar® User Behavior Analytics (UBA) analyses user activity to detect malicious insiders and determine if a user's credentials have been compromised. Security analysts can easily see risky users, view their anomalous activities, and drill down into the underlying log and flow data that contributed to a user's risk score.

As an integrated component of the QRadar Security Intelligence Platform, UBA leverages out-of-the-box behavioural rules and machine learning (ML) models to add user context to network, log, vulnerability, and threat data to more quickly and accurately detect attacks.

- **IBM QRadar Incident Forensics**

QRadar Incident Forensics allows you to retrace the step-by-step actions of a potential attacker, and quickly and easily conduct an in-depth forensics investigation of suspected malicious network security incidents. It reduces the time it takes security teams to investigate offense records, in many cases from days to hours, or even minutes. It can also help you remediate a network security breach and prevent it from happening again. The solution offers an optional QRadar Packet Capture appliance to store and manage data used by QRadar Incident Forensics if no other network packet capture (PCAP) device is deployed. Any number of these appliances can be installed as a tap on a network or subnetwork to collect the raw packet data

- **IBM QRadar Advisor with Watson**

The IBM® QRadar® Advisor with Watson™ app is designed to complement the IBM QRadar Intelligence platform by helping analysts triage and investigate incidents.

The QRadar Advisor with Watson app uses IBM Cognitive Artificial Intelligence to assist users with incident and risk analysis, triage, and response, and enables security operations teams to do more, with greater accuracy. As a result, it helps reduce the time spent investigating incidents from days and weeks down to minutes or hours.

“IBM QRadar: The Intelligent SIEM” https://www.youtube.com/watch?v=n6lQ_cMg-3Q&feature=emb_logo

IBM also offers the Security App Exchange, which enables QRadar customers to download curated content developed by IBM or third parties to extend IBM QRadar’s coverage or value proposition. Other relevant IBM solutions include the IBM QRadar Network Packet Capture appliance, for stronger network forensics capabilities, and IBM Resilient, a SOAR solution that has supported, bidirectional integration between Resilient and the QRadar SIEM solution. This can help organizations streamline their security incident workflow processes.

IBM QRadar SIEM can be deployed on-premises, via hardware virtual appliances and software packages, or it can be hosted in the cloud via IBM’s cloud-based SIEM solution, QRadar on Cloud (QROC). Core SIEM licensing is based on the customer’s event velocity (number of EPS across the data sources in scope) and flows per minute (FPM).

- The number of flows for IBM QRadar Network Insights
- The number of assets in scope for IBM QRadar Vulnerability Manager
- The number of systems from which configuration data is pulled for IBM QRadar Risk Manager

QRadar Network Insights is available only in hardware appliance format, and QRadar Incident Forensics is only sold as a perpetual license.

In past months, IBM has improved alert efficiency via its **Tuning App**, simplified data ingestion from various sources, whereby extracting event properties from a common log format can be accomplished with little or no customization required. IBM has also mapped its QRadar Advisor with Watson to the MITRE ATT&CK framework.

IBM has a wide customer base on the end-user and MSSP side and tends to appeal to larger organizations, by offering a robust platform to build a threat detection and response function. However, smaller organizations can also benefit from the QRadar SIEM solution, with its relative ease of use and extensive out-of-the-box content for less advanced security use cases.

7. Strengths

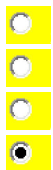
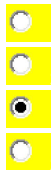
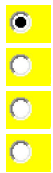
- Deployment/Support: QRadar offers users extensive options in deployment architecture, with a choice of form factors that can be deployed in various combinations. These include physical and virtual appliances that can be all-in-one and separate components, as well as bring-you-own-license for cloud deployment. The exception is the Network Insights component, which is available as a physical appliance only.
- Operations: QRadar has an extensive open API to enable customers and partners to develop integrations with the platform. The app marketplace has extensive integrations provided by IBM and by third parties.
- Product: QRadar offers strong capabilities for managing the collection of events. Users can configure logging to automatically detect multiple event formats, with options to filter them, forward them to real-time analytics or bypass the analytics tier and send them to the data store. Direct forwarding of events to the data store does not contribute to the EPS licensing metric.
- UBA: QRadar includes UBA in the base licensing for QRadar, so there is no additional cost to acquire UBA.
- Product: The QRadar Advisor with Watson offers strong support for incident investigation by providing context enrichment from internal and external sources, suggesting next steps based on attacker actions and prioritizing alerts for further action.

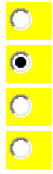
8. Log Management

Log management refers to the process of collecting and storing log data generated by an organization's operating system. A log management tool collects log data coming in from multiple **endpoints** and provides a **centralized location** in which to store it. This centralized location makes it easy for security analysts to access and analyze logs as necessary. The log management tool will also tell you how long logs will be stored and which specific logs need to be pulled, depending on what events or variables you want to investigate.

Log management describes all the activities and processes used to **generate, collect, centralize, parse, transmit, store, archive, and dispose of massive volumes of computer-generated log data**. Log management tools are used to handle all the logs generated by apps, systems, networks, software, or users, and deal with them in any way that best suits the needs of an

enterprise or organization. Log management is a popular topic not only among system administrators and SecOps but also among developers.





Module 2:

Security

Operations

Centre and

Network

Security

Monitoring

-
1. [What is SOC?](#)
 2. [Log v. Event v. Incident](#)
 3. [SOC Components](#)
-
4. [Threat Intelligence](#)
 5. [Introduction to Firewall, Switches, IPS & Directories](#)
-
6. [Types of Prevention](#)
 7. [Collection, Detection and Analysis](#)
 8. [QRadar Log/Event Monitoring](#)
-
9. [QRadar Network/Flow Monitoring](#)
-

1. What is SOC?

The security operations centre (SOC) is to monitor, prevent, detect, investigate, and respond to cyber threats 24x7. SOC teams will be monitoring and protecting the organization's assets including **intellectual property, personnel data, business systems, and brand integrity**. SOC's are proactive where they ensure that the incident does not occur in the first place. **CISO will be liable for defining the general security operations of the organization**. They also manage compliance and communicate across the organization on security issues. The SOC managers will supervise all the SOC activities as managing team members and instrumental in **creating new policies and procedures**.

Security operations teams are charged with monitoring and protecting many assets, **such as intellectual property, personnel data, business systems, and brand integrity**. As the implementation component of an organization's overall cybersecurity framework, security operations teams act as the **central point** of collaboration in coordinated efforts to **monitor, assess, and defend** against cyberattacks.

SOCs have been typically built around a hub-and-spoke architecture, where a security information and event management (SIEM) system aggregates and correlates data from **security feeds**. Spokes of this model can incorporate a variety of systems, such as **vulnerability assessment solutions, governance, risk and compliance (GRC) systems, application and database scanners, intrusion prevention systems (IPS), user and entity behavior analytics (UEBA), endpoint detection and remediation (EDR), and threat intelligence platforms (TIP)**.

The SOC is usually led by a SOC manager and may include incident responders, SOC Analysts (levels 1, 2 and 3), threat hunters, and incident response manager(s). The SOC reports to the CISO, who in turn reports to either the CIO or directly to the CEO.

A SOC framework is the overarching architecture that defines the components delivering SOC functionality and how they interoperate. In other words, a SOC framework should be based on a monitoring platform that tracks and records security events (see figure). An analytics platform provides the ability to analyze these events and determine which combinations of events might indicate an attack or incident. The analytics platform can be either manual -- human beings running various analytics to determine what's going on -- or automated via AI and machine learning algorithms -- the system itself detects attacks and security incidents.

It's not enough to determine that an attack has occurred or is underway; there has to be a response. Depending on whether the SOC is internal or external, the response may be as simple as an alert to inform the client or as complex as automatically executing a full-on incident response process.

Most SOCs have multiple platforms for detection and monitoring, which may or may not be integrated. The SOC framework also may include other functionality, such as threat hunting. These main components should serve as the starting point for a complete SOC framework. Finally, the components should be integrated with ongoing threat intelligence services to ensure detection, analysis, and responses to attacks are in line with the best available information.

- 5 core principles of a SOC framework

Highly effective SOC frameworks have several operational capabilities that include the following:

- **Monitoring.** The most fundamental function a viable security operations centre framework can provide is to monitor activity. The goal of such monitoring, of course, is to determine whether a breach has occurred or is underway. But, before cybersecurity professionals can make that determination, they need to be aware of what's going on. Automated tools and technologies can help with monitoring, including SIEM tools, behavioural threat analytics and cloud access security brokers. These tools may, but not necessarily, use technologies such as AI and machine learning. Cybersecurity analysts typically provide the top layer of such monitoring, reviewing the status of the alarms and alerts.
- **Analysis.** The next function a SOC should provide is analysis. The goal of the analysis is to determine, based on enterprise activity, whether a breach has occurred or a vulnerability is present. As part of the examination function, SOC analysts review alarms and alerts generated by the monitoring system to see if they correlate with known patterns of attack or vulnerability exploits. Once again, AI and machine learning come

into play, along with human intelligence. The aforementioned tools may also provide some degree of analysis.

- **Incident response and containment.** If the SOC is internal or if the enterprise's agreement with an outsourced SOC provider calls for assistance beyond alert notification, the next function the security operations centre framework delivers is an incident response -- precisely how to handle the incident depends on the incident's type, scope and severity. A companywide ransomware attack obviously requires a different response than the compromise of a single server. This is where security orchestration, automation and response(SOAR) tools can help.

Incident response and containment include not only the immediate fire drill responses -- isolating affected systems and applications and notifying relevant stakeholders -- but, ultimately, the longer process of remediation. Effective remediation goes beyond fixing the immediate problem; it also addresses the policies, processes and technical issues that fueled the problem in the first place. Although the SOC doesn't always have a direct role to play in remediation, it's a useful source of detailed information that can be reviewed to determine the root causes of the security incident. And, of course, any policy, process or technology change may affect SOC operations.

- **Auditing and logging.** As noted, the SOC has an important, though often overlooked, role to play in logging and auditing: to verify compliance and to document the response to security incidents that may be used as part of a post-mortem assessment. Many SOAR tools contain an impressive array of timestamped documentation, which can be of value both to cybersecurity analysts and compliance professionals.
- **Threat hunting.** Even when systems are operating normally -- that is, no significant incidents are detected in the environment -- SOC analysts have other responsibilities. They monitor and assess threats in the outside environment by reviewing threat intelligence services and, if they are third parties with multiple customers, scan and analyze cross-customer data to determine patterns of attack and vulnerability. By proactively hunting for threats, SOC providers -- whether internal or external -- can stay a step ahead of the attackers and take protective steps in the event an attack occurs.

2. Log v. Event v. Incident

A log is an entry or a file that contains raw data stored by a device or an application about an action or activity. An event is a set of entries that can be extracted from log data, and it relates to something that has occurred somewhere on a computer network or a system. An incident is an event that is identified as a **potential security breach**.

3. SOC Components

- Awareness of assets, aggregation, and correlation

Logs are the perfect source for providing an accurate picture of what is taking place in real-time. Firewall logs, server logs, database logs, or any other type relevant as SIEM logs being generated in your environment, SIEM systems are able of collecting this data and storing it in one central location for extended retention. This collection process is usually performed by agents or applications, deployed on the monitored system, and configured to forward the data to the SIEM system's central data store.

Once collected, parsed, and stored, the next step in SIEM systems is in charge of connecting the dots and correlating events from the different data sources. This correlation work is based on rules that are either provided by various SIEM tools, predefined for different attack scenarios, or created and fine-tuned by the analyst.

A correlation rule defines a specific sequence of events that could be indicative of a breach in security. For example, a rule could be created to identify when more than x amount of requests are sent from specific IP ranges and ports within an amount of time.

While data logged by large organizations is huge. Even small to medium-sized organizations will be shipping tens of GBs of data a day. In effect, rules help condense that data into more manageable data sets by cutting through the noise and pointing at events that could potentially mean something.

SIEM systems also provide built-in mechanisms for producing reports. These reports can be useful for administration, auditing, or compliance reasons. For example, a daily report detailing alerts or rules triggered could be embedded into a dashboard.

- Log Collection

Log files are generated by every device and application in the network, along with NetFlow data, which monitors network traffic, both provide insights into network activities, making them the main sources of input to security information and event management (SIEM) solutions. A SIEM solution collects, stores, and analyses this information to gain deeper insights

into network Behavior, detect threats, and proactively mitigate attacks. This article will discuss some techniques used for collecting and processing this information.

Logs are collected from all devices such as databases, routers, firewalls, servers, IDS/IPS devices, domain controllers, workstations, and applications.

The log data generated by the devices are automatically sent to a SIEM server securely. There is no need for an additional agent to collect the logs, which reduces the load on the devices.

Agent-based log collection demands an agent be deployed on every device that can generate logs. This method can help filter out logs while collecting them, based on defined parameters. Agents also take up less bandwidth and resources and help provide filtered and structured log data. This method is employed when the devices are in a secure zone where communication is restricted, and it is difficult to send logs to a SIEM server.

- Monitoring & Reporting

Security operations centres monitor and analyze activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported.

The 24/7 monitoring provided by a SOC gives organizations an advantage to defend against incidents and intrusions, regardless of source, time of day, or attack type. the SOC must keep up with the latest threat intelligence and leverage this information to improve internal detection and defense mechanisms.

4. Threat Intelligence

Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviours. Threat intelligence enables us to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors. CTI often includes signature, reputation, and threat data feeds

“Threat intelligence is evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets” – Gartner

Threat intelligence sheds light on the unknown, enabling security teams to make better decisions. helps security professionals better understand the threat actor's decision-making process. empowers business stakeholders, such as executive boards, CISOs, CIOs, and CTOs; to invest wisely, mitigate risk, become more efficient and make faster decisions Monitor the discovery of security threats - their names and impact.

The goal is to collect indicators of compromise on a national and international level from different sources, correlate them, and send it to systems like SIEM or the next-generation firewalls (NGFW) that provide real-time analysis of security alerts so that it is monitored and examined by security analysts to take correct remediation steps. This importance of TI has also led to monetary investment by organizations in threat data.

Threat intelligence benefits organizations of all shapes and sizes by helping process threat data to better understand their attackers, respond faster to incidents, and proactively get ahead of a threat actor's next move. For SMBs, this data helps them achieve a level of protection that would otherwise be out of reach. On the other hand, enterprises with large security teams can reduce the cost and required skills by leveraging external threat intel and make their analysts more effective.

From top to bottom, threat intelligence offers unique advantages to every member of a security team, including:

- Sec/IT Analyst
- SOC
- CSIRT
- Intel Analyst
- Executive Management

A good threat intelligence solution requires good threat intelligent data.

5. Introduction to Firewall, Switches, IPS & Directories

A firewall is a protective layer for your server that monitors and filters incoming and outgoing network traffic. It is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic, and based on a defined set of security rules it

accepts, rejects, or drops that specific traffic. A firewall establishes a barrier between secured internal networks and outside untrusted networks, such as the Internet

In network security, the first line of defense that should always be used is a firewall. Firewalls can now examine individual packets of traffic and test the packets to determine if they are safe. The firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic.

From the perspective of a server, network traffic can be either outgoing or incoming. The firewall maintains a distinct set of rules for both cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better to achieve more security and prevent unwanted communication.

Incoming traffic is treated differently. Most traffic that reaches the firewall is one of these three major Transport Layer protocols- TCP, UDP, or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses type code instead of port number which identifies the purpose of that packet.

Types Of Firewalls

- Web application firewalls
- Stateful firewalls
- Proxy-based firewalls
- Firewall hardware
- Firewall software

A switch is used in a wired network to connect to other devices using Ethernet cables. The network switch keeps track of which device is attached to each of its ports. When a packet arrives on a network port, the switch looks at the recipient's address contained in the packet. The switch then determines which port the recipient is on and sends the packet to that port.

Thus, switches efficiently manage the travel of packets throughout a network by switching each packet travelling on the network through the correct cables, ensuring that each packet arrives at its destination.

- Switches allow you to connect dozens of devices.
- Switches keep traffic between two devices from getting in the way of your other devices on the same network.

- Switches allow you to control who has access to various parts of the network.
- Switches allow you to monitor usage.
- Switches allow communication (within your network) that's even faster than the Internet.
- High-end switches can be tailored to your network needs with pluggable modules.

Intrusion Prevention System (IPS), also known as intrusion detection prevention system (IDPS), is a technology that keeps an eye on a network for any malicious activities attempting to exploit a known vulnerability.

An intrusion prevention system (IPS) is a form of network security that works to detect and prevent identified threats. Intrusion prevention systems continuously monitor your network, looking for possible malicious incidents and capturing information about them. IPS, the abbreviation for Intrusion Prevention System, is designed to monitor various network attacks in real-time and take appropriate actions (like block) against the attacks according to your configuration.

IPS can implement a complete state-based detection which significantly reduces the false positive rate. Even if the device is enabled with multiple application layer detections, enabling IPS will not cause any noticeable performance degradation. Besides, the system will update the signature database automatically every day to assure its integrity and accuracy.

Intrusion prevention systems work by scanning all network traffic. There are several different threats that an IPS is designed to prevent, including:

- Denial of Service (DoS) attack
- Distributed Denial of Service (DDoS) attack
- Various types of exploits
- Worms
- Viruses

6. Types of Prevention

An intrusion prevention system is typically configured to use different approaches to protect the network from unauthorized access. These include:

- Signature-Based - The signature-based approach uses predefined signatures of well-known network threats. When an attack is initiated that matches one of these signatures or patterns, the system takes necessary action.
- Anomaly-Based - The anomaly-based approach monitors for any abnormal or unexpected Behavior on the network. If an anomaly is detected, the system blocks access to the target host immediately.
- Policy-Based - This approach requires administrators to configure security policies according to organizational security policies and the network infrastructure. When an activity occurs that violates a security policy, an alert is triggered and sent to the system administrators.

7. Collection, Detection, and Analysis

SIEM basically follows the below process for alerting any activity which needs to be acted upon.

1. Collection SIEM collects a variety of data from the log sources like Network devices, a variety of Operating systems, Storage devices, etc, and session details from the network. Through Events or flows, It will help us get the details like source, destination, etc, and any custom information specific to log sources.
2. Analysis From the data collected, SIEM has own intelligence to analyze the data through policies including the anomaly detection, User behaviour pattern detection, and Machine learning based process to correlate the data obtained from the various process.
3. Detection From the Detection techniques, SIEM Detects any activity that should be acted upon or triggering any alert mechanism.

8. QRadar Log/Event Monitoring

The core functions of IBM® QRadar® SIEM are managing network security by monitoring flows and events.

A significant difference between event and flow data is that an event, which typically is a log of a specific action such as user login, or a VPN connection, occurs at a specific time and the event is logged at that time. A flow is a record of network activity that can last for seconds, minutes, hours, or days, depending on the activity within the session. For example, a web request might download multiple files such as images, ads, videos, and last for 5 to 10 seconds, or a user who

watches a Netflix movie might be in a network session that lasts up to a few hours. The flow is a record of network activity between two hosts.

- **Events**

QRadar accepts event logs from log sources that are on your network. A log source is a data source such as a firewall or intrusion protection system (IPS) that creates an event log.

QRadar accepts events from log sources by using protocols such as Syslog, Syslog-TCP, and SNMP. QRadar can also set up outbound connections to retrieve events by using protocols such as SCP, SFTP, FTP, JDBC, Check Point OPSEC, and SMB/CIFS.

In QRadar, an Event is a message that we receive and process from some log source. Most log sources are devices on your network creating logs for occurrences of actions and that are then received by QRadar. Thus an Event represents the log of some particular action on this device at a point in time. Examples of such actions include:

- SSH login on a UNIX server
- VPN connection to a VPN device
- Firewall Deny logged by your perimeter firewall

Events can provide below main information about the activity which happened at an instant

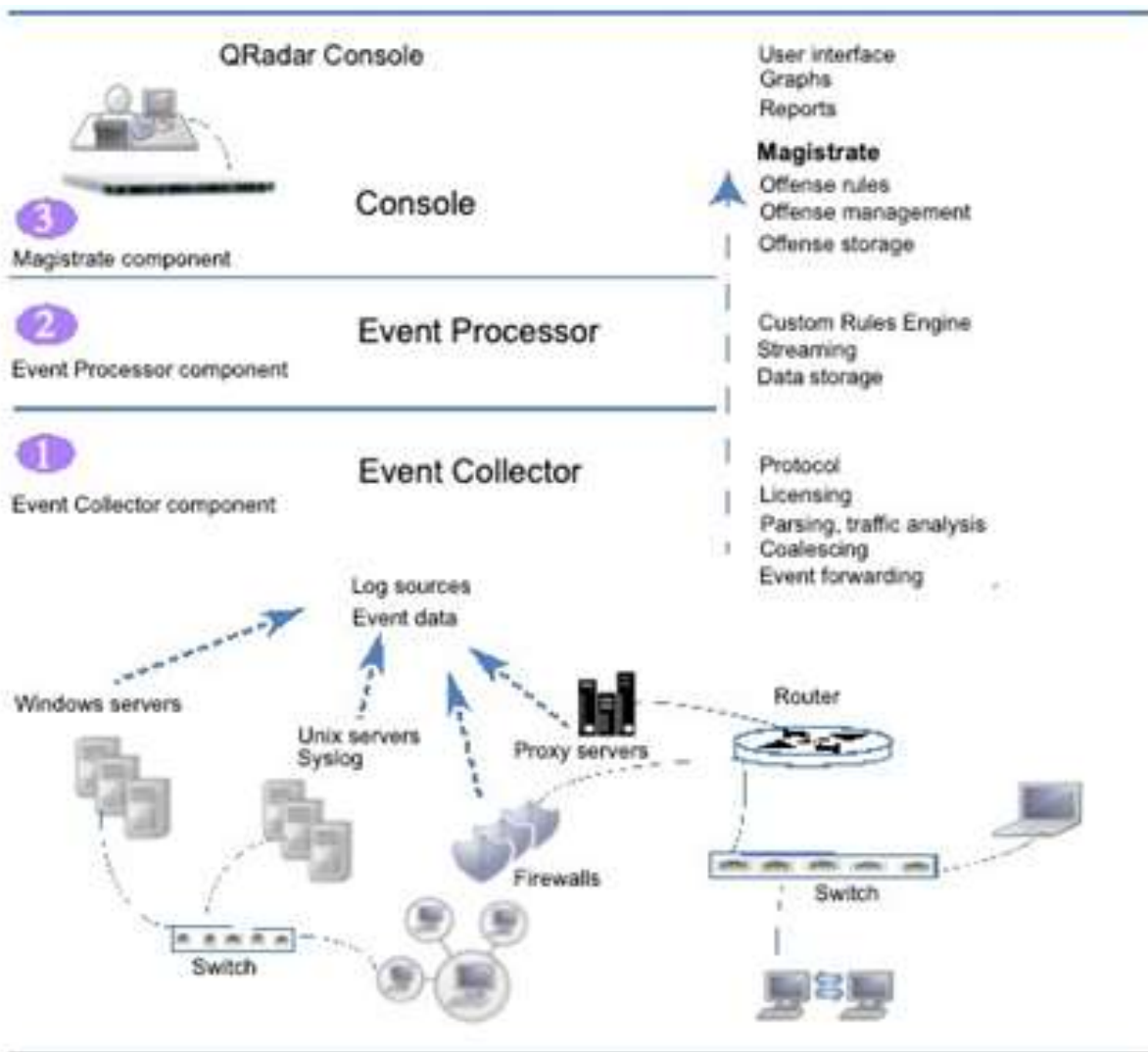
- Point in time Everything that QRadar investigates needs to provide an exact point in time. This timestamp allows QRadar to correlate the most complex relationships between disparate log sources and network flows to present those as one connected event
- Offending users QRadar extracts user information wherever possible allowing an analyst to further investigate individual users. QRadar also uses this information for user behavioural analytics. • Origins The origin represents the starting point for all QRadar correlation activity. The origin is captured as an IP address.
- Targets The target represents the final point for all QRadar correlation activity. The target is captured as an IP address.

- **Event pipeline** [QRadar Log/Event Monitoring](#) Event pipeline

Before you can view and use the event data on the QRadar Console, events are collected from log sources and then processed by the Event Processor. A QRadar All-in-One appliance functions as the Event Collector and Event Processor, in addition to fulfilling the role of the QRadar Console.

QRadar can collect events by using a dedicated Event Collector appliance, or by using an All-in-One appliance where the event collection service and event processing service runs on the All-in-One appliance.

The following diagram shows the layers of the event pipeline.



- Event collection [QRadar Log/Event Monitoring](#) Event collection

QRadar will accept events from a variety of sources, using syslog, syslog-tcp, snmp, etc. as well as having the ability to establish outbound connections and retrieve events, using scp, sftp, ftp, JDBC, Checkpoint OPSEC, SMB/CIFS, etc. As these events are received, they are placed into input queues for processing. The queue sizes will vary based on the protocol/method used, and from these queues, events are fed to the Event Parsers/DSMs.

Known Log Sources (based on the source IP address or hostname in the header) are parsed and coalesced into records, and unknown sources are redirected to Traffic Analysis for Log Source autodetection. If new sources are found, a configuration request message is sent back to the QRadar console to have the new source added, unless you have disabled Autodetection, or if you have reached your Log Source limit, which is controlled by your licenses.

EPS, License Rates:

Events are pulled off of the source queues at a rate dictated by your QRadar licenses, and each event processor can have a distinct licensed event rate. If you are receiving events at a higher rate than your license, they will sit in the source queues until the rate drops. However, if you continue to send at a higher rate than your license, and the queue is filled, your system will start dropping events, with a warning that you have reached your license.

Data Collection, Sources:

Each Log Source type has its own queue:

Syslog: 100000

Syslog (TCP): 100000

Windows Event Log: 100000

Windows IIS/Exchange/DHCP/etc: 10000 each JDBC: 10000

SDEE/ESTreamer: 10000 each

Log File Protocol (scp/sftp/ftp): 50000

The queues are processed in sequence, with parsing servicing each queue in series. For example, if a JDBC connection was to burst to 5000 eps for a few seconds, it's possible that the queue would fill and drop events, while the syslog queue, at a burst of 10000 eps for 5-10 seconds would not, since the queue size is much larger. This varying size is due to the fact that most sources come in over UDP. Note, that ALE connections will also use Syslog UDP to send events in, not the Windows Event log or other Windows methods.

Parsing/Normalization & Coalescing:

Events are parsed and then coalesced based on common patterns across events. Once 4 events are seen with the same source ip, destination ip, destination port, and username, subsequent messages for up to 10 seconds of the same pattern are coalesced together. This is done to reduce duplicate data being stored. Note, that some customers are required to disable coalescing to meet certain audit (PCI/HIPPA) requirements. In these instances, you should expect that data retention requirements will increase, as you are no longer coalescing multiple records into fewer.

Traffic Analysis (Auto Detection):

Events that come into the system from new sources that have not been previously detected are redirected to the traffic analysis (autodetection) engine. These events are run through log sources types that are defined in traffic analysis. A minimum number of messages per minute are required to create a Log Source, and this number may be different for multiple devices. A number of devices are very common from one sort to another, such as AIX, Solaris, Linux, and may not be enabled in traffic analysis. In these instances, or in cases where event rates are low from particular devices, we recommend you create the Log Sources manually. If you are having issues where devices are getting detected incorrectly, especially if they are Log Source types not even on your network, it is possible with the assistance of IBM Support, to remove some of these devices from Traffic Analysis. If you are having this issue, please contact support.

Identity Updates:

In addition to parsing our normalized fields, some log sources and event types will also update identity. Identity records are typically generated from messages that indicate a successful connection/authentication to a resource, such as an SSH login, windows domain authentication, etc. Other events may still have a username parsed out, such as an antivirus update from a Windows host, or a program started from windows, but do not really indicate an authentication. These kinds of events would not generate an identity update.

Identity updates are sent from the event collectors parsing code directly back to the console and do not go through the remaining event pipeline. This is stored with the host information there, under the Asset tab of the QRadar user interface.

A few users have also asked if VA data comes through the event pipeline. This is not the case: VA/Scanner information can be retrieved and processed on any system, which is then parsed by the vis component, sent back to the console, then stored with the Asset information as well.

- Event forwarding

For data redundancy, configure IBM® QRadar® systems to forward data from one site to a backup site.

The target system that receives the data from QRadar is known as a forwarding destination. QRadar systems ensure that all forwarded data is unaltered. Newer versions of QRadar systems can receive data from earlier versions of QRadar systems. However, earlier versions cannot receive data from later versions. To avoid compatibility issues, upgrade all receivers before you upgrade QRadar systems that send data. Follow these steps to set up forwarding:

1. Configure one or more forwarding destinations.

A forwarding destination is the target system that receives the event and flow data from the IBM QRadar primary console. You must add forwarding destinations before you can configure bulk or selective data forwarding. For more information about forwarding destinations, see the IBM QRadar Administration Guide.

2. Configure routing rules, custom rules, or both.

After you add one or more forwarding destinations for your event and flow data, you can create filter-based routing rules to forward large quantities of data. For more information about routing rules, see the IBM QRadar Administration Guide.

3. Configure data exports, imports, and updates.

You use the content management tool to move data from your primary QRadar Console to the QRadar secondary console. Export security and configuration content from IBM QRadar into an external, portable format. For more information about using the content management tool to transfer data.

- **Event processing:**

The Event Processor component

Custom Rules Engine (CRE): The Custom Rules Engine (CRE) is responsible for processing events that are received by QRadar and comparing them against defined rules, keeping track of systems involved in incidents over time, generating notifications to users. When events match a rule, a notification is sent from the Event Processor to the Magistrate on the QRadar Console that a specific event triggered a rule. The Magistrate component on the QRadar Console creates and manages offenses. When rules are triggered, responses or actions such as notifications, Syslog, SNMP, email messages, new events, and offenses are generated.

Streaming: Sends real-time event data to the QRadar Console when a user is viewing events from the Log Activity tab with Real-time (streaming). Streamed events are not provided from the database.

Event storage (Ariel): A time-series database for events where data is stored on a minute-by-minute basis. Data is stored where the event is processed.

The Event Collector sends normalized event data to the Event Processor where the events are processed by Custom Rules Engine (CRE). If events are matched to the CRE custom rules that are predefined on the QRadar Console, the Event Processor executes the action that is defined for the rule response.

Magistrate on the QRadar Console: The Magistrate component completes the following functions:

Offense rules: Monitors and acts on offenses, such as generating email notifications.

Offense management: Updates active offenses, changes statuses of offenses and provides user access to offense information from the Offenses tab.

Offense storage: Writes offense data to a Postgres database.

The Magistrate Processing Core (MPC) is responsible for correlating offenses with event notifications from multiple Event Processor components. Only the QRadar Console or All-in-One appliance has a Magistrate component.

- **Flows**

While log events are critical, they can leave gaps in visibility. When attackers compromise an IT system, they first turn off logging to obfuscate their tracks. Traditional SIEMs are blind at this point. However, no attacker can disable the network, or they cut themselves off as well. Network flow analytics in QRadar allows deep packet inspection for OSI Layer 7 flow data, which can contain very helpful information for advanced forensics. Network flow information helps to detect communication flow anomalies, zero-day attacks that have no signature yet and provides visibility into all attacker communications. Using passive monitoring, flow analytics builds up an asset database and profiles your assets. For example, an IT system that has responded to a connection on port 53 UDP is obviously a DNS server. Another IT system that has accepted connections on ports 139 or 445 TCP is a Windows server.

Network Flow provides insight into raw network traffic. Attackers can interfere with logging to erase their tracks, but they cannot cut off the network (flow data)

- Allows deep packet inspection for Layer 7 flow data. Pivoting, drill-down, and data-mining activities on flow sources allow for advanced detection and forensics
 - Helps to detect anomalies that might otherwise be missed
 - Helps to detect zero-day attacks that have no signature
 - Provides visibility into all attacker communications
 - Uses passive monitoring to build asset profiles and classify hosts

- Improves network visibility and helps resolve traffic problems

QRadar flows represent network activity by normalizing IP addresses, ports, byte and packet counts, and other data, into flow records, which effectively are records of network sessions between two hosts. The component in QRadar that collects and creates flow information is known as QFlow.

QRadar Flow collection is not full packet capture. For network sessions that span multiple time intervals (minutes), the flow pipeline reports a record at the end of each minute with the current data for metrics such as bytes and packets. You might see multiple records (per minute) in QRadar with the same "First Packet Time" but the "Last Packet Time" values increment through time.

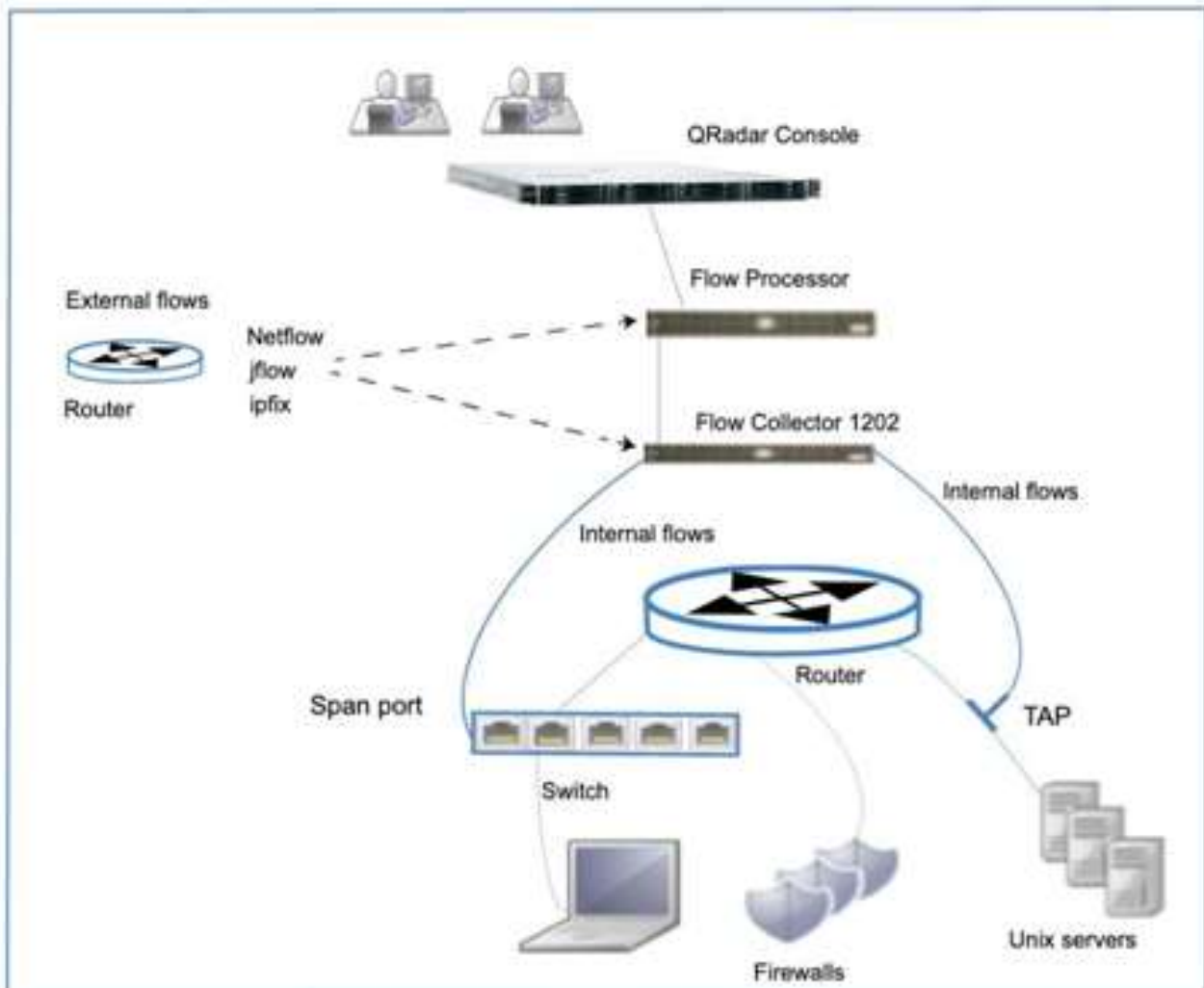
A flow starts when the Flow Collector detects the first packet that has a unique source IP address, destination IP address, source port, destination port, and other specific protocol options, including 802.1q VLAN fields.

Each new packet is evaluated. Counts of bytes and packets are added to the statistical counters in the flow record. At the end of an interval, a status record of the flow is sent to a Flow Processor and statistical counters for the flow are reset. A flow ends when no activity for the flow is detected within the configured time.

QFlow can process flows from the following internal or external sources:

- External sources are flow sources such as netflow, sflow, jflow. External sources can be sent to a dedicated Flow Collector or a Flow Processor such as the QRadar Flow Processor 1705 appliance. External sources do not require as much CPU processing because every packet is not processed to build flows. In this configuration, you might have a dedicated Flow Collector and a Flow Processor that both receive and create flow data. In smaller environments (less than 50 Mbps), an All-in-One appliance might handle all the data processing.
- The Flow Collector collects internal flows by connecting to a SPAN port, or a network TAP. The QRadar QFlow Collector 1310 can forward full packets from its capture card to a packet capture appliance but it does not capture full packets itself.

The following diagram shows the options for collecting flows in a network.



- Flow Pipeline

The Flow Collector generates flow data from raw packets that are collected from monitor ports such as SPANs, TAPs, and monitor sessions, or from external flow sources such as netflow, sflow, jflow. This data is then converted to QRadar flow format and sent down the pipeline for processing.

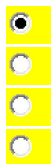
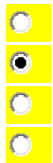
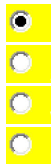
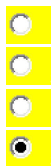
The Flow Processor runs the following functions:

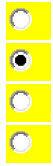
Flow deduplication: Flow deduplication is a process that removes duplicate flows when multiple Flow Collectors provide data to Flow Processors appliances.

Asymmetric recombination: Responsible for combining two sides of each flow when data is provided asymmetrically. This process can recognize flows from each side and combine them into one record. However, sometimes only one side of the flow exists.

License throttling: Monitors the number of incoming flows to the system to manage input queues and licensing.

Forwarding: Applies routing rules for the system, such as sending flow data to offsite targets, external Syslog systems, JSON systems, and other SIEMs. Flow data passes through the Custom Rules Engine (CRE), and it is correlated against the rules that are configured, and an offense can be generated based on this correlation. You view offenses on the Offenses tab.





Module 3:

SIEM

Deployment &

Use cases

1. Security Policies & Best Practices for SIEM

2. SIEM deployment architecture

3. QRadar Deployment Options

4. QRadar SIEM Component Architecture

1. [Security Policies & Best Practices for SIEM](#)

In this Unit, we will understand the SIEM Deployment scenarios and options along with the best practice scenario and Use cases for enhanced security posture.

Security Policies & Best Practices for SIEM

A security policy is a strategy for how an organization/enterprise will implement Information Security principles and technologies. It is essentially a business plan that applies only to the Information Security aspects of a business.

A security policy must specifically accomplish three objectives: 1)It must allow for the confidentiality and privacy of your company's information. It must protect the integrity of the company's information. 3)It must provide for the availability of your company's information.

There are three principles of Information security, or three primary tenants called the CIA triad: confidentiality (C), integrity (I), and availability (A). The security policies support the CIA triad and define the who, what, and why regarding the desired Behavior, and they play an important role in an organization's overall security posture.

Confidentiality: The protection of information against unauthorized disclosure

Integrity: The protection of information against unauthorized modification and ensuring the authenticity, accuracy, non-repudiation, and completeness of the information

Availability: the protection of information against unauthorized destruction and ensuring data is accessible when needed

Why is information security important? Without information security, an organization's information assets, including any intellectual property, are susceptible to compromise or theft. As a result, consumer and shareholder confidence and reputation suffer potentially to the point of ruining the company altogether. It is important to keep the principles of the CIA triad in mind when developing corporate information security policies.

Common reasons why companies create security policies today is to fulfil regulations and meet standards that relate to the security of digital information. A few of the more commonly encountered are:

- The PCI Data Security Standard (DSS)
- The Health Insurance Portability and Accountability Act (HIPAA)
- The HITECH Act
- The Sarbanes-Oxley Act (SOX)
- Massachusetts 201 CMR 17.00

- The ISO family of security standards • The Graham-Leach-Bliley Act (GLBA)

SIEM Best Practices

- Having a clear scope defined and goals based on the threat landscape, business, compliance and security goals.
- Having a dedicated SIEM team and ensure maintenance of the system
- Starting with the out-of-box rules and carefully customize them as the system and the team gains experience with the system.
- Developing new rules.
- Having the right threat intelligence feeds
- Continuous testing and tuning.

Plan & Scope: Plan and scope your security needs. thorough analysis to determine primary risks, decide which systems, users, networks, and applications are in scope for monitoring and consider which parts of your business or data are highly sensitive. This would ensure vital logs/events are being monitored and avoid unnecessary large amounts of data collection.

Correlation Rules: Setting up correlation rules to link in with whatever your security risks are.

Audit and Compliance: ensure scope and correlation rules are always correct, maintain an up-to-date record based on the organization's compliance requirements.

SIEM Deployment: Deploying the right SIEM and ensuring all the required infrastructure and operating equipment setup.

Test Run: Running regular tests and ensuring the SIEM tool works well before making it production-ready. Creating test scripts to test the SIEM by creating unusual logs or access patterns to ensure everything works well. This would help in tuning the correlation rules and other SIEM configurations

Regular Monitoring: Regular logs collection will ensure that the SIEM software to be effective and this would also help in building a pattern and look for any abnormal behaviour. Baselining your system helps SIEM tools detect anomalies, while constant monitoring ensures unusual log behaviour isn't accidentally missed.

Access Management: SIEM should be the last line of defence when working with sensitive data. Access rights management tools will ensure nobody has access to information they shouldn't be

able to see. Sensitive information should be protected, and any temporary access should be revoked as soon as the user no longer needs access.

Security Tools: firewall and malware detectors will be additional tools alongside SIEM and access rights management tools to support the overall system. Having all these tools in place would help in flagging issues quickly of any breach, troubleshoot and protect sensitive data

Response Plan: If intruders attack or gain access to any confidential information an appropriate plan has to be in place and ensure its quickly remedied. SOAR should be in place with a playbook where appropriate people are informed, escalated as required, and troubleshooting in place. This will ensure any breach is minimized.

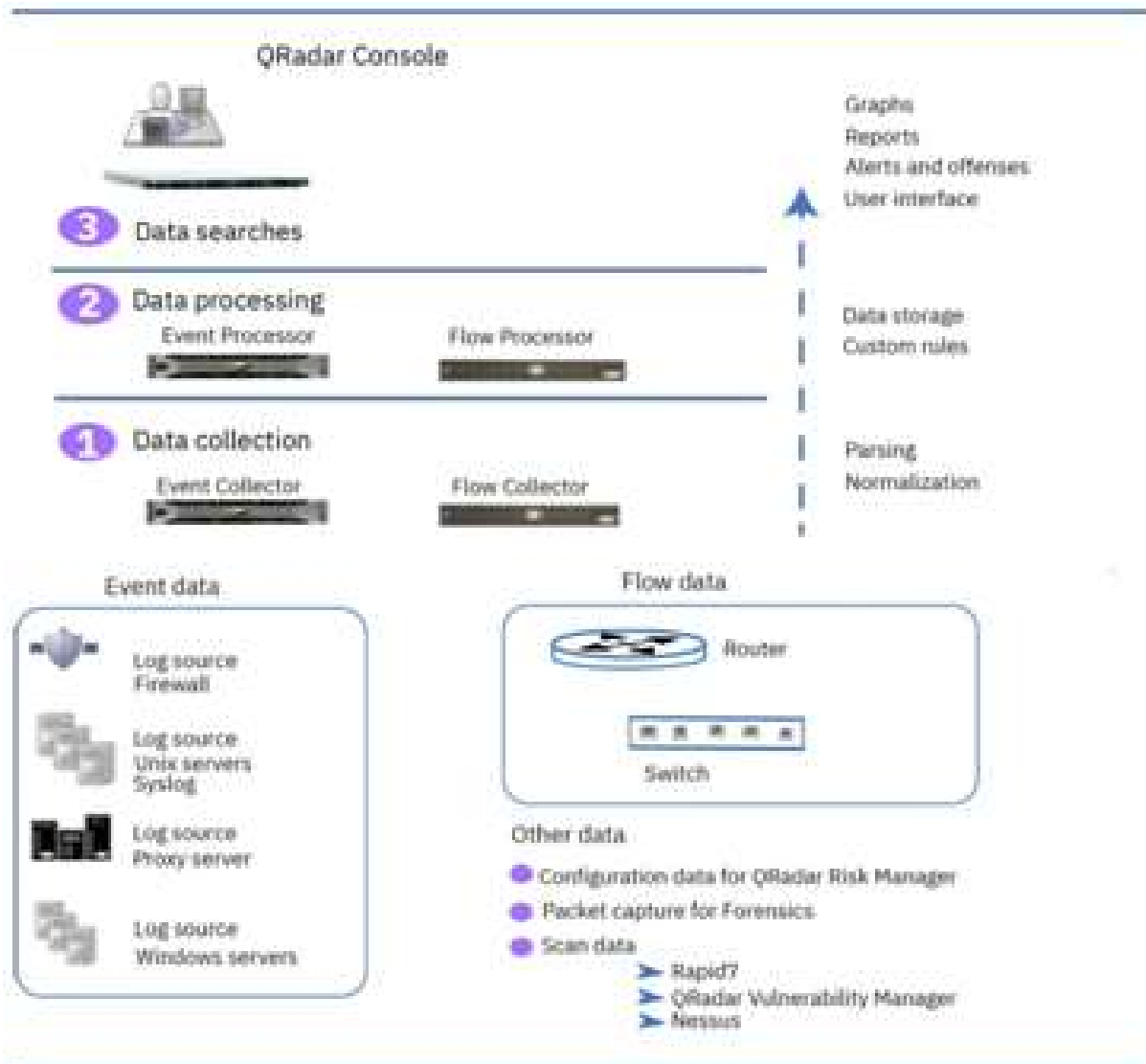
Frequent Reviews: frequent reviews have to be in place to check the deployments, infrastructure health checks, system resource utilization, performance tuning to ensure that the SIEM works well. It is also recommended to keep all the packages and software updated as time progress

2. SIEM deployment architecture

IBM QRadar collects, processes, aggregates, and stores network data in real-time. QRadar uses that data to manage network security by providing real-time information and monitoring, alerts and offenses, and responses to network threats.

IBM QRadar SIEM (Security Information and Event Management) is a modular architecture that provides real-time visibility of your IT infrastructure, which you can use for threat detection and prioritization. You can scale QRadar to meet your log and flow collection, and analysis needs. You can add integrated modules to your QRadar platforms, such as QRadar Risk Manager, QRadar Vulnerability Manager, and QRadar Incident Forensics.

The operation of the QRadar security intelligence platform consists of three layers, and applies to any QRadar deployment structure, regardless of its size and complexity. The following diagram shows the layers that make up the QRadar architecture.



The QRadar architecture functions the same way regardless of the size or number of components in a deployment. The following three layers that are represented in the diagram represent the core functionality of any QRadar system.

- Data collection

Data collection is the first layer, where data such as events or flows is collected from your network. The All-in-One appliance can be used to collect the data directly from your network or you can use collectors such as QRadar Event Collectors or QRadar QFlow Collectors to collect event or flow data. The data is parsed and normalized before it passed to the processing layer. When the raw data is parsed, it is normalized to present it in a structured and usable format.

The core functionality of QRadar SIEM is focused on event data collection and flow collection. Event data represents events that occur at a point in time in the user's environment such as user logins, email, VPN connections, firewall Deny's, proxy connections, and any other events that you might want to log in to your device logs.

Flow data is network activity information or session information between two hosts on a network, which QRadar translates into flow records. QRadar translates or normalizes raw data into IP addresses, ports, byte and packet counts, and other information into flow records, which effectively represents a session between two hosts. In addition to collecting flow information with a Flow Collector, full packet capture is available with the QRadar Incident Forensics component.

- **Data processing**

After data collection, the second layer or data processing layer is where event data and flow data are run through the Custom Rules Engine (CRE), which generates offenses and alerts, and then the data is written to storage.

Event data and flow data can be processed by an All-in-One appliance without the need for adding Event Processors or Flow Processors. If the processing capacity of the All-in-One appliance is exceeded, then you might need to add Event Processors, Flow Processors, or any other processing appliance to handle the additional requirements. You might also need more storage capacity, which can be handled by adding Data Nodes.

Other features such as QRadar Risk Manager (QRM), QRadar Vulnerability Manager (QVM), or QRadar Incident Forensics collect different types of data and provide more functions.

QRadar Risk Manager collects network infrastructure configuration and provides a map of your network topology. You can use the data to manage risk by simulating various network scenarios through altering configurations and implementing rules in your network.

Use QRadar Vulnerability Manager to scan your network and process the vulnerability data or manage the vulnerability data that is collected from other scanners such as Nessus, and Rapid7. The vulnerability data that is collected is used to identify various security risks in your network.

Use QRadar Incident Forensics to perform in-depth forensic investigations and replay full network sessions.

- Data searches

In the third or top layer, data that is collected and processed by QRadar is available to users for searches, analysis, reporting, and alerts or offense investigation. Users can search and manage the security admin tasks for their network from the user interface on the QRadar Console. In an All-in-One system, all data is collected, processed, and stored on the All-in-One appliance.

In distributed environments, the QRadar Console does not perform event and flow processing, or storage. Instead, the QRadar Console is used primarily as the user interface where users can use it for searches, reports, alerts, and investigations.

3. QRadar Deployment Options

IBM® QRadar® architecture supports deployments of varying sizes and topologies, from a single host deployment, where all the software components run on a single system, to multiple hosts, where appliances such as Event Collectors, and Flow Collectors, Data Nodes, an App Host, Event Processors, and Flow Processors, have specific roles.

The primary focus of the first deployment example is to describe a single All-in-One appliance deployment for a medium-sized company. Later examples describe the deployment options as the company expands. The examples describe when to add QRadar components, such as Flow Processors, Event Collectors, and Data Nodes, and when you might need to co-locate specific components.

The requirements for your QRadar deployment depend on the capacity of your chosen deployment to both process and store all the data that you want to analyze in your network.

Before you plan your deployment, consider the following questions:

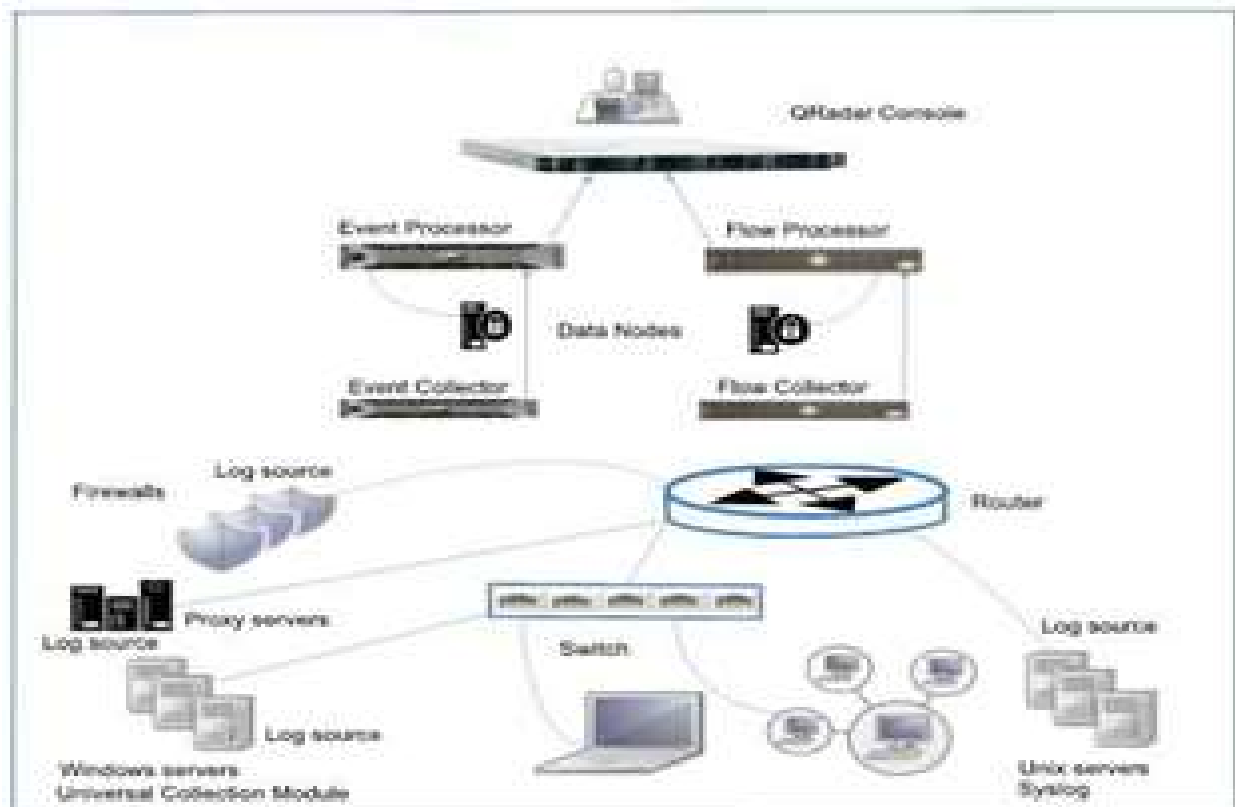
- How does your company use the Internet? Do you upload as much as you download? Increased usage can increase your exposure to potential security issues.
- How many events per second (EPS) and flows per minute (FPM) do you need to monitor?

EPS and FPM license capacity requirements increase as deployment grows.

- How much information do you need to store, and for how long?

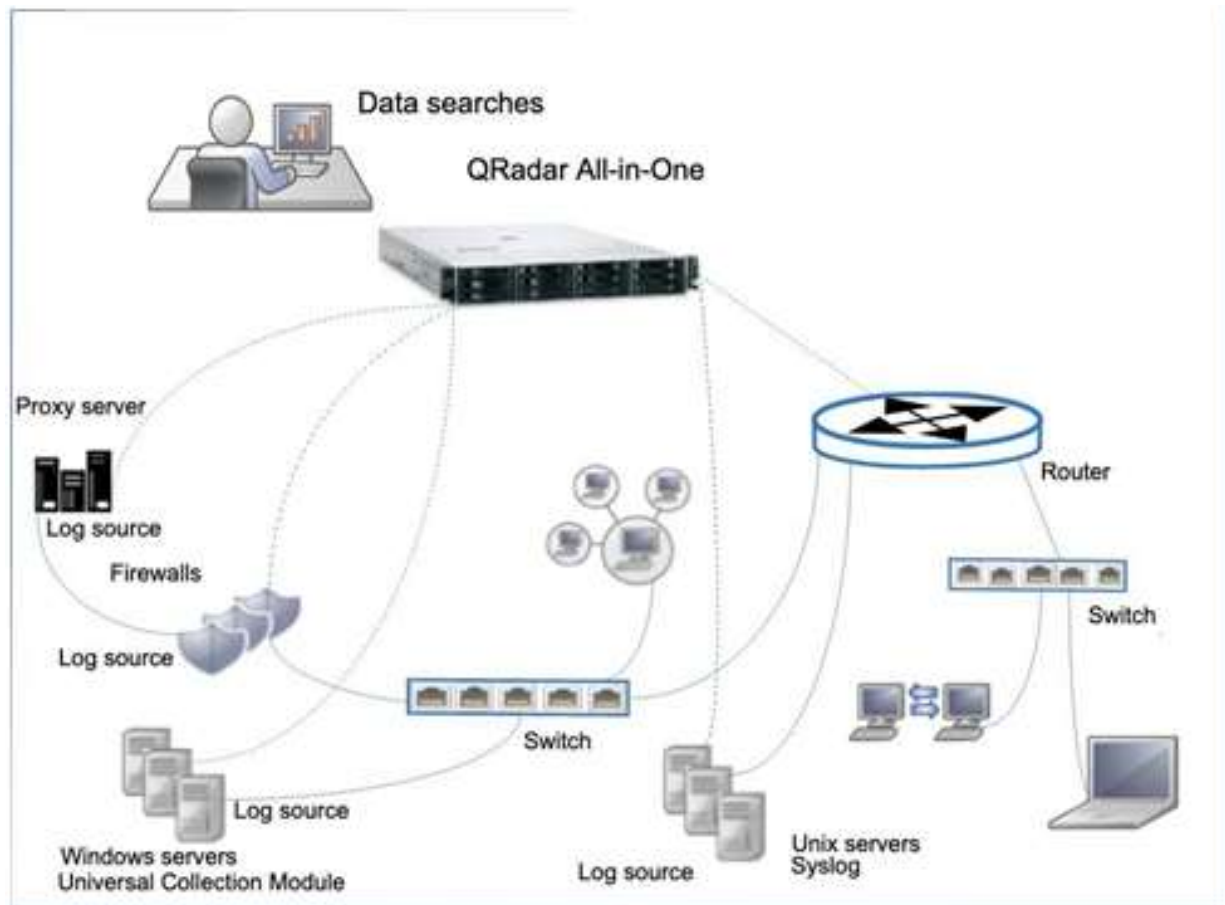
The following diagram shows the QRadar components that you can use to collect, process, and store event and flows data in your QRadar deployment. An All-in-One appliance includes the data collection, processing, storage, monitoring, searching, reporting, and offense management capabilities.

The Event Collector collects event data from log sources in your network, and then sends the event data to the Event Processor. The Flow Collector collects flow data from network devices such as a switch SPAN port, and then sends the data to the Flow Processor. Both processors process the data from the collectors and provide data to the QRadar Console. The processor appliances can store data but they can also use the Data Nodes to store data. The QRadar Console appliance is used for monitoring, data searches, reporting, offense management, and administration of your QRadar deployment.



All-in-One deployment

In a single host QRadar deployment, you have an All-in-One QRadar appliance that is a single server that collects data, such as Syslog event data logs, and Windows events, and also flow data, from your network.

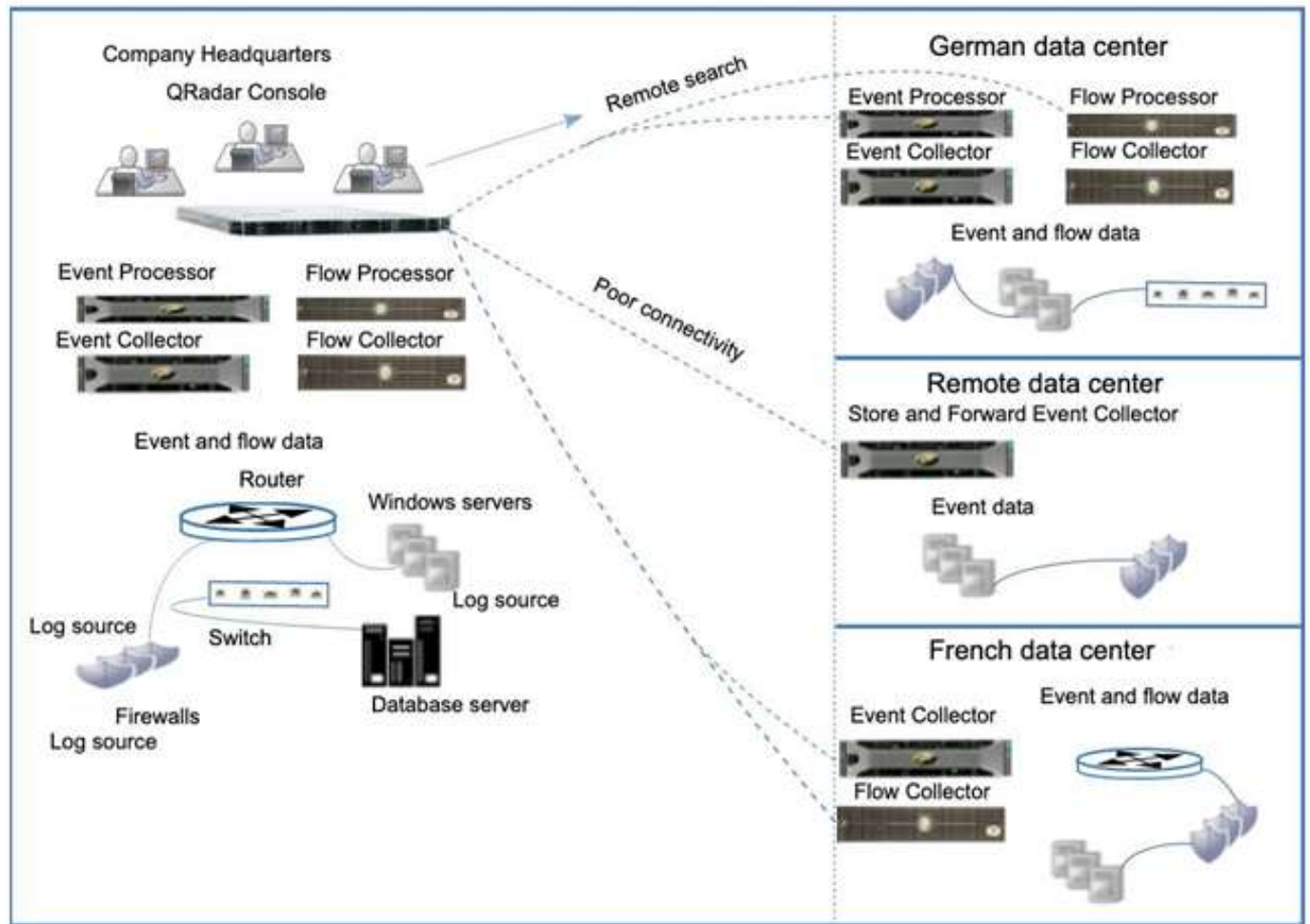


Expanding deployments to add more capacity

Your business might create or expand a deployment beyond an IBM QRadar All-in-One appliance because of the lack of processing or data storage capacity, or when you have specific data collection requirements.

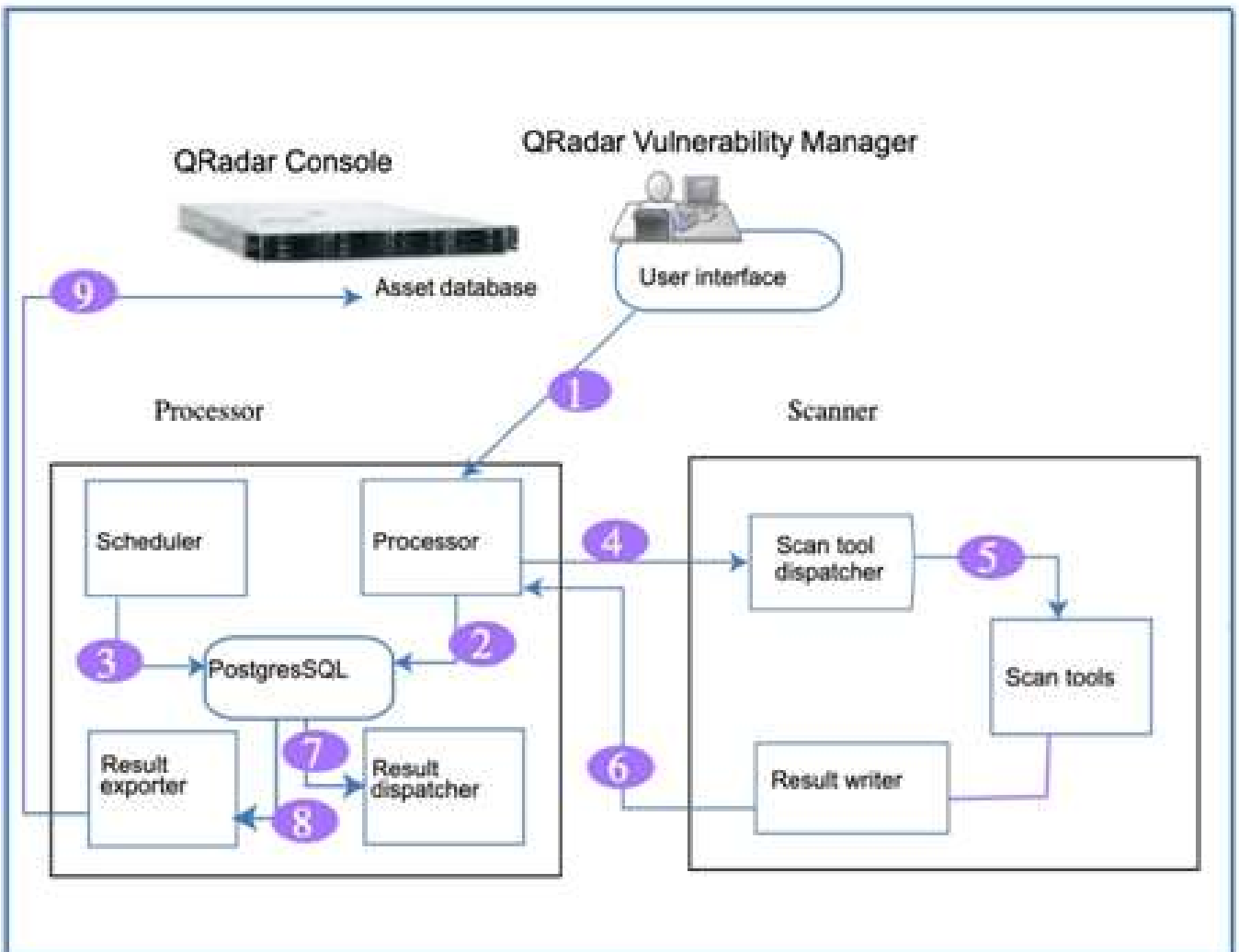
Geographically distributed deployments

In geographically distributed deployments your IBM QRadar deployment might be impacted by intermittent or poor connectivity to remote data centres. You might also be impacted by local regulations, such as complying with specific state or country regulations to keep data in the place of origin. Both of these situations require that you keep collectors on site. If you must keep data in the place of origin, then you must keep the processor on site.



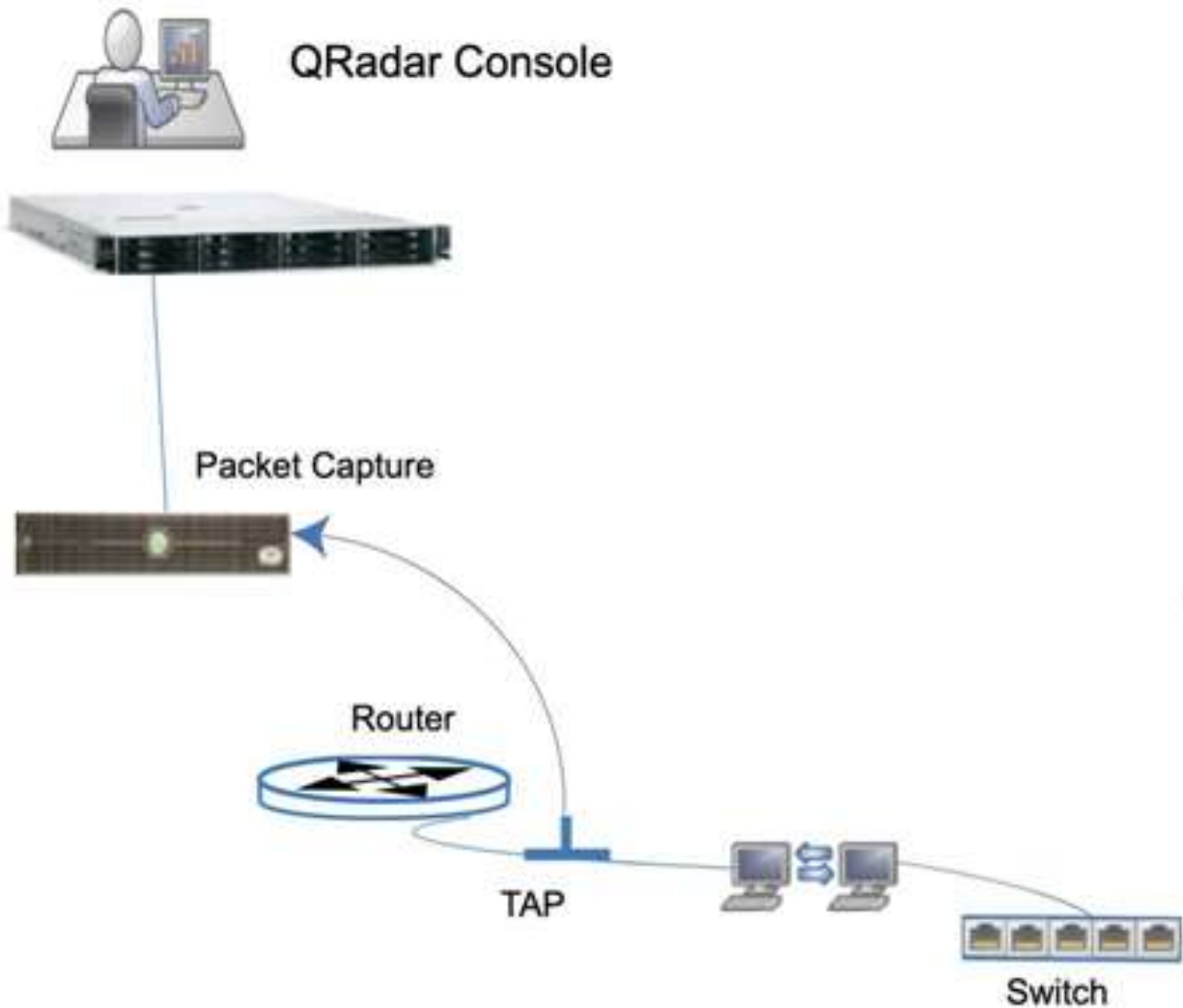
QRadar Vulnerability Manager deployments

Locate and manage the vulnerabilities in your network by deploying IBM QRadar Vulnerability Manager. Enhance your network security by integrating add-on features such as IBM BigFix® and IBM Security SiteProtector.



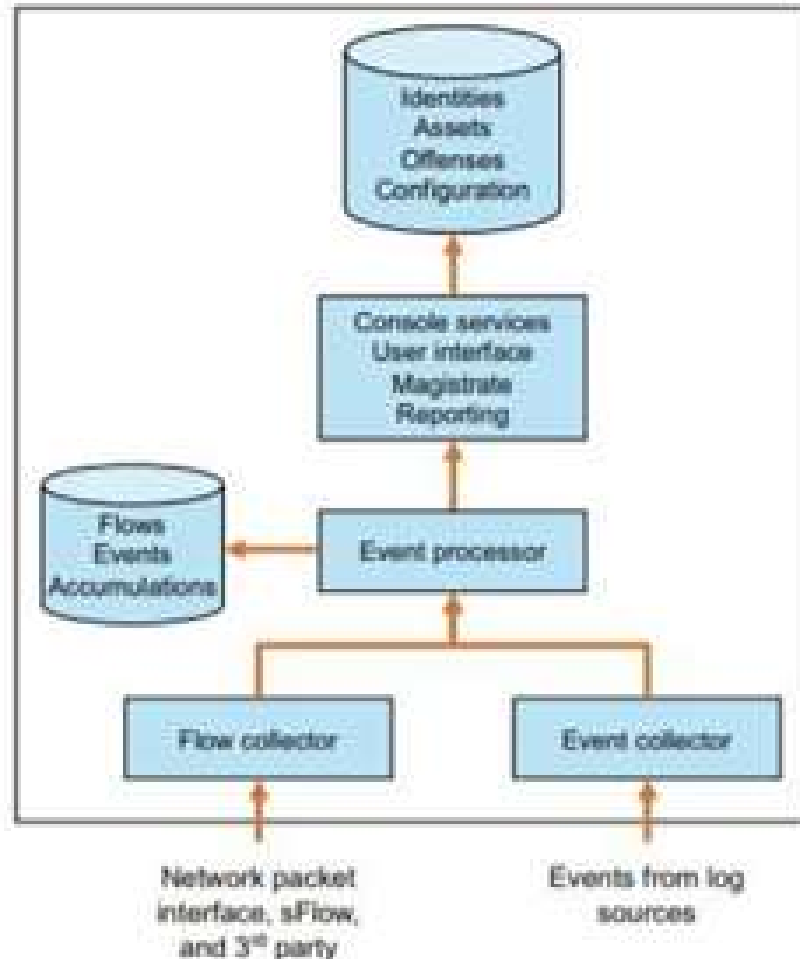
Forensics and full packet collection

Use IBM QRadar Incident Forensics in your deployment to retrace the step-by-step actions of a potential attacker, and conduct an in-depth forensics investigation of suspected malicious network security incidents.



4. QRadar SIEM Component Architecture

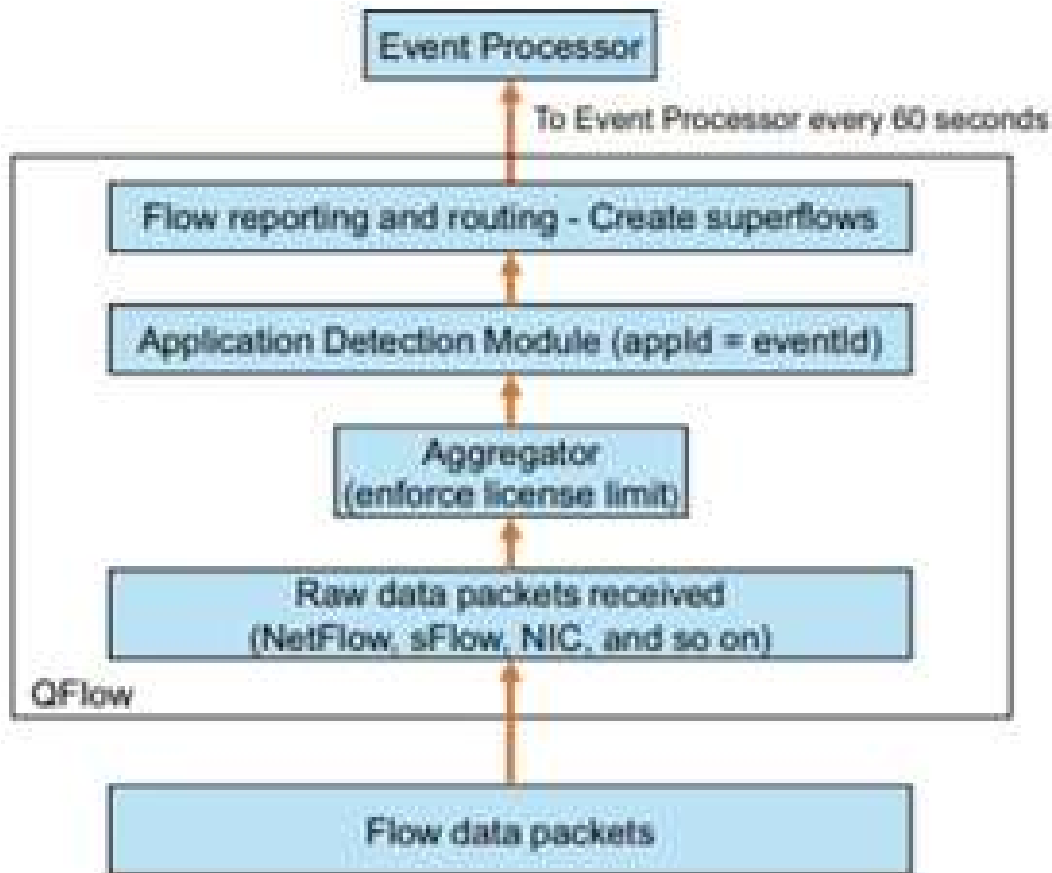
- High-level component architecture and data stores



Events from individual log sources and network flow data is collected by the QRadar Event and Flow collectors. Once the flow and event data is forwarded to the Event Processor it is stored in the Ariel database on the Event Processor. If accumulation is required, the accumulated data is stored in Ariel accumulation data tables. To fulfil the tamper proof data storage aspects for compliance mandates, data cannot be changed as soon as it is stored in the Ariel database. At any point in time, data can be selectively indexed to support specific search and report requirements. Once the Event Processor is finished processing, the data is passed on to the QRadar Console, where further consolidated processing occurs. Offenses, assets, identity, and configuration information are stored in the master PostgreSQL database on the Console. There is one master database with optional copies on each processor for backup and automatic restore.

Secure SSH communication between appliances in a distributed environment is supported.

- FLOW COLLECTOR ARCHITECTURE



A network flow record provides information about a conversation between two devices using a specific protocol and can include fields that provide details about the conversation. Examples include the source and destination IP addresses, the port, and other fields. Flow data packets can be collected from a variety of network device vendors, and directly from the network interface. Collected flow data can update asset profiles with the ports and services that are running on each host. If a new host is detected through network flow data, a new asset is created in the QRadar Asset database. Next in line is the Aggregator. This component enforces the license limit for the Flow Collector, which is measured in “flows per minute”, or FPM. If the license limit is exceeded, flows are temporarily stored in an overflow buffer, which will be processed with the next set of flows. Every log source protocol has an overflow buffer of 5 GB, and if the overflow buffer fills up, the additional flows are dropped.

The Application Detection Module uses four methods of determining the application of the flow.

- First is the User Defined method. This method is mainly used when users have a proprietary application running on their network. For example, all traffic going to host 10.100.100.42 on port 443 is recognized to be MySpecialApplication.
- The second method uses State-based decoders.

This method is implemented by looking at the source code. It determines the application by analyzing the payload for multiple markers, for example, if you see A followed by B, then application = X; and if you see A followed by C, then application = Y.

- The next method uses Signature matching. This method relies on basic string matching in the payload (see the Application Configuration Guide for signature customization).
- The final method uses Port-based matching. In this case, applications are matched based on their port use, for example, port 80= http. Finally, the flow data packets reach the Flow reporting and routing component. This component is responsible to create superflows. Superflows only store one single flow with the collection of IP addresses, which allows the processing of flows to be faster, and require less storage space.

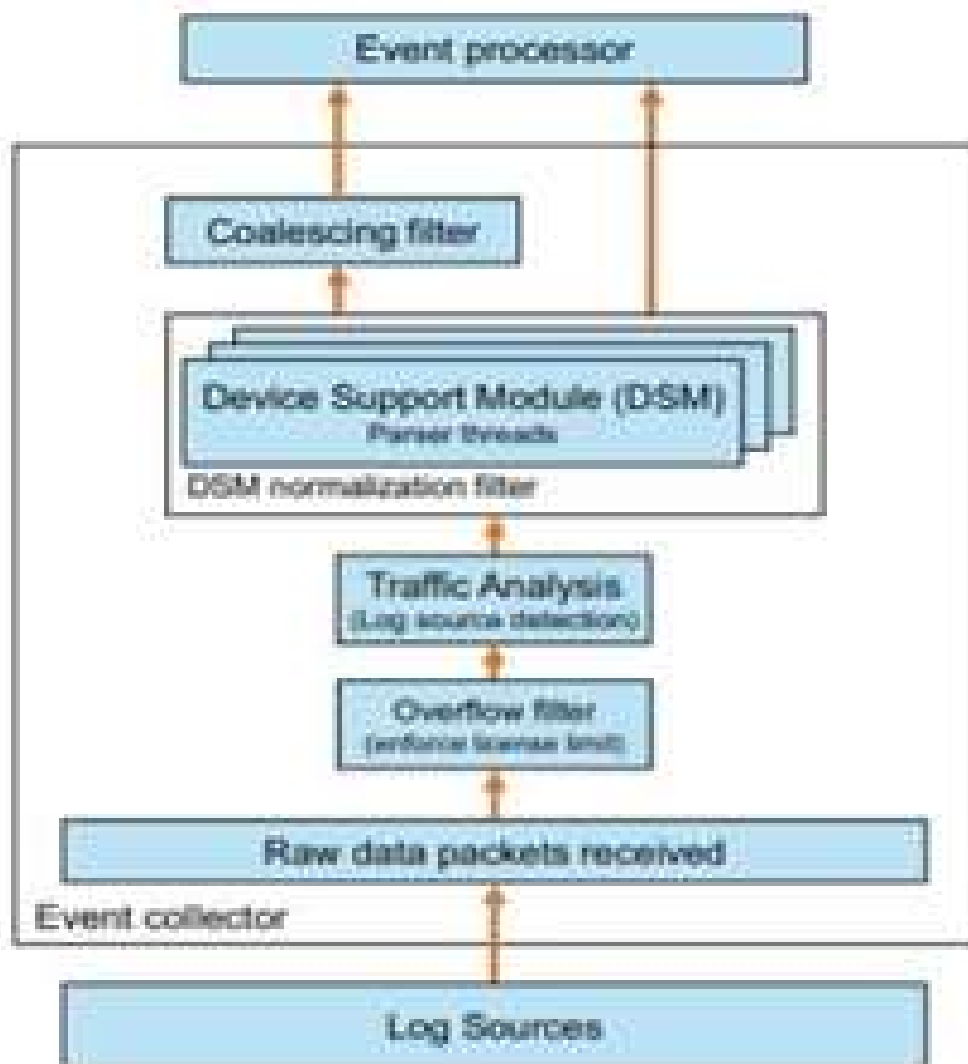
There are three types of superflows.

- Type A superflows contain a single source and multiple destinations addresses with the same destination port, byte count, and source flags or ICMP codes. An example for a type A superflow is a network sweep.
- Type B superflows contain multiple sources and a single destination address with the same destination port, byte count, and source flags or ICMP codes. An example for a type B superflow is a Distributed Denial of Service attack.
- Type C superflows contain a single source and destination address with changing source and destination ports. An example for a type C superflow is a port scan.

Specific rule tests can leverage the flow type to determine if an offense needs to be created. The creation of superflows can be disabled. Up to a configurable number of bytes, QFlow provides layer 7 insights into the payload if it is unencrypted. Using a tap or span port, QFlow collects raw packets and places them into 60-second chunks. QFlow can also receive layer 4

flows from other network devices in IPFIX/NetFlow, sFlow, J-Flow, Packeteer, and Flowlog file accounting technologies.

- Event collector architecture



Each Event Collector gathers events from local and remote log sources. Once the raw data packets have been received, the license limit is checked first. On the Event Collector, this limit is measured in Events per Second, or EPS. Events are temporarily stored in an overflow buffer if the EPS license is exceeded, and those events are processed during the next cycle. Should the

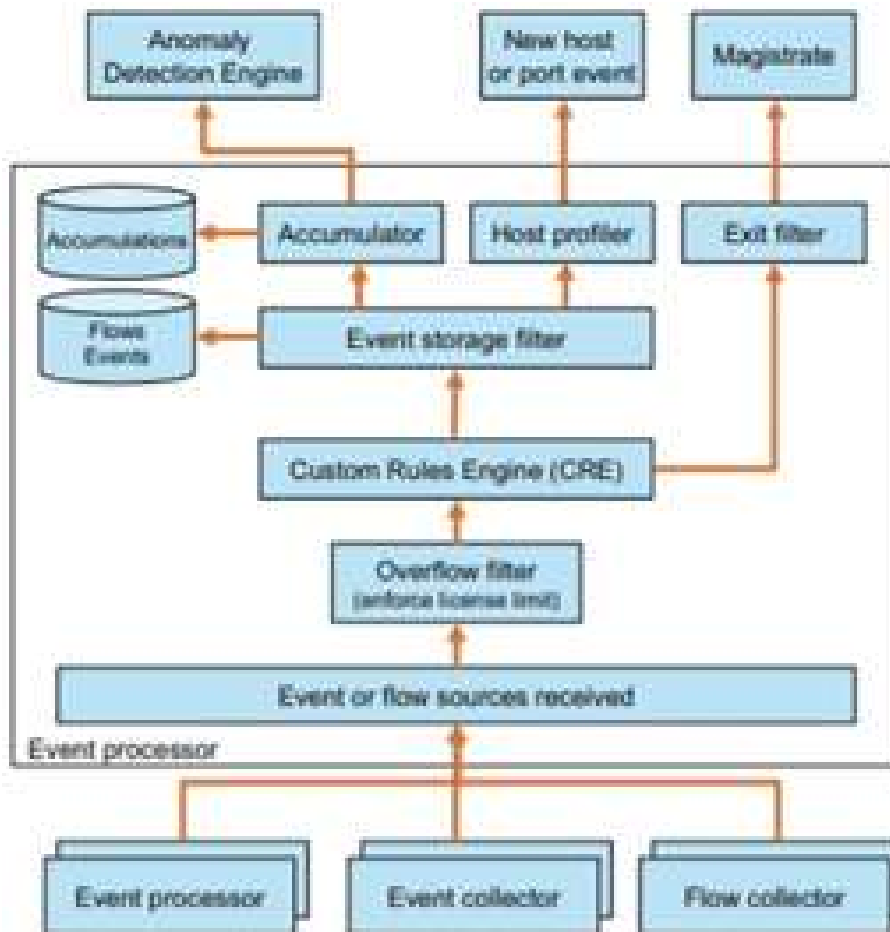
overflow buffer fill up, the additional events are dropped, and a message is logged for the administrators.

Log Sources are automatically discovered after record analysis in the Traffic Analysis module. This is an essential module for automating a successful evaluation or deployment because it categorizes traffic from devices that are unknown to the system. Log source detection creates a new QRadar log source if detection is successful on an IP address. The Traffic Analyses module only carries out detection on event protocols that are “pushed” to the event collector, for example, syslog.

After the correct log source has been detected, such as a Checkpoint Firewall, the individual Device Support Modules begin to parse the events. First, the events are normalized, where source-specific data fields are mapped into QRadar terminology for further processing. The log source parser then extracts the log source event ID from the log record and maps that to the QRadar Identifier, or QID. This is a unique ID that links the extracted log source event ID to a QID. Each QID relates to a custom event name and description, as well as severity and event category information. The event category information is structured into High-Level Categories (HLC) and Low-Level Categories (LLC). Every QID is linked to one of the low-level categories, for example, a valid category combination is "Authentication" (being a High-Level Category) and "Admin Login Successful" being a Low-Level Category.

Finally, the coalescing filter can optionally bundle identical events to conserve system usage before handing the data off to the Event Processor.

- Event processor architecture



The Event Processor can receive event and flow data from Event and Flow Collectors as well as other Event Processors that may be distributed throughout the organization's IT deployment. First, the Overflow Filter enforces the license in a similar way to the collectors.

Next, the Custom Rule Engine, or CRE, tests every single event or flow against all enabled rules. Matched rules can have responses or results. For example, a matched rule might trigger the creation of an offense, or create a new CRE event that triggers the creation of an offense. However, actual offenses are not created here at the Event Processor, but rather at the Console.

It is possible that multiple matched events, flows, and matched rules might correlate into a single offense. On the other hand, a single event or flow can also be correlated into multiple offenses.

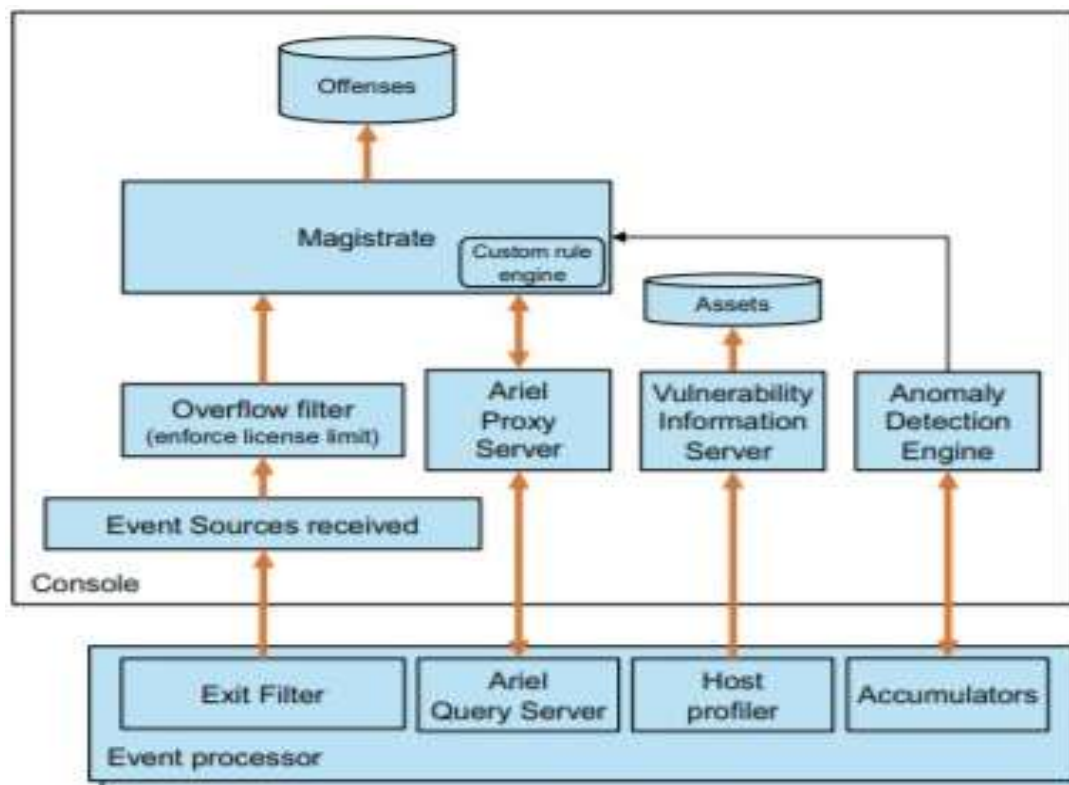
By default, rules are tested against events or flows received by a single event processor (local rules). The Exit Filter sends on any events or flows that have been marked for further processing by the Magistrate component on the Console.

Every event and flow is then sent on to the Event Storage Filter, where they are stored in the events or flows Ariel database.

If a new port or host is detected at this time, an asset profile needs to be updated or created in the PostgreSQL database. The Host Profiler, or Host Profiling Filter, sends the collected information about the new host to the Console, so that a new asset can be created or updated.

Finally, if an analyst has defined any searches to collect and investigate specific sets of data, events and flow records are accumulated every minute and stored in the accumulator Ariel database. These accumulations create time-series statistical metadata that is used for Dashboards, event and flow forensics and searching, reporting, and the Anomaly Detection Engine on the Console. Accumulated time intervals can be defined as 1 minute, 1 hour, and 1 day. The Accumulator is a distributed component that operates on each Event Processor.

- Console architecture



The Console receives data from the deployed Event Processors for further analysis by the Magistrate component, which creates and stores offenses in the PostgreSQL database. These offenses are then brought to the analyst's attention in the user interface. The Magistrate instructs the Ariel Proxy Server to gather information about all related events and flows that triggered the creation of an offense. The collected data is then available for further investigation by the analyst.

If data is collected from multiple Event Processors, the Console's Custom Rules Engine can utilize Global Cross Correlation to test rules on data from all deployed Event Processors. This helps to locate more complex attacks, which can span across the overall IT infrastructure and are not confined to being detected by a single Event Processor.

The Vulnerability Information Server (VIS) creates new assets, or adds open ports or discovered services to existing assets, based on information from the Host Profiler on the Event Processors. This happens when hosts, services, or vulnerabilities that cannot be mapped to existing assets are discovered.

The Anomaly Detection Engine (ADE) searches the Accumulator databases for anomalies, which are then used for offense evaluation. There are three categories of Anomaly Detection Rule types.

- The Threshold rule examines a numeric range, such as greater than, less than, or a particular range. This rule can help detect the bandwidth of an application, the number of users connected to a VPN, or a large and unusual outbound data transfer.
- The Anomaly rule looks at a change in short term when comparing against a longer time frame. This can help to locate new service activity or a change in the bandwidth volume on a specific link.
- The Behavioural rule can detect changes from the same time yesterday or last week. This includes mail traffic, for example, the increase in external SMTP server traffic, which could be a relay. This rule can also be used for regular IT services, such as backup monitoring, where the rule would trigger if a backup failed.

Let us take one closer look at how Offenses are being managed by the Magistrate component. Events and flows that have been tagged by the Custom Rules Engine for further processing in the Event Processors are being handed over to the Console through the Exit Filter. Until now, we have examined the QRadar component structure from a deployment viewpoint. Let us now take a final look into dissecting the flow of a captured event.

5. Real-World Attack Scenarios

- **About Target Corporation**

Target Corporation is an American retailing company, founded in 1902 and headquartered in Minneapolis, Minnesota. It is the second-largest discount retailer in the United States, with Walmart being the largest. The company is ranked 36th on the Fortune 500 as of 2013 and is a component of the Standard & Poor's 500 indexes. Target grew and eventually became the largest division of Dayton Hudson Corporation, culminating in the company being renamed as Target Corporation in August 2000. Target operates 1,916 stores in the United States; it began operations in Canada in March 2013 and operates 127 locations through its Canadian subsidiary. In December 2013, a data breach of Target's systems affected up to 110 million customers.

The situation In November and December 2013, cyber thieves executed a successful cyber-attack against Target, one of the largest retail companies in the United States. The attackers gained access to Target's computer network, stole the financial and personal information of as many as 110 million Target customers, and then removed this sensitive information from Target's network to a server in Eastern Europe. John Mulligan, Target's Executive Vice President and Chief Financial Officer, testified that his company "had in place multiple layers of protection, including firewalls, malware detection software, intrusion detection, and prevention capabilities and data loss prevention tools." He further stated that Target had been certified in September 2013 as compliant with the Payment Card Industry Data Security Standards (PCI-DSS), which credit card companies require before allowing merchants to process credit and debit card payments."

Within a very short period of two months, cyber thieves executed a successful cyber-attack against Target. The attackers gained access to Target's computer network, stole the financial and personal information of as many as 110 million Target customers, and then removed this sensitive information from Target's network to a server in Eastern Europe.

Target had in place multiple layers of protection, including firewalls, malware detection software, intrusion detection, and prevention capabilities, and data loss prevention tools. Additionally, Target had been certified in September 2013 as compliant with the Payment Card Industry Data Security Standards (PCI-DSS), which credit card companies require before allowing merchants to process credit and debit card payments.

How

This investigative data has been made publicly available through the United States Committee On Commerce, Science, And Transportation.

Phases of the intrusion kill chain

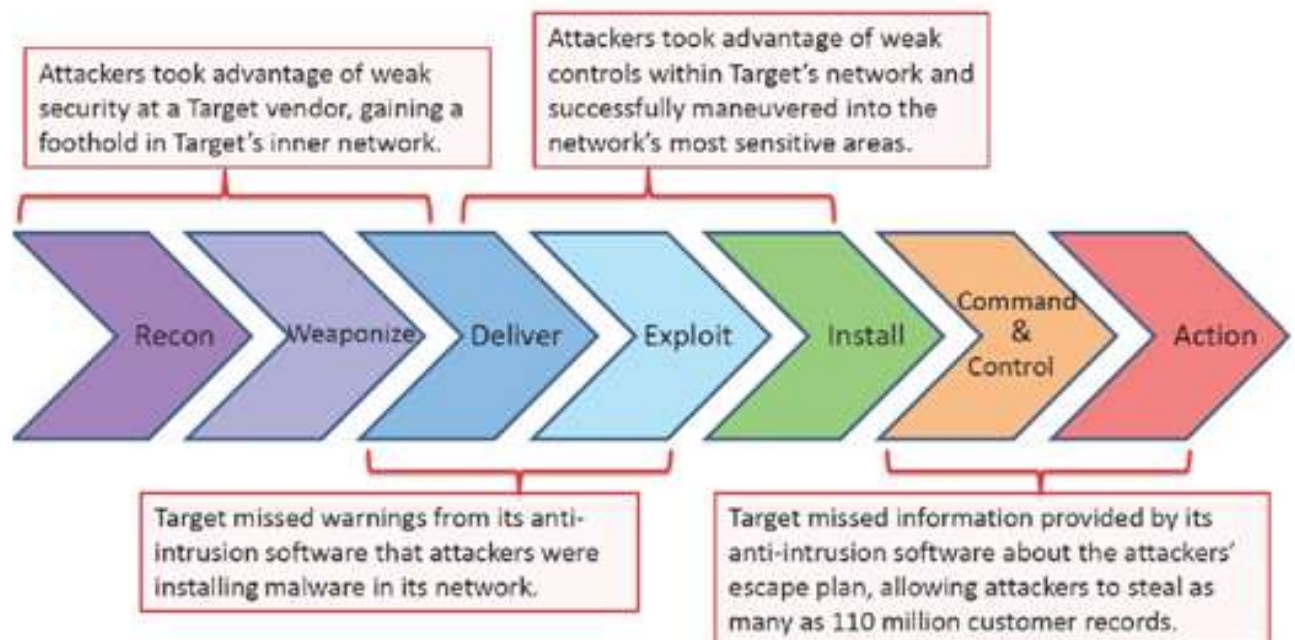


Every attack begins with a reconnaissance phase where the attackers select their main targets. Once they have their data identified, they research and identify external and potentially vulnerable connections. These can include direct network access points or systems, as well as employees or third-party vendors and business partners. In the weaponization phase the attacker's pair remote access malware with well-known exploits into a deliverable payload, such as Adobe PDF or Microsoft Office files.

The delivery phase consists of the actual transmission of the weapon to a target. The most common approach is to use phishing attacks via email attachments, websites, or even physical USB drives. Once delivered, the weapon's code is triggered on the target systems, exploiting vulnerable applications or systems. During the installation phase, the weapon now installs a backdoor on a target's system, allowing persistent access. It is also very common for the weapon to regularly install new variants to avoid or distract detection.

Once the weapon is activated it begins communicating with outside servers that provide real-time system access for the attackers, who can now extend their reconnaissance from within the attacked network and systems. After final weapons and communication paths are established, the attackers work to achieve the objective of the intrusion. Most likely, this includes exfiltration, encryption, or destruction of data.

Missed opportunities



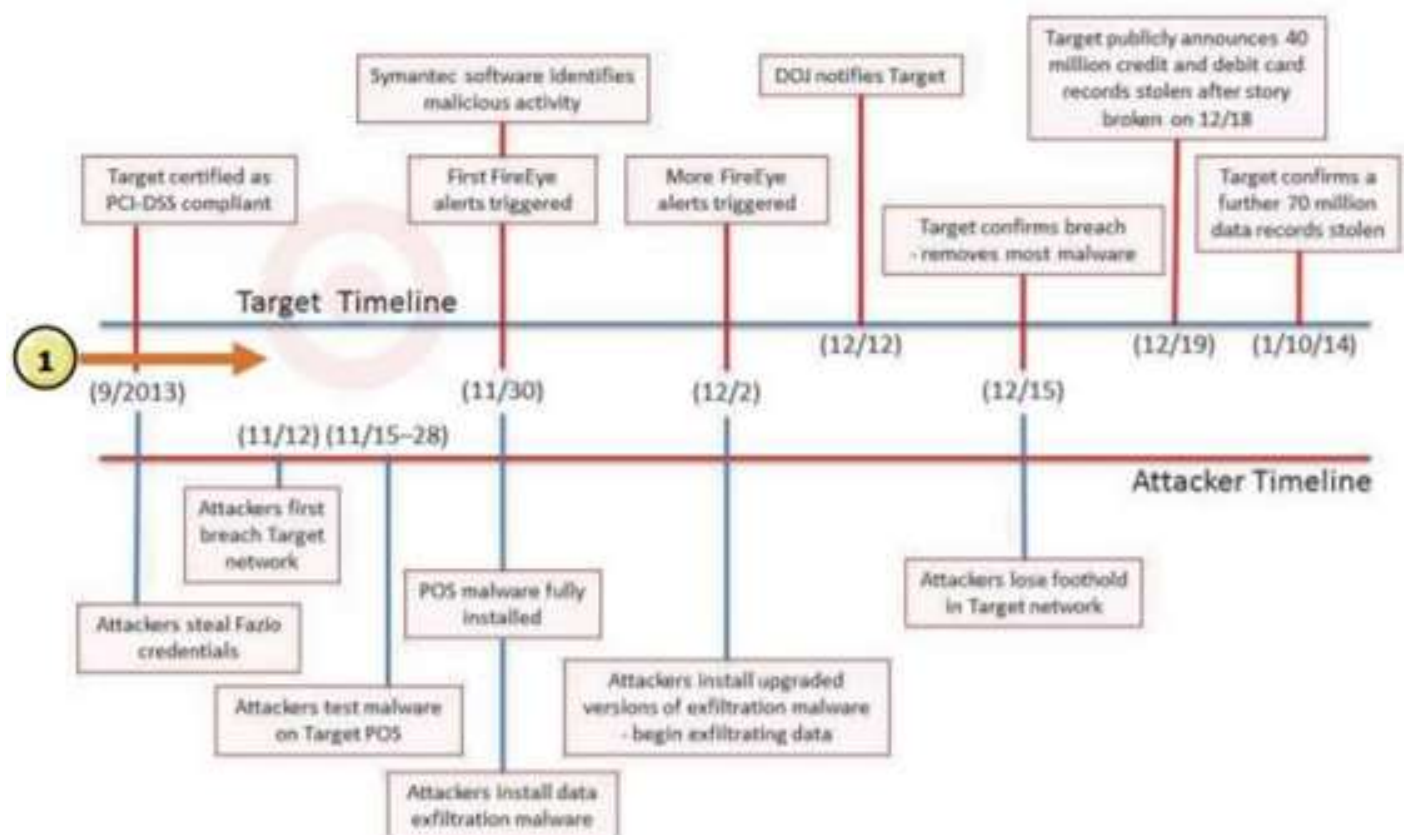
Several situational actions and reactions lead to the disaster. First, the attackers took advantage of weak security at a Target vendor, and thus, gaining an initial foothold in Target's inner IT network. This happened while

Target missed initial warnings from their anti-intrusion software that attackers were installing malware on their deployed assets.

Then the attackers took advantage of further weak controls within Target's network and successfully maneuvered into the network's most sensitive areas. During the final phase of the attack, Target missed more information by its anti-intrusion software about the attackers' escape plan, allowing them to steal as many as 110 million customer records.

Source: https://www.commerce.senate.gov/public/_cache/files/24d3c229-4f2f-405d-b8db-a3a67f183883/23E30AA955B5C00FE57CFD709621592C.2014-0325-target-kill-chain-analysis.pdf

- Kill Chain Timeline

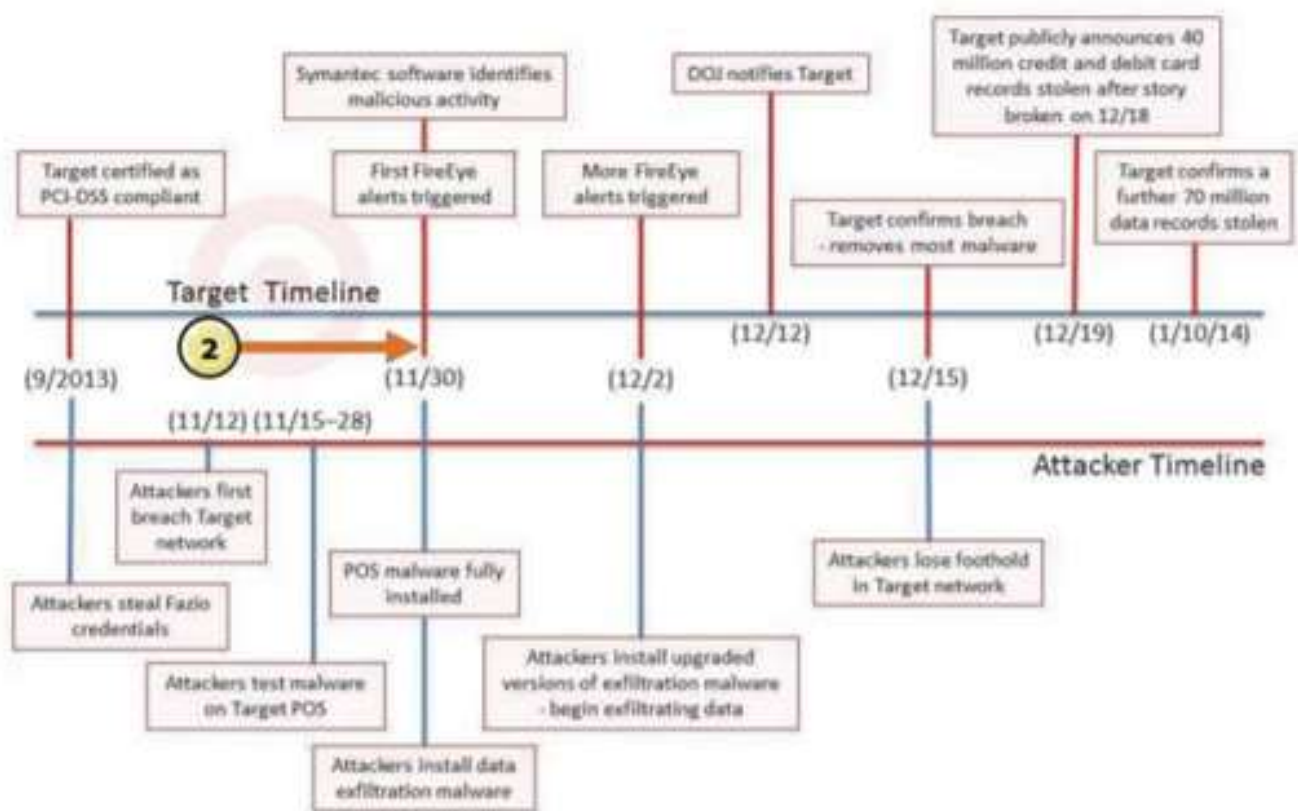


Roughly at the same time when Target was PCI-DSS certified, the first phases of the attack were executed. In the first reconnaissance phase, the attacker gathered as much information about the victim. In this case, the attackers were able to find information about Target's third-party

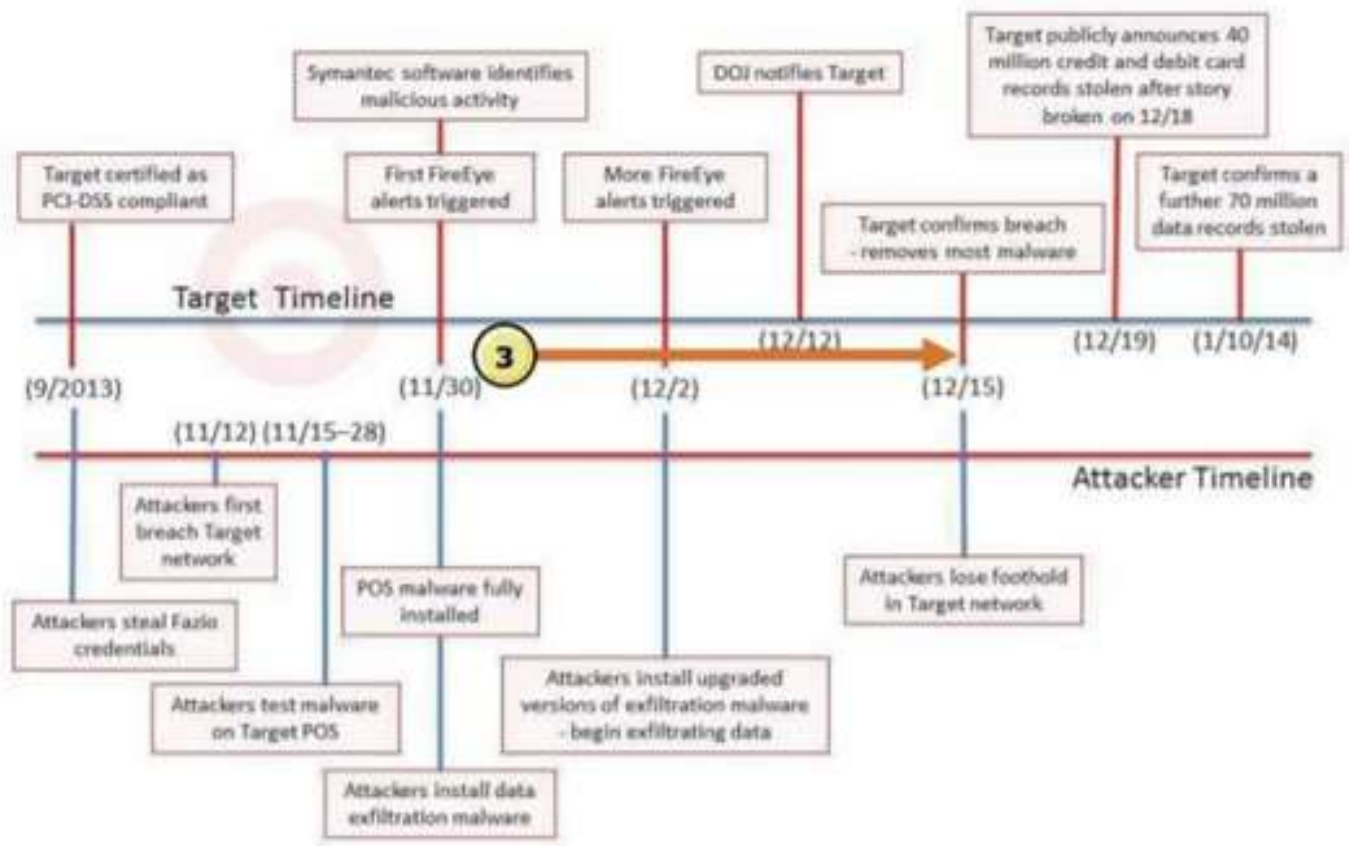
vendor through simple Internet searches. Target even displayed a public Internet portal for vendors, which gave away the kind of software that was used for their online vendor billing. Equipped with this knowledge, the attacker then started their reconnaissance on one particular vendor, Fazio.

In the weaponization phase, the attackers created malware stricken emails, likely attaching a PDF or Microsoft Office document. In the first part of the delivery phase, the attacker sent infected emails to the vendor in a so-called phishing attack.

Once deployed, the malware started to record passwords and provided the attackers with their key to Target's external billing system.



In the second part of the delivery phase, the attackers leveraged their access to this vendor's system to enter Target's network. Weak security at the perimeter of Target's network may have contributed to the attackers' success in breaching the most sensitive area of Target's network containing cardholder data. Using the vendor's credentials to gain access to Target's inner network, it appears the attackers then directly uploaded their RAM scraping malware to POS terminals.



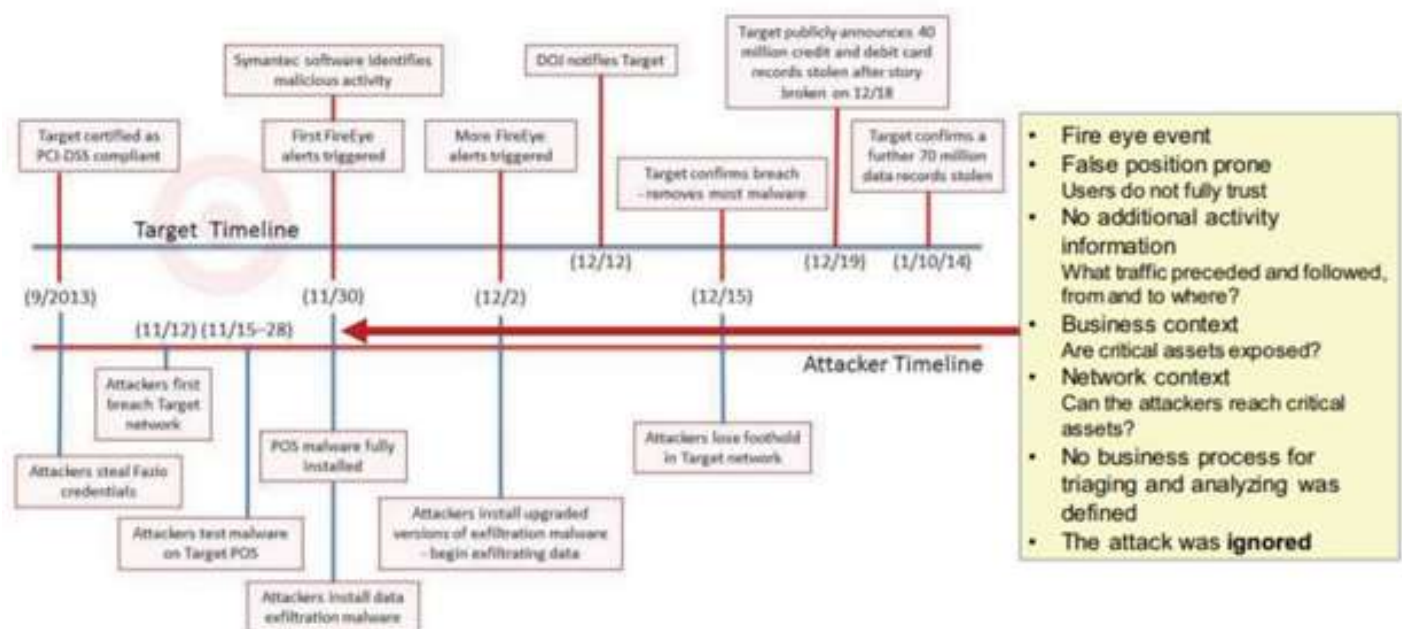
In the exploitation phase, the RAM scraping malware and exfiltration malware began recording millions of card swipes and storing the stolen data for later exfiltration. Reports suggest that the attacker maintained access to the vendor's systems for some time while attempting to further breach Target's network during the installation phase.

It is unclear exactly how the attacker could have escalated its access from the external billing system to deeper layers of Target's internal network. But given the installation of the Black POS malware on Target's POS terminals, the compromise of 70 million records of non-financial data, and the compromise of the internal Target servers used to gather stolen data, it appears that the attackers succeeded in moving through various key Target systems by exploiting default account names in Target's IT management system.

Based on the reported timeline of the breach, the attackers had access to Target's internal network for over a month and compromised internal servers with exfiltration malware by November 30. While the exact method by which the attackers maintained command and control is unknown, it is clear, that the attackers were able to maintain a line of communication between the outside Internet and Target's cardholder network. The attackers transmitted the stolen data to outside servers – at least one of which was located in Russia – in plain text via FTP (a standard method for transferring files) over the course of two weeks.

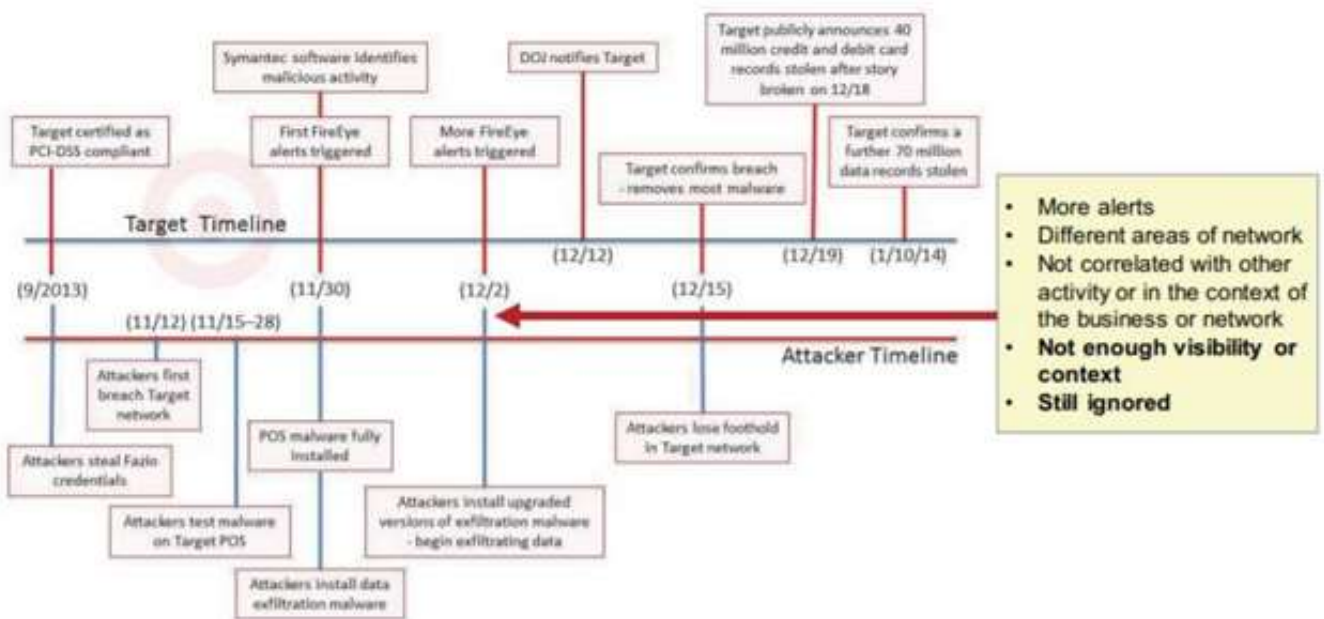
On December 12, the US Department of Justice notified Target that their stolen credit card credentials have been identified on a Russian Dark Web site where they were offered for sale. At this point in time, no one at Target had realized that there was an attack. Target immediately started intense investigations and was able to stop further activities to exfiltrate data, and three days later most of the malware had been removed. It was at this time when Target found out not only about the loss of 40 million credit card records but also an additional 70 million customer data records without financial information.

- Revisit the attack

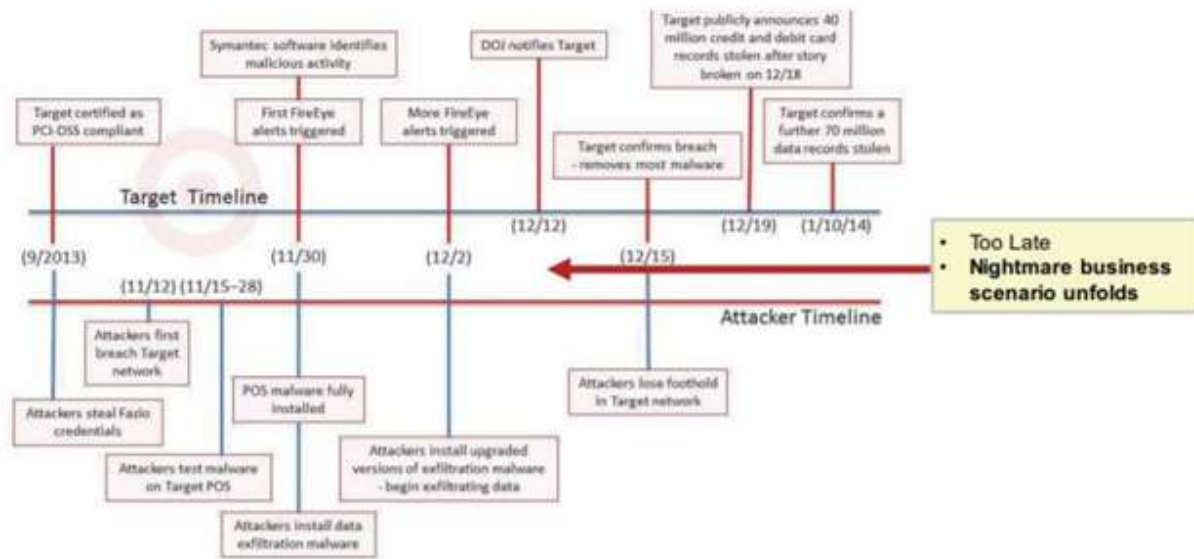


Revisiting the investigative timeline shows that the first security-relevant events from FireEye and Symantec endpoint were recorded on November 30.

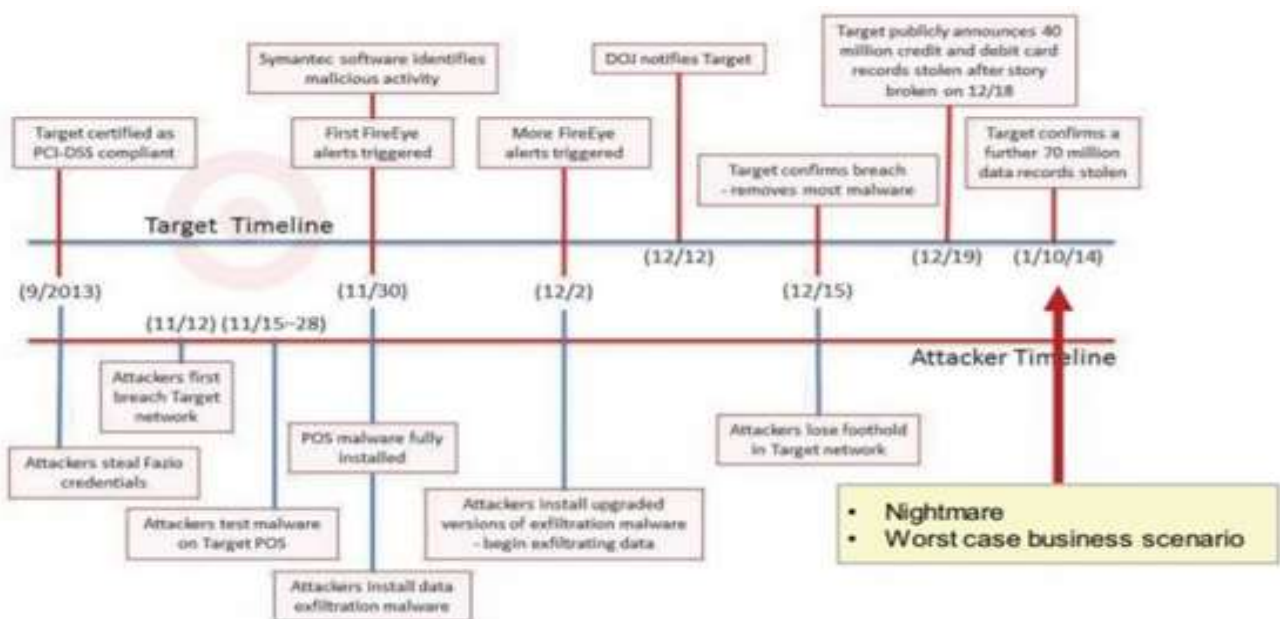
Firewall and endpoint analysts may have disregarded these events as false positives because no action was initiated. The reason for that can be founded in the complexity, where those point solutions do not communicate with one another. It is hard to retrieve additional activity information about the preceding and following traffic, and to realize business and network context by just looking at individual incidents without any correlation. The ability to include business context and risk management can show if any high-value assets are exposed by a certain attack pattern. Network context shows if those assets can be physically reached by the malware. Without the means for correlating the individual events, the attack was ignored.



Once the exfiltration began the Target security tools recorded more alerts. But again, without proper correlation to the earlier events and network traffic logs, there was simply not enough visibility into the ongoing malware deployment and data exfiltration. This resulted in the fact that the ongoing attack was still being ignored.



At the time when the DOJ called the Target executive management, it was too late to react. The started forensic investigation enabled the security team to find malware on POS terminals and on backend data servers as well as ongoing exfiltration transmissions to external FTP servers. The communication lines were then severed and the malware removed from the systems.



Only within their forensic activities, the security staff found out about the additional 70 million non-financial data records that had been compromised. It was an awakening of the worst-case business scenario any organization can possibly face.







Module 4:

Investigation

of Alerts

(Events/Flow)

-
- 1. Investigation of Alerts (Events/Flow) using Security Incident & Event Management solution**
-
- 2. Assets**
-
- 3. Events and Investigating Offences based on Events**
-
- 4. Flows and Investigating Offences based on Flows**
-
- 5. Contextual Data vs Event/Flows Data**
-

1. Investigation of Alerts (Events/Flow) using Security Incident & Event Management solution

Investigation of Alerts (Events/Flow) using Security Incident & Event Management solution

In this unit, we will learn about the SIEM Investigation methodology of Alerts/Incident using our SIEM Tools.

2. Assets

An asset profile maintains technical and organizational information about a system in your organization's network. Collecting and viewing asset data helps you to identify threats and vulnerabilities. An accurate asset database makes it easier to connect offenses that are triggered in your system to physical or virtual assets in your network.

- Asset data

An asset is any network endpoint that sends or receives data across your network infrastructure. For example, notebooks, servers, virtual machines, and handheld devices are all assets. Every asset in the asset database is assigned a unique identifier so that it can be distinguished from other asset records.

Detecting devices are also useful in building a data set of historical information about the asset. Tracking asset information as it changes helps you monitor asset usage across your network.

- Asset profiles

An asset profile is a collection of all information that IBM QRadar SIEM collected over time about a specific asset. The profile includes information about the services that are running on the asset and any identifying information that is known.

QRadar SIEM automatically creates asset profiles from identity events and bidirectional flow data or, if they are configured, vulnerability assessment scans. The data is correlated through a process that is called asset reconciliation and the profile is updated as new information comes into QRadar. The asset name is derived from the information in the asset update in the following order of precedence:

- Given name
- NetBIOS hostname
- DNS hostname
- IP address

- Collecting asset data

Asset profiles are built dynamically from identity information that is passively absorbed from an event or flow data or data that QRadar actively looks for during a vulnerability scan. You can also import asset data or edit the asset profile manually.

- Sources of asset data: Asset data is received from several different sources in your IBM QRadar deployment.
- Incoming asset data workflow: IBM QRadar uses identity information in an event payload to determine whether to create a new asset or update an existing asset.
- Updates to asset data: IBM QRadar uses identity information in an event payload to determine whether to create a new asset or update an existing asset.
- Identification of asset growth deviations: Sometimes, asset data sources produce updates that IBM QRadar cannot handle properly without manual remediation. Depending on the cause of the abnormal asset growth, you can either fix the asset data source that is causing the problem or you can block asset updates that come from that data source.
- Asset blacklists and whitelists: IBM QRadar uses a group of asset reconciliation rules to determine if asset data is trustworthy. When asset data is questionable, QRadar uses asset blacklists and whitelists to determine whether to update the asset profiles with the asset data.
- Asset profiles: Asset profiles provide information about each known asset in your network, including what services are running on each asset.

3. Events and Investigating Offences based on Events

Events and Investigating Offences based on Events

An Event is a record of action on a machine. The investigation of an offense usually leads to the investigation of the events that contributed to the offense. An offense alerts to suspicious activity and links to helpful information to investigate it. One of the first steps when investigating the events of an offense is to examine the event data at a high level.

- The prime benefit of QRadar SIEM for security analysts is that it detects suspected attacks or policy violations and ties helpful information together into offenses to investigate them
- Some common offenses include these examples
 - Multiple login failures
 - Malware infection
 - P2P traffic
 - Scanner reconnaissance
- Treat offenses as security incidents and have a security analyst investigate them

More examples of offenses include

- Clear Text Application Usage
- Remote Desktop Access from the Internet
- Connection to a remote proxy or anonymization service
- SSH or Telnet detected on Non-Standard Port
- Large outbound data transfer
- Communication to a known Bot Command and Control
- Local IRC Server detected

Creating and rating offenses

- QRadar SIEM creates an offense when events, flows, or both meet the test conditions specified in changeable rules that analyze the following information
 - Incoming events and flows
 - Organizational context
 - User information, such as admin, newhire, CFO-team
 - Network and server information, such as web server, PCI network, crown jewels
 - Threat intelligence
 - IP addresses and domain names of malicious hosts, such as

- spam senders
- malware hosts
- anonymous proxies
- IP address ranges dynamically assigned by ISPs•
- The **magistrate** component running on the Console appliance maintains all offenses; it rates each offense by its **magnitude**, which has these characteristics
 - Ranges from 1 to 10, with 1 being low and 10 being high
 - Prioritizes each offense by its relative importance

Commonly the term crown jewels refer to the servers that are most critical for an organization's mission. Typically, crown jewels store and process customer, employee and financial data, as well as intellectual property.

4. Flows and Investigating Offences based on Flows

Flows and Investigating Offences based on Flows

A flow is a record of the communication between network sockets. IP address, port, and transport protocol uniquely identify a network socket. QRadar SIEM correlates flows into an offense if it determines suspicious network activities

A flow provides information about a network activity between two or more systems. In this lesson, you learn from which data QRadar SIEM creates flows and which information they provide. An offense bundles information about suspicious activity, including flows

- From the network activity information that QRadar SIEM receives, it creates flows
- Like a phone bill, QRadar SIEM records inflows who talked to whom, at which time, but not the content of the conversation
 - From unencrypted communications, QFlow can capture layer 7 payloads up to a configurable number of bytes
- A flow can include information about the conversation, such as these examples
 - Start Time

- o End Time
- o Source and destination IP addresses
- o Source and destination ports
- o Number of bytes transferred
- o Number of packets transferred
- o Network protocol
- o Application protocol
- o TCP flags

While an event occurs at a single point of time, a flow has a start and end time. Most flows have only a short duration, but flows representing the transfer of a huge file or streaming of a movie can last for hours. Flows update asset profiles of servers with the ports and services that are running on them.

Creating flows from network activity information

- o External sources: Network devices
 - o Flow collectors create flows from IPFIX/NetFlow, sFlow, J-Flow, Packeteer, and Flow log file received from network devices
 - o Network devices provide only a subset of the control information in network packet headers and no payload
 - o To determine the application protocol, flow collectors look up which application protocol commonly uses the recorded network protocol and destination port
- o Internal sources: QFlow and QRadar Network Insights (QNI)
 - o Flow collectors create flows from network activity monitored by QFlow and QNI similar a network sniffer
 - o Both provide the first bytes of packets to QRadar SIEM in order to detect the application protocol without regard to the network protocol and destination port being used
 - o Both extract the same control information that is available in network activity information from external sources

- o QFlow can capture layer 7 payload up to a configurable number of bytes unless it is encrypted
- o QFlow can extract user-defined Custom Flow Properties from the part of the payload that it captured
- o QFlow stores the part of the payload that it captured
- o QNI analyses complete layer 7 payload unless it is encrypted
- o QNI can extract pre-defined properties, such as DNS queries, HTTP headers, and MD5 checksums of transferred files
- o QNI does not store payload other than the extracted properties

For flows created from IPFIX/NetFlow, sFlow, J-Flow, Packeteer, and Flow log files QRadar SIEM cannot detect the Skype application protocol because Skype uses many ports. QFlow and QNI detect Skype because they analyze the first bytes of packets. QFlow and QNI perform the same application protocol detection.

The QFlow application detection is unrelated to its ability to capture and store a configurable number of bytes from each packet. Therefore, the QFlow application detection still works if a QRadar administrator configures QFlow to capture and store 0 bytes from packets. However, Custom Flow Properties are not extracted any more if payload capture is disabled

6. Contextual Data vs Event/Flows Data

Contextual Data vs Event/Flows Data

Event/Flow data will give the details like Source, destination, username, point in time, etc. It collects data that is being generated by the only log sources. Here in order to have a better analysis of the current data, contextual information on top of event/flow data helps SIEM to detect the more accurate alerts. Threat intelligence provides contextual information that can be used by SIEM tools for better analysis and detection. Threat intelligence feeds which are continuous streams of actionable information on existing or potential threats and bad actors. Security vendors and analysts collect security data on IoCs such as anomalous activity and malicious domains and IP addresses, from a number of sources through threat intelligence feeds like X-force by IBM for the contextual data





Module 5:

SIEM

Detection

Mechanism

Using

Rules/Policies

1. SIEM Detection Mechanism Using Rules/Policies

2. SIEM Policies and groups

3. Identification of policies that triggered from alerts

4. Investigate which test conditions caused a rule to fire

5. Examine rule actions and responses

6. Anomaly detection rules

7. Network Hierarchy

8. Use networks in investigations

9. Offenses overview by network

1. SIEM Detection Mechanism Using Rules/Policies

Bookmark this page

SIEM Detection Mechanism Using Rules/Policies

In this unit, we will learn about the Security Incident & Event Management tool for using the detection mechanics. In most of the SIEM Solution basic detection mechanism includes Rules and/or Policies.

2. SIEM Policies and groups

Bookmark this page

SIEM Policies and groups

SIEM solutions now provide out-of-the-box correlation policies aka rules and sophisticated models to surface a broad range of abnormal behaviour and events. Once you understand how they work, you'll likely want to customize these resources, while also adding your own rules and models to suit your organization's unique situation

A correlation rule, a.k.a., fact SIEM Policies, is a logical expression that causes the system to take a specific action if a particular event occurs. For example, "If a computer has a virus, alert the user." In other words, a correlation rule is a condition (or set of conditions) that functions as a trigger.

- The tests of rules correlate the information to monitor for the following kind of indicators

Indicator of Compromise For example

- Reconnaissance from local hosts

- Beaconsing

Indicator of Concern For example

- Reconnaissance from remote hosts

- DDOS attack ramping up

- This module follows the common practice to use the following terms, instead of using the rule evaluate to true

- a rule fires

- a rule matches

- a rule tags an event or flow

- a rule contributes to an offense

3. Identification of policies that triggered from alerts

Bookmark this page

Identification of policies that triggered from alerts

Correlation Based on the alert generated, SIEM provides us the ability to track the originated policies or rules associated with it. In short, Policies decide what should be triggered at what point of time based on certain conditions.

4. Investigate which test conditions caused a rule to fire

Bookmark this page

Investigate which test conditions caused a rule to fire

Let's Analyse a rule from the SIEM QRadar which triggered an alert aka offense.

Rules test conditions

- Rules can perform the following tests
- IP address belongs to a network
- Flow Bias

- Only available for rules of type Flow
- Context
 - The Event and Flow Direction are equivalent to the Context

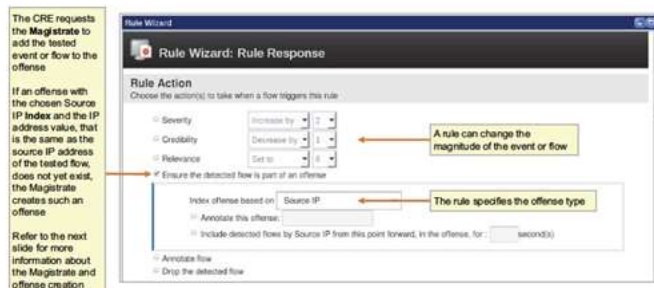


5. Examine rule actions and responses

Bookmark this page

Examine rule actions and responses

Like the if-then statement in programming languages, a custom rule executes actions and responses if it evaluates to true. When a rule fires, QRadar SIEM executes its actions.



Dropping an event or flow prevents the CRE from executing any further rules that have not already been executed. At this point, some of the rules that have already been executed might have fired and the CRE has already executed or initiated their actions and responses. Dropping an event or flow does not delete it. The event or flow is still stored and searchable; therefore, it shows up in search results and reports.

- Based on the index, the Magistrate maintains offenses

Bookmark this page

Based on the index, the Magistrate maintains offenses

- The Magistrate component of QRadar SIEM maintains all offenses and determines whether to add an event or flow to an existing offense or create a new offense
- The Magistrate assumes that rules firing for the same index property and property value relate to the same security issue; therefore, the Magistrate maintains only one active offense indexed on the same property and property value at any given time

Example: A rule fires and requests that the Magistrate add the event or flow to an offense indexed on source IP address 192.168.10.10

- If such an offense already exists, the Magistrate adds the event or flow to it. If such an offense does not exist, the Magistrate creates an offense indexed on the source IP address 192.168.10.10, and adds the event or flow to it
- A rule should index its offense on the key property in its tests; for example, the **Username** property is the appropriate index for a rule that tests for 5 login failures with the same user name
- More than one rule can fire for an event or flow
 - For rules firing with the same index property and property value, the Magistrate adds the event or flow to the same offense; therefore, more than one rule can add events and flows to one single offense
 - For each rule firing with different index properties or property values, the Magistrate adds the event or flow to each of the separate offenses
- To identify an offense uniquely, the Magistrate requires both the property and its value. The value alone is not enough. For example, an offense can be indexed on the source IP address 192.168.10.10, and another offense can be indexed on the same IP address 192.168.10.10, but as the destination IP address. This happens when a compromised machine attacks other target. QRadar SIEM chains such offenses.
- The difference between the CRE and Magistrate is as follows:
 - The CRE tests events and flows. It tags each event and flows with each custom rule and building block that fires for it, regardless of the Rule Action and Rule Response.
 - The Magistrate maintains offenses. It adds events and flows to offenses if told so by the Rule Action and Rule Response. The Magistrate only runs on the Console.

- Rule response

Bookmark this page

Rule response

The CRE requests the Magistrate to create an offense, if an offense with the same property chosen as index and same property value as the tested flow does not already exist.

The Magistrate adds the new event to the existing or newly created offense.

The rule requests the CRE to create a new event for these purposes:

- Name the offense appropriately
- Simplify searching and reporting on the detected indicator

- The Custom Rule Engine (CRE) is the log source of the new event because the CRE creates all events that are triggered by custom rules.
- The user interface often refers to the name of an offense as the description

Limit how often the CRE executes the configured rule responses

Send email to addresses

- Each CRE in a QRadar SIEM deployment maintains the counter and time frame separately. Therefore, you can, for example, receive more emails than the configured limit if a rule fire with separate CREs.
- The Response Limiter configuration limits every option under Rule Response, including the frequency of dispatched or forwarded events.

6. Anomaly detection rules

Anomaly detection rules

Anomaly Detection rules alert to deviations from recorded past activities.

- An anomaly detection rule tests the results of a saved event or flow search to detect deviations from usual activity patterns
- The saved search needs to be grouped and needs to have capturing of time series data enabled
- The Anomaly Detection Engine (ADE) executes the anomaly detection rules
- An anomaly detection rule only tags the event that it creates as a rule response but not the event or flow that triggered it; this has two implications
 - It is not possible to search and report on events and flows that triggered an anomaly detection rule
 - In the Rule Wizard, an anomaly detection rule has only a Rule Response but not a Rule Action because the Rule Action only works on the triggering event or flow
- Typically, anomaly detection rules monitor over longer timespans than custom rules

Like CRE instances, ADE instances run on the Console appliance and on each event and flow processor appliance.

Navigating to anomaly detection rules

- QRadar SIEM displays both anomaly detection rules and custom rules under the Offenses tab
- Three types of anomaly detection rules are available

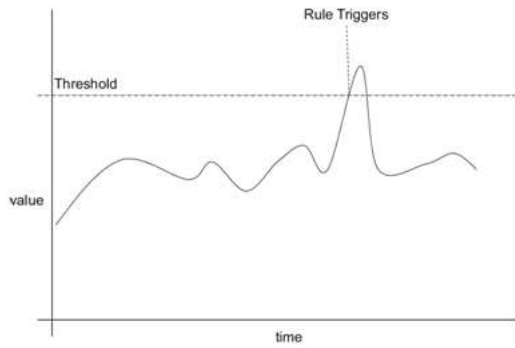


Rule Name	Group	Rule Category	Rule Type
Example: Anomaly	Example	Anomaly Detection Rule	Anomaly
Example: Behavioral	Example	Anomaly Detection Rule	Behavioral
Example: Threshold	Example	Anomaly Detection Rule	Threshold
100% Accurate Events	Intrusion Detection	Custom Rule	Event
All Exploits Become Offenses	Intrusion Detection	Custom Rule	Event

Rule groups can contain custom rules and anomaly detection rules. The predefined rule group with the name Anomaly is not restricted to anomaly detection rules

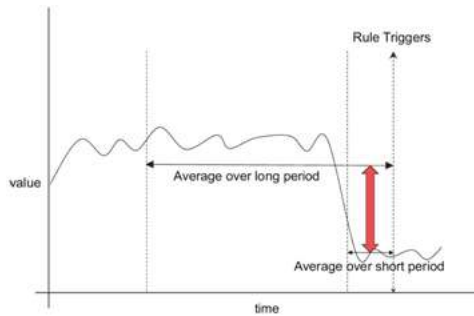
Threshold rules

Test whether a property value surpasses an upper or lower boundary



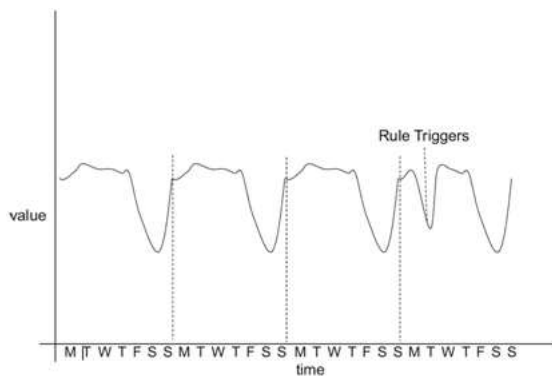
Anomaly rules

Test whether the average property value during the current short time range deviates above the configured percentage from the baseline over a longer time range



Behavioural rules

- Test whether current property values deviate from seasonal patterns
- A Behavior rule learns the rate or volume of a property value over the configured time to establish a baseline



Reference Links - <https://www.ibm.com/support/pages/node/264805>

7. Network Hierarchy

Network Hierarchy

Bookmark this page

Network Hierarchy

The Network Hierarchy reflects your environment from a security perspective.

- QRadar SIEM displays and uses network information, such as
 - IP address in the DMZ
 - Network connections initiated from an IP address belonging to your organization
 - The subnet storing and processing customer data that is the target of more offenses than any other subnet
- QRadar SIEM draws such network information from the Network Hierarchy
- QRadar SIEM considers every IP address that is part of a network configured in the Network Hierarchy as local to your organization's network
- QRadar SIEM considers any other IP address as remote
- Many rules, searches, and reports use the Network Hierarchy

The Network Hierarchy comes preconfigured with the IP address ranges reserved for private use because they cannot be routed through the public internet and therefore can only be local

Crown jewels

- Many organizations specify their crown jewels in the Network Hierarchy and monitor them more granularly for indicators, and run specific searches and reports
- The term crown jewels refers to the hosts that store and process data most critical for an organization's mission
- Crown jewels handle the following kinds of data

- o Customer
- o Employee
- o Financial
- o Intellectual property

Tree structure

- o If an IP address is part of a CIDR range of a network object, QRadar SIEM tags the IP address with this network object and its groups
- o If an IP address matches more than one network object, QRadar SIEM tags the IP address with the network object with the smallest IP range

CIDR ranges

The CIDR ranges do not need to match the tree structure

A CIDR of a network object can include a CIDR range of another network object regardless of its location in the hierarchy

The primary purpose of the hierarchy is to provide a structure for CIDR ranges that rules, searches, and reports can use

The Network Hierarchy structures your network according to security policies, requirements, and concerns

The Network Hierarchy does not need to reflect your technical network layout

Usually, the names of groups and network objects reflect purpose, department, and location because they determine security requirements

QRadar SIEM's Asset Profiler creates and updates asset profiles only for IP addresses that are part of any of the CIDR ranges in the Network Hierarchy

8. Use networks in investigations

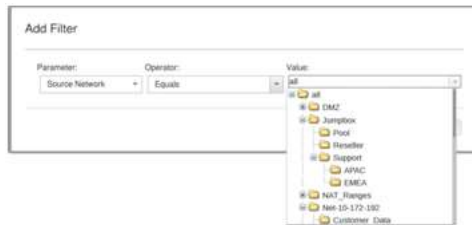
Use networks in investigations

The network hierarchy is often beneficial to security-related analysis, including offense investigation.

Filtering by network

- o You can use networks in many ways for investigations, for example for filtering

- If you select a group, QRadar SIEM filters for all CIDR ranges of the group's descendants



Grouping by network - LogActivitytab



NetworkActivity



9. Offenses overview by network

Offenses overview by network

Bookmark this page

Offenses overview by network

Survey your threat landscape from the perspective of your networks

[illegible]

- Other includes all IP address that are not part of a network configured in the Network Hierarchy
- Number of Offenses with one or more targeted network
- Number of offenses with one or more attackers in the network





Module 6:

SIEM

Reporting &

Dashboards

for SOC

Monitoring

1. SIEM Reporting & Dashboards for SOC Monitoring

2. Tabs

3. SIEM Dashboard

4. SIEM Reports

5. Applying filters

6. Filtering events and flows

7. Filtering events

1. SIEM Reporting & Dashboards for SOC Monitoring

SIEM Reporting & Dashboards for SOC Monitoring

In this unit, we will learn the Security Incident & Event Management tool capabilities of reporting & Dashboard which are basic needs of the Security Operations Centre as part of monitoring.

2. Tabs

Tabs

To leverage QRadar, use its tabs

- Dashboard: Monitor various activities in your environment
- Offenses: Query and display suspicious activities
- Log Activity: Query and display events
- Network Activity: Query and display flows
- Assets: Query and display information about systems in your environment.
- Reports: Create templates and generate reports
- Admin: Administrative system management



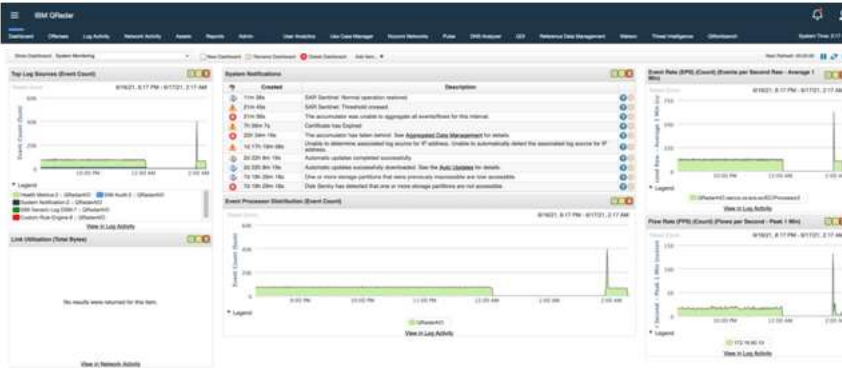
To reset a tab to its default settings, double-click it. The QRadar SIEM user interface provides tabs that let you navigate and focus on specific slices of the collected, analyzed, and displayed data. Two more tabs become available with a license for QRadar Vulnerability and Risk Manager installed:

- Risks: Query and display risks in your environment
- Vulnerabilities: Query and display vulnerabilities in your environment

3. SIEM Dashboard

SIEM Dashboard

QRadar SIEM displays the Dashboard tab after you have signed in. Items on a dashboard display information about activities in your network. The items enable you to focus on specific areas of interest. You can customize and add new items and dashboards. A dashboard hosts several dashboard items in order to provide real-time visibility into activity in your environment



The user interface of QRadar SIEM is your workbench to gain visibility into your environment from a security perspective

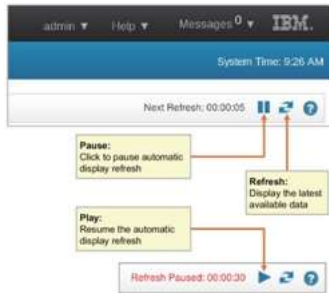
- Dashboards are like a canvas for dashboard items
- You can create custom dashboards to focus on your security or operations responsibilities
- Each dashboard is associated with a user; changes that you make to a dashboard do not affect the dashboards of other users



Managing the displayed data

Every minute QRadar SIEM automatically refreshes the data on the following tabs

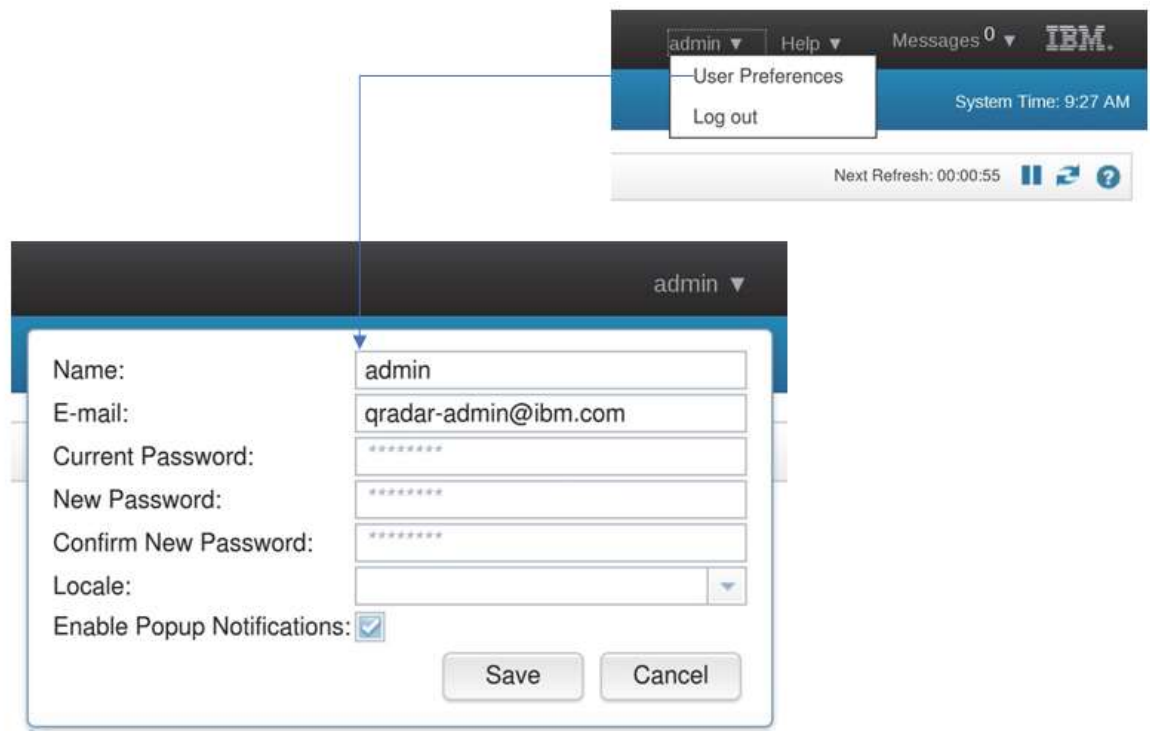
- Dashboard
- Log Activity
- Network Activity
- Reports



QRadar SIEM works in 1-minute cycles. When a 1-minute cycle finishes, event and flow processors send to the Console the data from the passed minute, that is needed there. Clicking the Refresh button resets the displayed countdown to 60 seconds, but the results returned can still come from the prior minute. The countdown in the user interface does not necessarily run-in sync with the 1-minute cycles.

The Pause button stops only refreshes of the display. QRadar SIEM continues to process data in the background

Managing your QRadar user



User Preferences:

Users can change their password in the Preferences if they authenticate with the local system authentication of QRadar SIEM. Users cannot change the password in the User Preferences if QRadar SIEM uses RADIUS, TACACS, Active Directory, or LDAP for their authentication.

In most deployments, the user admin authenticates with the local system authentication of QRadar SIEM even if other users use external authentication. Therefore, the user admin usually changes passwords in QRadar SIEM User Preferences.

Accessing help



- Customize dashboard items

Bookmark this page

Customize dashboard items

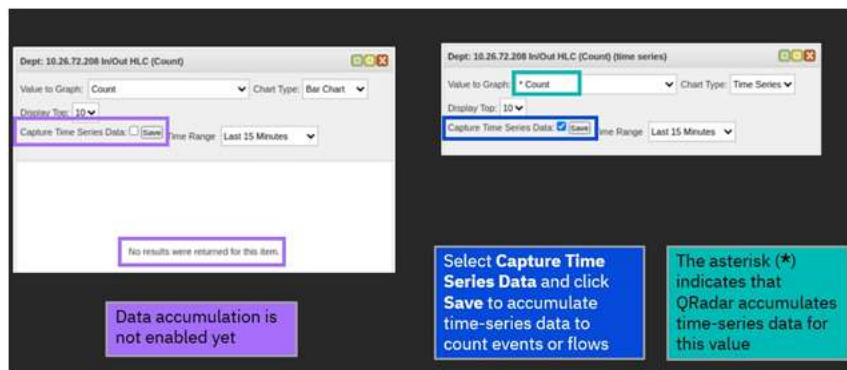
In this topic, we will learn how to use QRadar's Customized Dashboard items to get more advanced reporting functions.

Enabling time-series data

Capturing time-series data means that QRadar SIEM counts incoming events or flows according to your search criteria, grouping, and chosen value to graph.

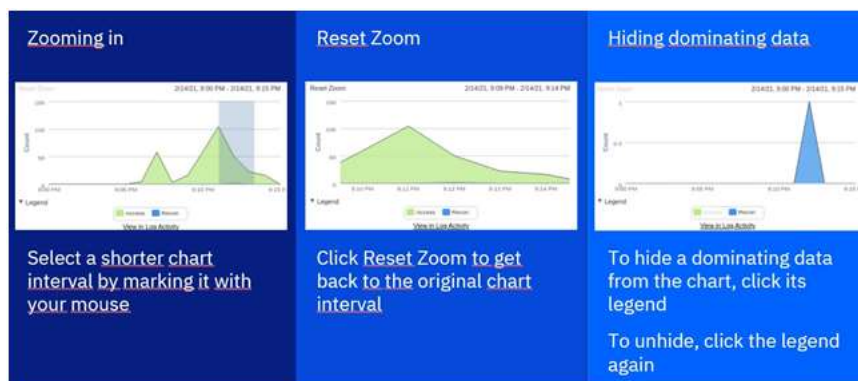
Most of the predefined searches capture time-series data. When you create dashboard items based on your own saved searches, the data accumulation might not be enabled yet.

Capturing time-series data increases resource consumption of QRadar.



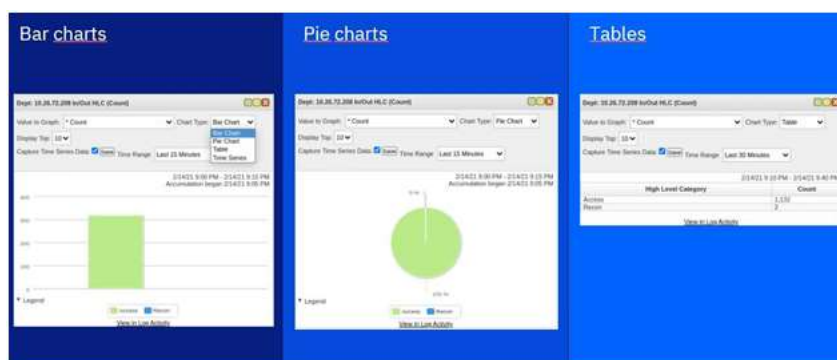
User permissions control the ability to configure and view time-series data.

Investigating data trends in time-series charts



Select other chart types to display

In addition to time-series charts, you can display data as a bar chart, pie chart, or a table.



4. SIEM Reports

SIEM Reports

Bookmark this page

SIEM Reports

Reports condense data to statistical views on your environment for various purposes, in particular, to meet compliance requirements. QRadar SIEM and extensions provide many templates you can use to generate reports

Reporting introduction

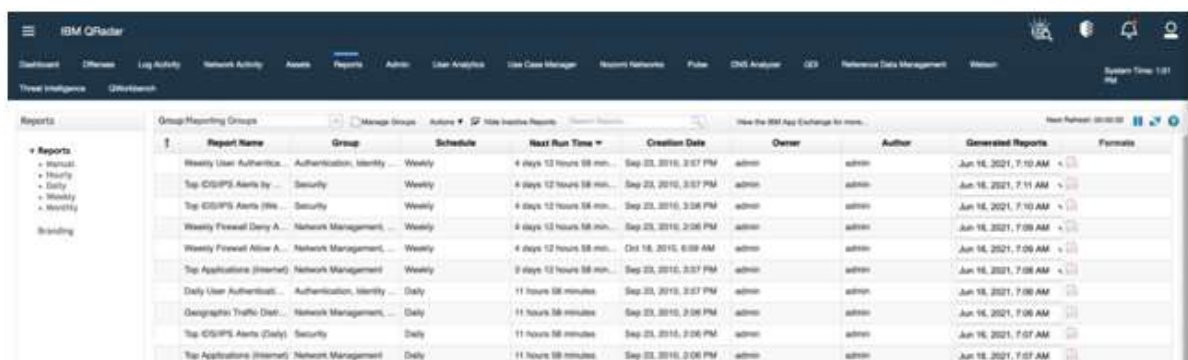
- A QRadar SIEM report is a means of scheduling and automating one or more saved searches
- QRadar SIEM reports perform the following tasks

- o Present measurements and statistics
- o Provide users the ability to create custom reports
- o Can brand reports and distribute them
- o Predefined report templates serve a multitude of purposes, such as the following examples
 - o Regulatory compliance
 - o Authentication activity
 - o Operational status
 - o Network status
 - o Executive summaries

QRadar SIEM administrators can install extensions to add report templates for the following regulatory schemas:

- o HIPAA: Health Insurance Portability and Accountability Act
- o COBIT: Control Objectives for Information and Related Technology
- o SOX: Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act
- o PCI: Visa Payment Card Industry Data Security Standard
- o GLBA: Gramm-Leach-Bliley Privacy Act
- o FISMA: Federal Information Security Management Act
- o NERC: The North American Electric Reliability Council
- o GSX: Government Secure Extranet

You can search and sort report templates in a similar way as events and flows



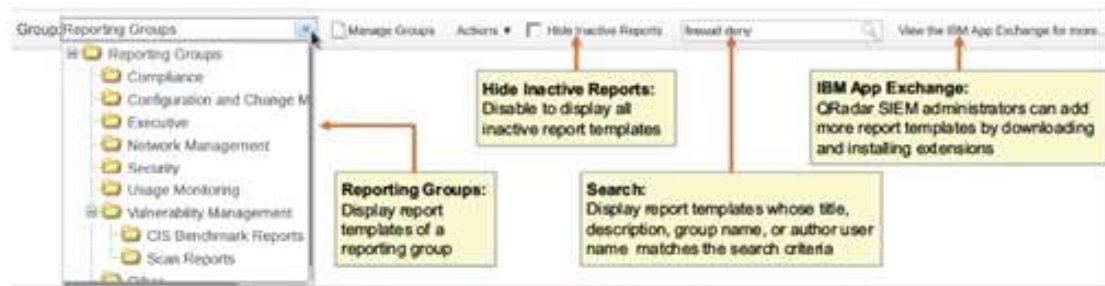
The screenshot shows the IBM QRadar Reports page. The top navigation bar includes links for Dashboard, Offense, Log Activity, Network Activity, Assets, Reports, Admin, User Analysis, Case Case Manager, Recent Networks, Pulse, DNS Analysis, IDS, Reference Data Management, and Release. The Reports page has a sidebar with 'Reports' and 'Branding' sections. The main content area displays a table of report templates with columns for Report Name, Group, Schedule, Next Run Time, Creation Date, Owner, Author, Generated Reports, and Formats. The table lists various reports such as 'Weekly User Authentication', 'Top IDS/IPS Alerts by...', 'Weekly Firewall Deny A...', 'Weekly Firewall Allow A...', 'Top Applications (Internet)', 'Daily User Authentication', 'Geographic Traffic Dist...', 'Top IDS/IPS Alerts (Daily)', and 'Top Applications (Internet)'.

Report Name	Group	Schedule	Next Run Time	Creation Date	Owner	Author	Generated Reports	Formats
Weekly User Authentication...	Authentication, Identity	Weekly	4 days 12 hours 58 min.	Sep 23, 2016, 2:57 PM	admin	admin	Jun 16, 2021, 7:10 AM	
Top IDS/IPS Alerts by...	Security	Weekly	4 days 12 hours 58 min.	Sep 23, 2016, 2:57 PM	admin	admin	Jun 16, 2021, 7:11 AM	
Top IDS/IPS Alerts (We...	Security	Weekly	4 days 12 hours 58 min.	Sep 23, 2016, 2:58 PM	admin	admin	Jun 16, 2021, 7:10 AM	
Weekly Firewall Deny A...	Network Management	Weekly	4 days 12 hours 58 min.	Sep 23, 2016, 2:58 PM	admin	admin	Jun 16, 2021, 7:09 AM	
Weekly Firewall Allow A...	Network Management	Weekly	4 days 12 hours 58 min.	Oct 16, 2016, 6:09 AM	admin	admin	Jun 16, 2021, 7:09 AM	
Top Applications (Internet)	Network Management	Weekly	9 days 12 hours 58 min.	Sep 23, 2016, 2:57 PM	admin	admin	Jun 16, 2021, 7:08 AM	
Daily User Authentication...	Authentication, Identity	Daily	11 hours 58 minutes	Sep 23, 2016, 2:57 PM	admin	admin	Jun 16, 2021, 7:08 AM	
Geographic Traffic Dist...	Network Management	Daily	11 hours 58 minutes	Sep 23, 2016, 2:58 PM	admin	admin	Jun 16, 2021, 7:08 AM	
Top IDS/IPS Alerts (Daily)	Security	Daily	11 hours 58 minutes	Sep 23, 2016, 2:58 PM	admin	admin	Jun 16, 2021, 7:07 AM	
Top Applications (Internet)	Network Management	Daily	11 hours 58 minutes	Sep 23, 2016, 2:58 PM	admin	admin	Jun 16, 2021, 7:07 AM	

QRadar SIEM administrators can select Branding on the left side to upload logos for your reports. Once a logo is uploaded, users can use the logo when creating or editing report templates.

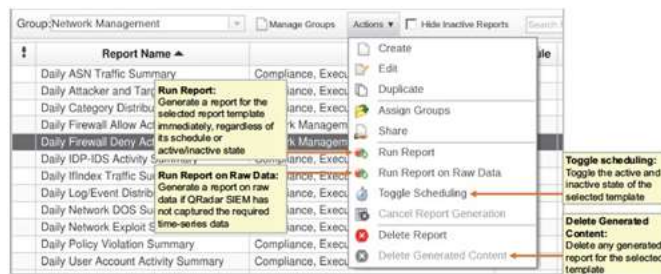
Finding a report

- QRadar SIEM and extensions provide many report templates
 - Before you create a new template, check the installed templates and the templates provided by extensions available on the IBM App Exchange



- Inactive reports: QRadar SIEM does not automatically generate reports for inactive templates.
- Active reports: QRadar SIEM generates reports for active templates automatically according to the schedule, unless the schedule is set to Manual. QRadar SIEM lists active templates with a manual schedule if the Hide Inactive Reports check box is enabled.

Running a report



- Exclamation mark:

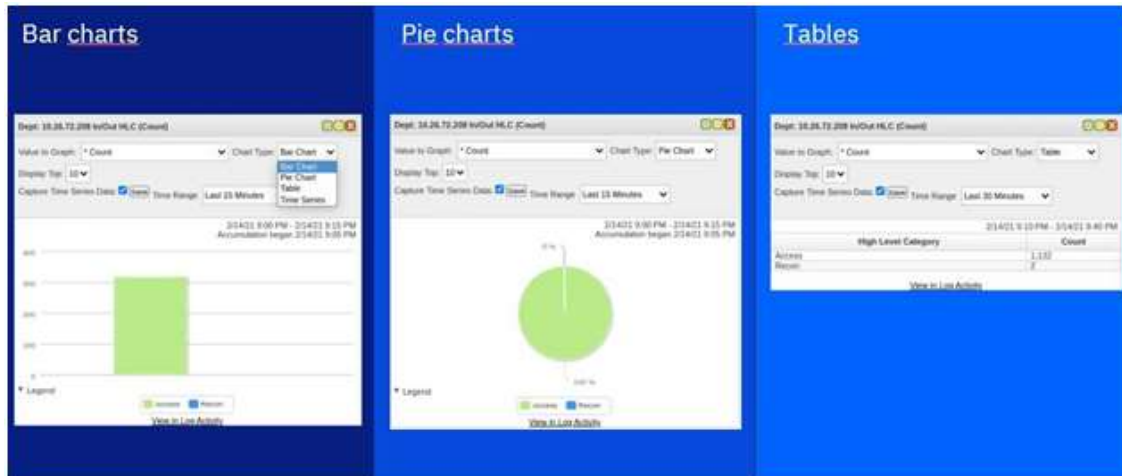
The leftmost column with the exclamation mark includes an error icon when a report fails to generate

- Run Report:

Initiate the generation of a report for the selected template. The generation uses accumulated time series data. If no accumulated data is available when the report runs, the generated report displays the message that accumulated data is not available. Refer to the next lesson to learn more about time series data for report generation.

- Run Report on Raw Data:

You can choose this option if QRadar SIEM has not accumulated time series data for your required reporting period. When a report runs on raw data, QRadar SIEM queries the data in its data store to generate the report. Running a report on raw data takes a longer time to process than running a report on accumulated time series data.



Selecting the generated report

Schedule	Next Run Time	Creation Date ▲	Owner	Author	Generated Reports	Formats
Weekly	5 days 9 hours 35 minutes	Sep 23, ...	admin	admin	None	
Daily	Generating (34 sec(s))	Sep 23, ...	admin	admin	None	

Estimated 34 seconds until the report is generated

Schedule	Next Run Time	Creation Date ▲	Owner	Author	Generated Reports	Formats
Weekly	5 days 9 hours 31 minutes	Sep 23, ...	admin	admin	None	
Daily	10 hours 31 minutes	Sep 23, ...	admin	admin	Aug 28, 2017, 2:25 PM	

Select a generated report from the list and click the PDF icon to view it

QRadar SIEM generates reports one at a time. When you start a report generation while another report is already generating, your report displays **Queued** in the Next Run Time column.

5. Applying filters

Applying filters

Bookmark this page

Applying filters

Filters limit a search result to the data that meets the conditions of the applied filters. Use filters to look for specific activities or to view your environment from various angles. QRadar SIEM provides filters so that you can focus on specific data

Filters introduction

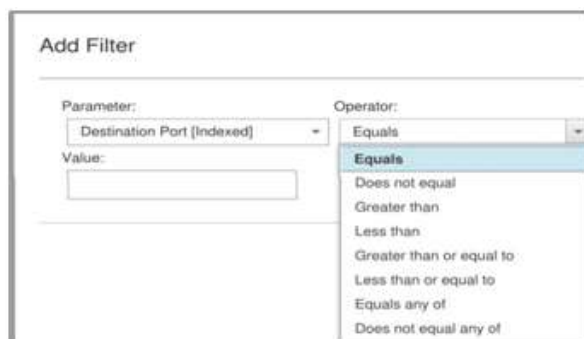
- Filters are a search criteria
- Use filters to look for specific activities and narrow down search results
- Right-click a property value in a list of events or flows to open a menu with a few filter options To use other filters, click the **Add Filter** icon



- A wide variety of parameters is available for filtering. Previous course modules have already introduced the following parameters
 - o Source and Destination IP addresses
 - o Source and Destination port numbers
 - o Event and Flow Direction
 - o Rules and building blocks that have fired
 - o Groups and network objects as defined in the Network Hierarchy
- Navigate the Log Activity and Network Activity tabs

Operators

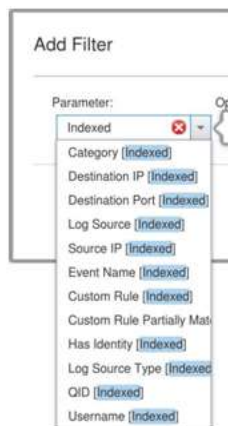
- A wide variety of operators is available for filtering
- The nature of the parameters determines which kind of operators are available



- To build an OR expression, use **Equals any of**.

Indexes

- [Indexed] behind a property in the Parameter drop-down list indicates that QRadar SIEM maintains an index for values of the property
- An index on a filtered property significantly reduces the run-time of a search.
- If you use a property without index in a filter, add additional filters with indexed properties to lower the number of events or flows that QRadar SIEM needs to search



Source and Destination IP

The very often used Source or Destination IP filter is not appended with [Indexed] although it uses the indexes of Source IP and Destination IP

Event Name	Log Source	Event Count	Time ▼	Low Level Category	Source IP
Firewall Deny	Check Point @ FW-1Machine	1	May 31, ...	Firewall Deny	10.127.15.37
Firewall Deny	Check Point	Filter on Source IP is 10.127.15.37			127.15.37
Firewall Deny	Check Point	Filter on Source IP is not 10.127.15.37			127.15.37
Firewall Deny	Check Point	Filter on Source or Destination IP is 10.127.15.37			127.15.37

Instead of an IP address, you can enter a range of IP addresses, in CIDR notation, such as 10.100.0.0/16.

6. Filtering events and flows

- Filtering events and flows

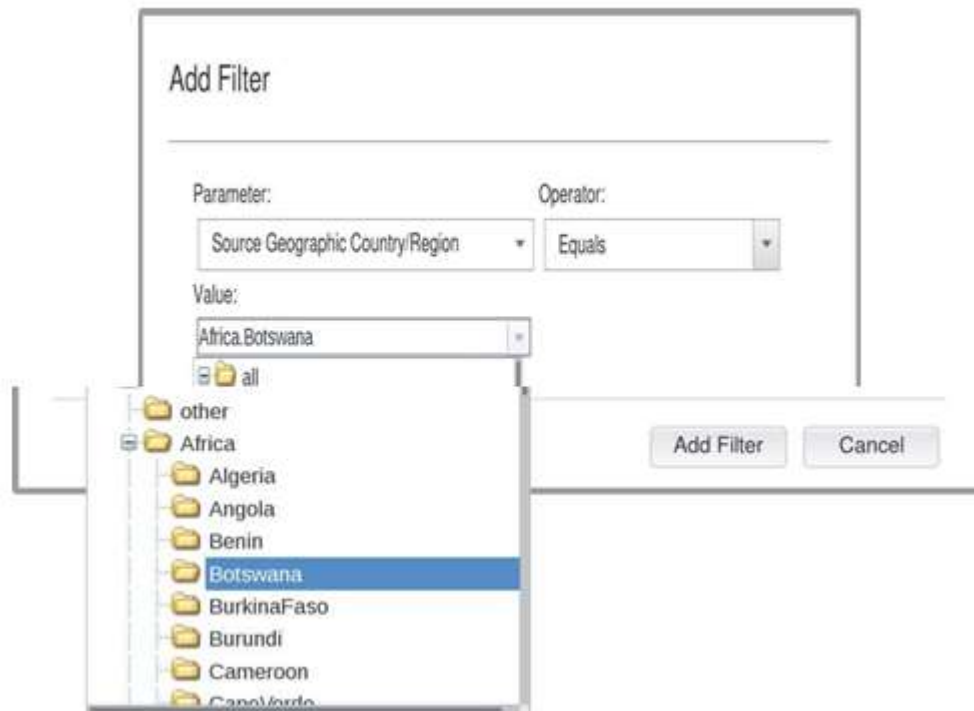
Filtering events and flows

Use filters to focus only on data relevant for a purpose

- Continents, countries, and regions

Continents, countries, and regions

Use filters for events or flows to include or exclude traffic from or to IP addresses located in the selected continents, countries, or regions.



- Associated With Offense

Associated With Offense

Use the Associated With Offense filter to include or exclude events or flows that QRadar SIEM added to one or more offenses.



- Payload Matches Regular Expression

Payload Matches Regular Expression

- When applying a regular expression (regex) to the payload of events, QRadar SIEM tests the raw events from which the event collector created the normalized events
- When applying a regex to the payload of flows, QRadar SIEM tests the captured layer 7 content sent by the source or destination socket
- Performing a regex on payloads consumes more computational resources than any other filter
 - With a regex filter, do not select real time or last interval viewing of log activity or network activity
 - The Log Activity and Network Activity tabs always display the result of a search; if you add a filter, QRadar SIEM performs the test of the filter only to this search result

The screenshot shows a dialog box titled "Add Filter". It contains a "Parameter" field with the text "Source Payload Matches Regular Expression", an "Operator" field with the text "is", and a "Value" field with the text "Referrer: http://ben.*". At the bottom right, there are two buttons: "Add Filter" and "Cancel".

- Payload Contains

Bookmark this page

Payload Contains

- The only difference between Payload Matches Regular Expression filters and the Payload Contains filters is that the latter performs a substring test instead of a regular expression test
- Follow the same best practices as for regular expressions, because the substring operation is less expensive than regular expression matching but still consumes much more computational resources than other filters

Add Filter

Parameter: Destination Payload Contains Operator: is Value: torrent

Add Filter Cancel

- Event Processor

Bookmark this page

Event Processor

- The appliances that store events and flows perform searches and transfer the result to the Console appliance
- If you know which appliances store the relevant events and flows, add a filter on these Event Processor appliances
- The Event Processor parameter is not only available for events but also for flows because the event and flow processor functionality is provided by the same software component

Add Filter

Parameter: Event Processor Operator: Equals Value: vulntr

Add Filter Cancel

7. Filtering events

Filtering events

Use filters to focus only on data relevant for a purpose

Log Source

Use the log source filter to include or exclude events from a specific service

Add Filter

Parameter: Operator:

Value:

Log Source Group:

Log Source Filter:

Log Source:

- JuniperMXSeries @ 10.0.216.22
- JuniperMXSeries @ 10.0.216.88
- LinuxServer @ 10.0.216.112
- LinuxServer @ 10.0.216.113
- LinuxServer @ 10.0.216.114

- Use the log source filter with the Does not equal any of operator to exclude events from the selected log sources

Viewing real time events View: Display:

Current Filters:

Log Source is not any of [Asset Profiler-2 :: vulmgr or Health Metrics... [\(Clear Filter\)](#)

Log Source is not any of [Asset Profiler-2 :: vulmgr or Health Metrics-2 :: vulmgr or SIM Audit-2 :: vulmgr or Search Results-2 :: vulmgr or System Notification-2 :: vulmgr]

Event Name	Log Source	Event Count
------------	------------	-------------

- For example, you can exclude the log sources that Qradar SIEM uses for its own services

Add Filter

Parameter: Operator:

Value:

Log Source Group:

Log Source Filter:

Log Source:

- Anomaly Detection Engine-2 :: vulmgr
- Asset Profiler-2 :: vulmgr
- Custom Rule Engine-8 :: vulmgr
- Health Metrics-2 :: vulmgr
- SIM Audit-2 :: vulmgr

Log Source is not Asset Profiler-2 :: vulmgr
Log Source is not Health Metrics-2 :: vulmgr
Log Source is not SIM Audit-2 :: vulmgr
Log Source is not Search Results-2 :: vulmgr
Log Source is not System Notification-2 :: vulmgr

Log Source Type:

Use the log source type filter to include or exclude events from services of the selected type

The screenshot shows the 'Add Filter' dialog box. The 'Parameter' dropdown is set to 'Log Source Type (Indexed)'. The 'Operator' dropdown is set to 'Equals'. The 'Value' dropdown is open, showing a list of log source types. The first two items, '3Com 8800 Series Switch' and '3Com 8800 Series Switch', are highlighted in blue. A 'Cancel' button is visible on the right side of the dialog.

Parameter	Operator	Value
Log Source Type (Indexed)	Equals	3Com 8800 Series Switch

Cancel

Event Is Unparsed

- Use the Event Is Unparsed filter to include or exclude events that event collectors linked to a generic log source
- Event collectors link events to a generic log source when they cannot automatically discover the kind of software or device sending the raw events, and no log source type has been configured manually by a QRadar administrator

The screenshot shows the 'Add Filter' dialog box. The 'Parameter' dropdown is set to 'Event Is Unparsed'. The 'Operator' dropdown is set to 'Equals'. The 'Value' dropdown is open, showing a list of values: 'True' and 'False'. The 'True' value is highlighted in blue. 'Add Filter' and 'Cancel' buttons are visible at the bottom right of the dialog.

Parameter	Operator	Value
Event Is Unparsed	Equals	True

Add Filter Cancel

AccountID Custom Event Property

- Custom event and flow properties can be used as filters
- Extensions and QRadar administrators can add custom event and flow properties in order to parse information specific to certain kinds of software or devices, for example, the HTTP version from web servers

The screenshot shows a dialog box titled "Add Filter". It contains three main sections: "Parameter:", "Operator:", and "Value:". The "Parameter:" dropdown is set to "AccountID (custom)". The "Operator:" dropdown is set to "Equals any of". The "Value:" field is empty, but a list of suggestions is shown below it: "AccountID (custom) is badguy" and "AccountID (custom) is intruder". A "Remove Selected" button is located below the suggestions. At the bottom right of the dialog are "Add Filter" and "Cancel" buttons.

Filtering flows

Flow Source and Flow Interface: Use the Flow Source and Flow Interface filter to include or exclude network activity captured by the selected flow sources or interfaces

The first screenshot shows the "Add Filter" dialog box with the "Parameter:" dropdown set to "Flow Source", the "Operator:" dropdown set to "Equals", and the "Value:" field set to "vulmgr".

The second screenshot shows the "Add Filter" dialog box with the "Parameter:" dropdown set to "Flow Interface", the "Operator:" dropdown set to "Equals", and the "Value:" field set to "vulmgr:ens32".

TCP Flags: Use the Source and Destination Flags filters to include or exclude flows with the selected TCP flags

The 'Add Filter' dialog shows the 'Parameter' set to 'Source Flags', the 'Operator' set to 'Equals', and the 'Value' set to 'F'. A dropdown menu is open for the 'Value' field, showing options: S, R, P, A, U, illegal/7, and illegal/8. 'Add Filter' and 'Cancel' buttons are visible.

DSCP: Use the Source and Destination DSCP filters to include or exclude flows with the selected Quality of Service precedence in IP headers

The 'Add Filter' dialog shows the 'Parameter' set to 'Source DSCP', the 'Operator' set to 'Equals', and the 'Value' set to 'Class 1 Low Drop'. A dropdown menu is open for the 'Value' field, showing various DSCP classes and drop types. 'Add Filter' and 'Cancel' buttons are visible.

ICMP Type/Code: Use the ICMP Type/Code filter to include or exclude flows with the selected ICMP Type and Code

The 'Add Filter' dialog shows the 'Parameter' set to 'ICMP Type/Code', the 'Operator' set to 'Equals', and the 'Value' set to 'ICMP Type: Redirect' and 'ICMP Code: Redirect Datagram for the Network (or subnet)'. A dropdown menu is open for the 'ICMP Type' field, showing various ICMP types. 'Add Filter' and 'Cancel' buttons are visible.

Data Loss: Combine filters to look for large amounts of data leaving your organization

The 'Viewing real time flows' interface shows a 'View' dropdown set to 'Select An Option' and a 'Display' dropdown set to 'Custom'. Below, the 'Current Filters' section shows two filters: 'Flow Direction is L2R' and 'Source Bytes is greater than 100,000'. 'Clear Filter' links are provided for each filter.

Applications using a nonstandard port

- Combine filters to look for applications listening on non-standard ports
- Use a similar filter to look for non-web applications using the standard web ports 80 and 443

Viewing real time flows View: Display:

Current Filters:

Application is Web [\(Clear Filter\)](#), Destination Port is not any of [80 or 443] [\(Clear Filter\)](#)

Viewing real time flows View: Display:

Current Filters:

Application is Web [\(Clear Filter\)](#), Destination Port is not any of [80 or 443] [\(Clear Filter\)](#)







Glossary

[Bookmark this page](#)

Glossary

Selected terms used in the publication are defined below.

Baselining: Monitoring resources to determine typical utilization patterns so that significant deviations can be detected.

Computer Security Incident: See “incident.”

Computer Security Incident Response Team (CSIRT): A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Centre, Computer Incident Response Capability).

Event: Any observable occurrence in a network or system.

False Positive: An alert that incorrectly indicates that malicious activity is occurring.

Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Incident Handling: The mitigation of violations of security policies and recommended practices.

Incident Response: See “incident handling.”

Indicator: A sign that an incident may have occurred or may be currently occurring.

Intrusion Detection System (IDS): Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to only detect possible incidents.

Intrusion Prevention System (IPS): Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Malware: A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.

Precursor: A sign that an attacker may be preparing to cause an incident.

Profiling: Measuring the characteristics of expected activity so that changes to it can be more easily identified.

Signature: A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

Social Engineering: An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

Threat: The potential source of an adverse event.

Vulnerability: A weakness in a system, application, or network that is subject to exploitation or misuse.

Security Incident & Event Management: Also referred as SIEM tool. Security information and event management is a subsection within the field of computer security, where software products and services combine security information management and security event management. They provide real-time analysis of security alerts generated by applications and network hardware

Security Operations Centre: Also referred as SOC, A security operations centre 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.

Security Orchestrator, Automation & Response: SOAR (Security Orchestration, Automation and Response) is a solution stack of compatible software programs that allow an organization to collect data about security threats from multiple sources and respond to low-level security events without human assistance and helps in automation.

Conclusion

Bookmark this page

Conclusion

This will enable the participant with deep drive knowledge on Security Incident & Event Management Concepts using real-life examples and IBM Tools to demonstrate the capabilities along with next future technologies.

SIEM Tools ensure the right set of Monitoring & Reporting tools to help protect the Environment against the rapid raise in Cyber Security Attacks. Planning for Cyber Security Alerts to occur should be the mindset you have with your Organization. By being ready and preparing your Organization for these types of incidents, you will handle the disaster with less time spent and less money used. A great Incident Response plan will ensure the stakeholders confidence and will mitigate future disasters from happening.





☐☒☐☐☒☒☐☐☐















