

The IBM QRadar Security Intelligence Platform

Monitor, detect and investigate threats

Highlights

- Gain comprehensive visibility into on-premises and cloud environments
 - Identify and prioritize known and unknown threats with advanced analytics
 - Scale security monitoring, detection and investigation
-

Security analytics on the rise

The evolution of attack tactics coupled with poor threat visibility keeps defenders on their toes, especially when adversaries exploit users and use individually crafted, short-lived malware to establish their initial foothold. As a result, security analytics—which collects security data and transforms it into actionable threat insights—is becoming a priority for security teams. The ability to identify attacks quickly and accurately empowers security teams to respond before major damage is done. Accurate threat visibility has been a core capability of the IBM QRadar Security Intelligence Platform since its inception. The solution has been deployed by thousands of security teams around the world to automatically identify, scope and prioritize threats. This paper explains how IBM QRadar collects and analyzes data to help security teams better detect and manage threats.

Data as the foundation: Benefits and challenges

The first step in security analytics is collecting the right data. To gain visibility into the different pillars of enterprise IT environments, IBM QRadar ingests data from a broad set of information sources. Most of these data sources are readily available, and each offers unique insight. For instance:

- **Network data** produced by firewalls, gateways, routers or through sensors can deliver a broad view of communication flows inbound, outbound and within the enterprise environment. This data shows who is talking to whom, how and when. By additionally using deep packet inspection, security teams can gain deeper insight into the type of data being transferred, discover network session anomalies and detect data exfiltration behind covert channels such as DNS tunnels.
- **Endpoint data** is typically generated by operating systems and provides deep insights into individual system activity, processes, configuration changes, running applications and individual user interactions on a system. This information is excellent for monitoring, tracking and auditing system or user activity. It also allows security analysts to detect suspicious processes and execute deep forensics once a compromise has been discovered.
- **Cloud data** produced by IaaS or SaaS providers allows security and cloud teams to monitor and retain all activity across their cloud infrastructures. For example, AWS CloudTrail events can be used for governance, compliance and operational auditing. They can also be analyzed by a centralized security information and event management (SIEM) solution to detect risks and threats to cloud resources.
- **User and identity data** ingested from Active Directory, LDAP or other identity and access management (IAM) solutions provide a contextual understanding of the person or resource behind a logon ID.
- **Application data** can help expose fraud or advanced attacks by providing insights into what is happening on a system beyond access and authentication activity. When it comes to the cloud, application log data can be used to track the use of cloud services, detect unauthorized access or even identify potential configuration risks.
- **Security data** typically originates from specific security controls such as antivirus tools, vulnerability scanners, intrusion detection systems, malware sandboxing solutions or data loss prevention systems. Output from these systems informs the security team when specific security policies have been violated, potentially indicating a threat is eminent.
- **Threat intelligence**, often consumed by analysts through external feeds, offers insights into known threat actors, tactics, techniques and procedures (TTPs), malicious assets (IP, URL and FQDN) and even goals. These Indicators of Compromise (IOCs) help security analysts identify and understand their adversary so they can make more informed decisions and take quick, decisive action to better protect the organization.

While these data sources have the potential to provide unique views into the enterprise to surface specific security insights, they also come with a set of challenges:

- **Volume:** Even small environments with hundreds of users can create a lot of data. Once network and endpoint reporting gets fully turned on, the amount of data to be evaluated, stored and managed can quickly exceed megabytes of data per minute.

- **Data complexity:** The fact that each data source provides insights solely into its own IT function can make building full enterprise visibility a challenge. For instance, to understand who or what is behind network traffic, multiple forms of network activity data (flows, IPFix, packet information) first need to be collected from multiple places, parsed and enriched with system names or identity data to get a full picture. The process of ingesting, parsing and correlating different data formats in a timely manner can pose a major challenge for defenders.
- **Missing business context:** Behind each log entry or network session is a system, service or user with a specific role or function within the organization. This information is important to understand the business criticality of events and to discover potential insider threats, such as users accessing sensitive data outside their department. Unfortunately, business context data is not always easily accessible, may be distributed over various sources or may be buried in undocumented institutional knowledge.
- **Lack of analytics processes:** Security analytics requires a process to discover potential threats and prove or disprove their credibility. Not all organizations have the defined and automated steps needed to sort through large volumes of complex data, so they instead rely on manual processes. This leaves advanced security analytics anchored around a few individuals who have both the time and knowledge to cross-correlate the data. As a result, time-pressured users, such as first-line responders, or users with fewer data insights may be unaware of what is really happening.
- **Adversaries living off the land:** Attackers are continuously changing their tactics, exploiting users and crafting short-lived weaponized tools to evade prevention and detection mechanisms. Once inside, attackers hide behind authorized users and systems as they advance toward their end goal of data exfiltration, data alteration and/or system destruction. Traditional signatures and heuristic-based detection are often ineffective at detecting sophisticated attacks. More advanced analytics, such as behavioral monitoring, are required to identify the symptoms of a hidden attacker.

Given these challenges, it becomes clear that security analytics are not individual stand-alone elements, such as known threat detection, pattern matching or machine learning elements. Instead they need to be combined to form a set of overlapping processes capable of quickly analyzing high volumes of data and producing insightful findings that can be cross-correlated to quickly and accurately detect known and unknown threat activity.

QRadar integrated analytics processes

The IBM QRadar Security Intelligence Platform offers automated analytics for detection and investigation, as well as search-based threat hunting tools that are designed to analyze and sort through a broad array of logs, events and network flows.

Processing of the data can be classified into three integrated analytics groups:

- Monitoring
- Detection
- Investigation

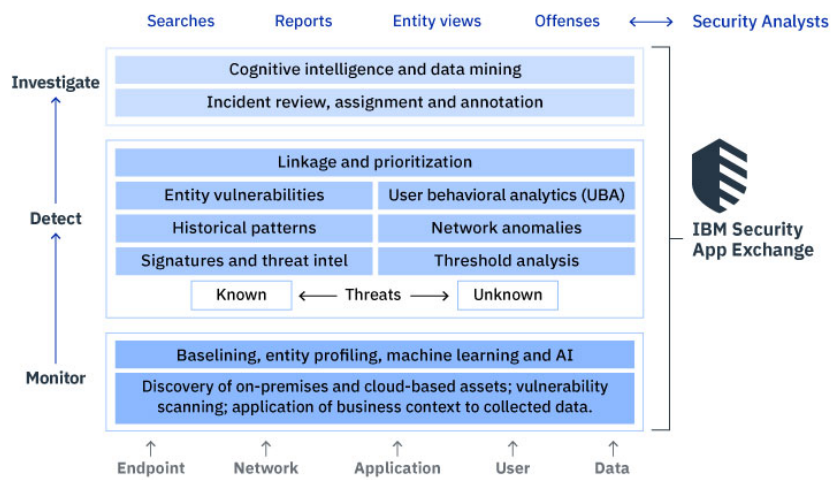


Figure 1: IBM QRadar analytics components enable security analysts to monitor, detect and investigate known and unknown threats.

Monitoring

Monitoring provides insights into who is on the network, what is happening and the presence of potential risks. Analysts typically have limited visibility into assets or users on their network, as changes continuously occur. By looking at the various sources of machine data and network traffic flows, IBM QRadar automatically takes an inventory of assets. The platform can discover applications, protocols, services or ports in use by those assets. This analysis provides insight into the asset type, network location and baseline configuration, helping analysts define critical assets without requiring manual uploads of the network topology or asset inventory. Additionally, through an integrated vulnerability manager with optional automated scanning, IBM QRadar can reveal vulnerabilities along with their severity levels to help prioritize patching efforts. Lastly, IBM QRadar includes a set of anomaly detection and machine learning algorithms to profile and establish a known baseline of network and user activity.



Figure 2: The IBM QRadar Pulse app provides dynamic dashboards to help teams visualize offenses, network data, threats, and malicious user behavior throughout the environment.

Detection

IBM QRadar is designed to correlate activity across the entire network and apply a spectrum of signature-based and behavioral-based detection methods to identify both known and unknown threats.

Unique IBM QRadar detection capabilities include:

- **Real-time and historical threat detection** based on rules, IOCs and pattern-matching to find known and emerging threats
- **Deviation from normal behavior** at both the network and user levels to identify suspicious activities. Anomaly-based detection is especially useful to surface unknown—hidden threats for which no known signatures or IOCs exist
- **Advanced network analysis** to sense a change in network traffic, such as the appearance of a new host or abnormal communications between existing hosts
- **Risk-based detection and prioritization** that uses advanced event analysis and correlation between assets, users, network activity, vulnerabilities and threat intelligence to understand the severity of the threat and automatically prioritize it based on potential business impact

Unique to the IBM QRadar detection process is its ability to link related events into a single “Offense.” This event chaining process helps reduce the total number of alerts generated. Because all information is available on one screen, the user can immediately see an overview of all related suspicious activity that has been detected. As new events occur, the original Offense is automatically updated with the new data so that analysts do not have to flip between multiple alerts.

IBM QRadar automatically prioritizes Offenses based on relevance, credibility and severity:

- **Relevance** determines the impact of the Offense on your network. For example, if a network port is open, the relevance is high.
- **Credibility** indicates the integrity of the Offense as determined by the credibility rating configured in the log source. Credibility increases as multiple log sources report the same event.
- **Severity** indicates the level of threat that a source poses in relation to how vulnerable the destination is for the attack.

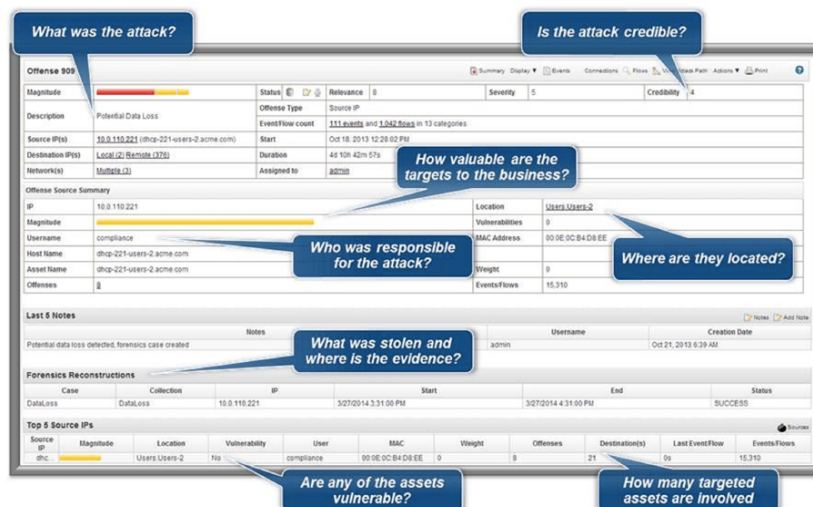


Figure 3: The Offenses screen within QRadar provides actionable insight into potential incidents so that analysts can quickly and easily understand each threat.

Combined, these measurements translate into a magnitude score, which is a risk score that helps analysts easily understand which Offenses should be reviewed first. Magnitude is calculated for each Offense. As new events are added to an Offense, the magnitude score automatically adjusts.

Investigation

The third component of the IBM QRadar analytics process is the automated investigation of observables within an Offense to help analysts make faster, more informed decisions about what to do next.

When using IBM QRadar Advisor with Watson, analysts can optionally forward Offenses to IBM QRadar Advisor for initial investigation. IBM QRadar Advisor collects external observables within the Offense—such as IP addresses, URLs and file hashes—and sends them to the Watson for Cybersecurity cloud for analysis. Watson for Cybersecurity uses cognitive intelligence to research observables and return new insights—such as related IOCs, details on the likely threat actor, and insight into the threat campaign. IBM QRadar Advisor can then use that new information to identify the root cause of the threat, search for the related IOCs in the environment and visually display the true scope of the threat.

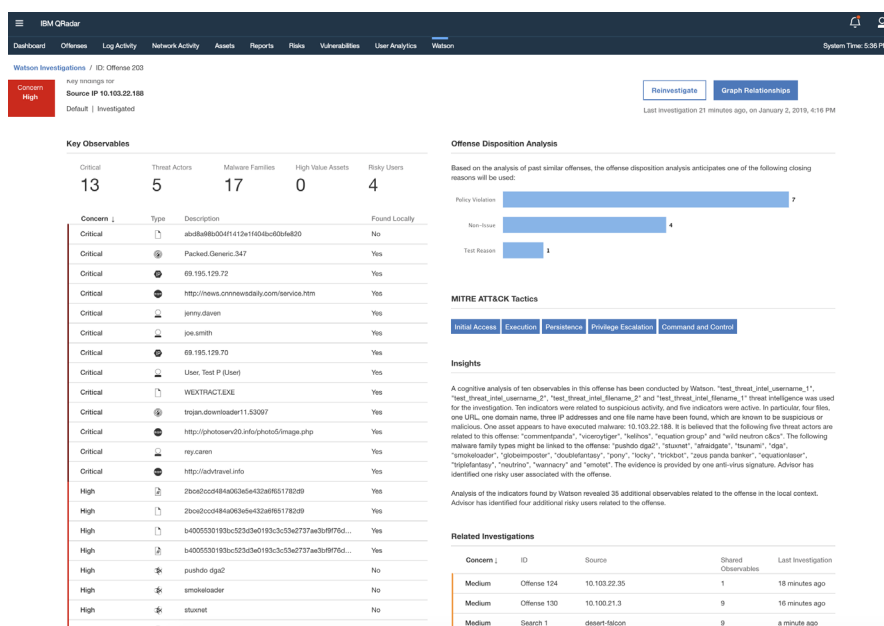


Figure 4: IBM QRadar Advisor with Watson aggregates all observables and automates offense analysis using MITRE ATTACK.

IBM QRadar offers several distinct investigative benefits to the user:

- **Prioritized, actionable offenses:** By grouping and prioritizing all related events under a single Offense, the user gets a full view of a potentially evolving attack scenario. This allows analysts to focus their attention on the highest priority threats while reducing the amount of time lost on low priority events. In addition, analysts can add annotations or assign Offenses to specific

users to streamline the investigation processes.

- **Cognitive insights:** IBM QRadar Advisor with Watson provides a combination of cognitive insights and local data mining designed to uncover related IOCs. This helps security analysts quickly gain deeper insights into Offenses to make more informed, faster triage decisions.

The IBM QRadar Security Intelligence Platform offers a wealth of out-of-the-box integrations, analytics and correlation rules to help customers turn machine data into actionable insights without first requiring significant customization. While these built-in analytics are automated and usable out-of-the-box, advanced users may want to customize log enrichment policies, rules or machine learning algorithms. The flexible platform supports as much or as little customization as preferred, and it offers quick search and advanced search functionality so users can proactively hunt threats.

IBM Security App Exchange: An open platform

IBM QRadar offers hundreds of validated apps through the IBM Security App Exchange to help you extract greater value from your solutions. Using validated apps, administrators can extend and enhance their IBM QRadar deployment with new data sources and ready-to-use rules, reports and dashboards to support new use cases. Apps can easily be downloaded and added into existing QRadar deployments without requiring costly upgrades or interrupting functionality.

Advanced IBM QRadar users can optionally build their own integrations with open APIs or create their own apps using the Software Development Kit (SDK). New apps can be packaged and shared with other IBM QRadar customers through the IBM Security App Exchange.

Use cases powered by security analytics

In many environments, increasing complexity makes it difficult to identify risks, and as a result, critical assets aren't necessarily as secure as they can—or should—be. To effectively mitigate risks, organizations need solutions that provide visibility and insights into the complete environment without any blind spots. From the moment it's installed, IBM QRadar begins collecting data and building actionable security intelligence that can help organization address their most important security use cases.

Advanced threat detection

Using real-time analytics, security teams can detect if a host visits a potentially malicious domain, but an alert might not be required for just a visit. However, if that same host starts demonstrating beaconing behavior—detected by using historical long-term analysis—and it also starts transferring abnormally high data volumes, deviating from behavioral baselines, the combination of all three conditions allows IBM QRadar to produce a single, heightened alert.

IBM QRadar can also detect a sudden change in network traffic, such as the appearance of a new application on a host or the termination of a typical service, capturing it as an anomaly. Unlike malware signatures or other known vulnerabilities, anomalies are not easily spotted by security teams when they search through system logs. By definition, an anomaly is an oddity, and is only discoverable by a security solution that monitors and profiles the actions of all users and entities.

Critical data protection

Overnight, a new application begins operating on a network host. This activity might be the result of a new business requirement or someone simply installing a chat application. But if that host has access to critical data, starts sharing confidential data, and also has a known vulnerability associated with it, IBM QRadar can create a high-priority alert to prompt security teams to investigate the incident.

IBM QRadar Network Insights can detect and analyze network traffic patterns, and it can look inside the traffic to check for personal information, confidential data, scripts or redirects. For example, when a device starts sending or receiving critical data or when traffic exceeds a certain threshold, an event and subsequent Offense can be generated.

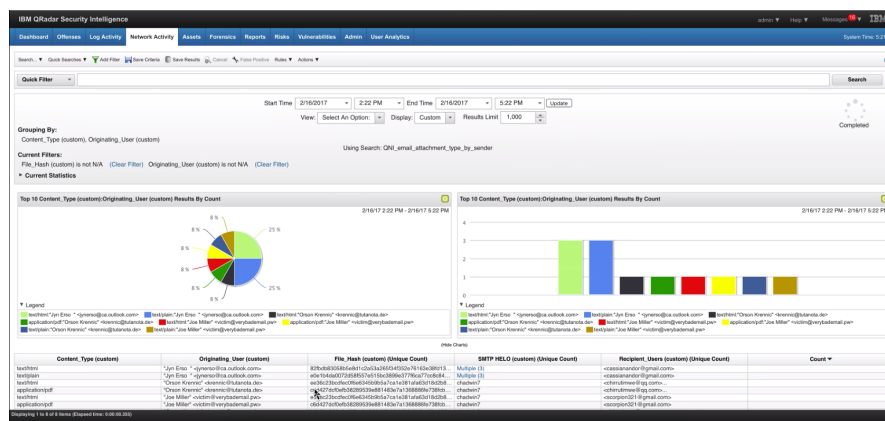


Figure 5: IBM QRadar Network Insights provides visibility into network level activity, such as which users received phishing emails and what content was included in those emails.

Threshold policies can be set based on any data collected by IBM QRadar, such as network device configurations, servers, network traffic telemetry, applications, and users and their activities. IBM QRadar can enrich an event or Offense with the context of user identities, ports and protocols in use, IP reputations and reported threat activities. This provides security teams with a deeper perspective about the incident.

Insider threat monitoring

A customer service representative suddenly begins downloading twice the normal amount of data from a client information system, which might be part of some new sales analysis activity. But if QRadar identified that the representative recently visited a suspicious website and now small amounts of data are being sent to a competitor's site, the security staff can be informed before a large amount of information is leaked.

By profiling entities and individuals, IBM QRadar stands out from other security products. The combination of a comprehensive set of data, business context and threat intelligence—coupled with the ability to detect deviations from normal behavior and unauthorized activity—provides for a powerful incident detection capability.

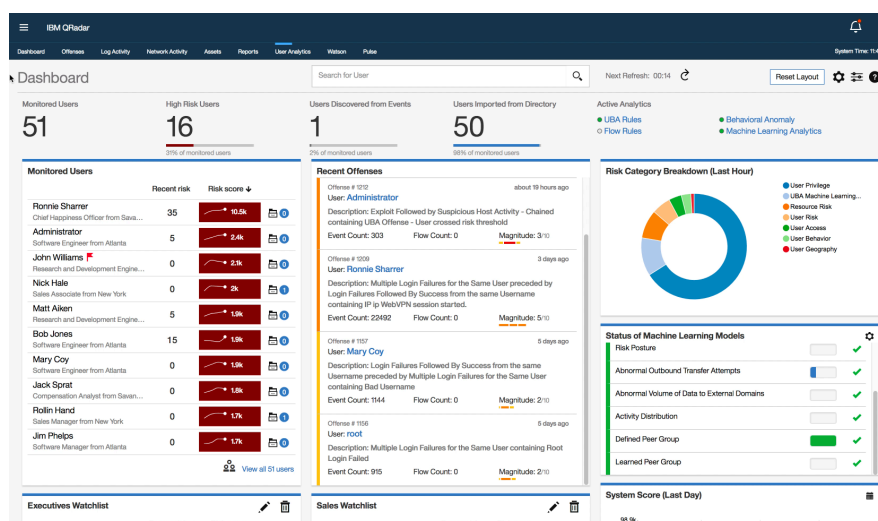


Figure 6: QRadar User Behavior Analytics profiles user activity, assigns risk scores and shows which users have been involved in which offenses.

Threat hunting for low and slow attacks

Once inside the network, threat actors attempt to quietly and slowly extract data behind covert channels. This tactic can be very hard to detect, as the amount of data needed to identify these small events may be extremely high and no external threat intelligence may exist.

Users can hunt for these hard-to-find attacks by starting with an abnormal endpoint, user or network activity and then pivoting into other activity, such as configuration changes, abnormal connections to associated assets, or data transfers either within the network or to external systems.

This process of adding, pivoting and searching for anomalies is supported by Ariel Query Language (AQL). AQL provides a set of commands to retrieve, compare, group and order query data, as well as hunt for additional event activity to surface a potential threat. For example, by filtering out high-risk users, pivoting to related contacted assets, and then comparing this against network traffic anomalies, a list of potentially compromised systems can be identified.

Cloud visibility and monitoring

Organizations of all sizes are adopting multi-cloud strategies to streamline costs and reduce vendor lock-in. While this approach has clear business benefits, it can also generate new blind spots for security monitoring.

The IBM QRadar Cloud Visibility app allows security teams to centrally monitor activity in Amazon Web Services, Microsoft Azure and IBM Cloud environments. The app uses existing IBM QRadar integrations that collect log data from IaaS environments, and it uses rules from IBM QRadar's cloud content extensions, which are available in the IBM Security App Exchange. Using these data streams and security use cases, IBM QRadar can detect cloud misconfigurations—such as those common in AWS S3 buckets or Azure Blob storage—and identify threats within these environments.

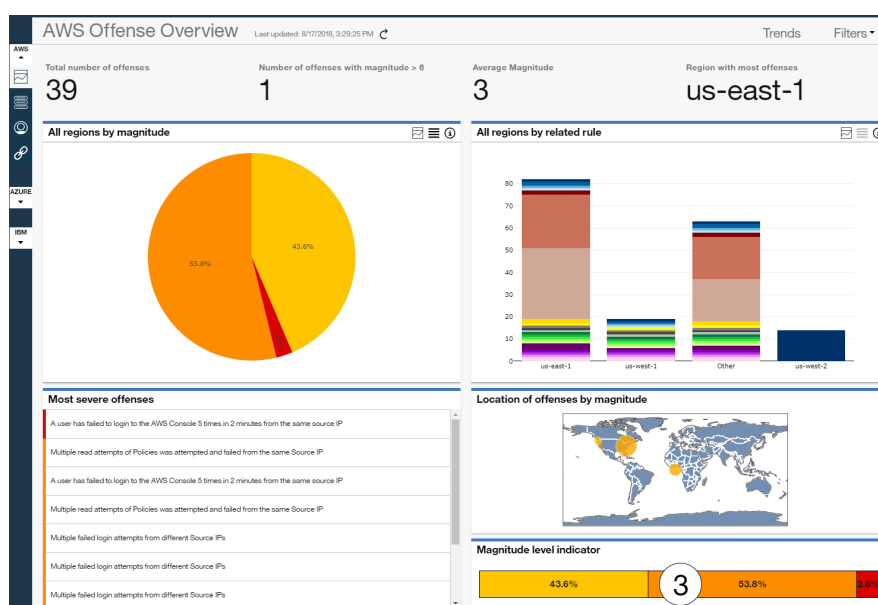


Figure 7: IBM QRadar Cloud Visibility app enables analysts to monitor, detect and visualize potential offenses in AWS, Microsoft Azure, and IBM Cloud.

Risk and vulnerability management

When a new entity appears on the network, IBM QRadar automatically detects its existence through passive profiling of log and flow data. With its integrated vulnerability scanner, IBM QRadar can trigger a scan of the new entity to discover if it has any urgent or high-risk vulnerabilities that are exposed to potential threat sources.

For example, when a new server is added to the network, IBM QRadar can detect if it is missing critical patches or has default administrative credentials. IBM QRadar can then notify the appropriate team to remediate and/or schedule a patch, and then escalate the issue if necessary.

New vulnerability disclosures are automatically correlated with existing data without needing a rescan, which helps improve the speed and accuracy of detection. The resulting operational savings also allows security analysts to spend more time focused on proactive tactics, such as risk analysis and vulnerability patching activities.

Users of security analytics

Security analytics help streamline the workflows of multiple users within a security operations team.

For first-line analysts: Reacting to and triaging alerts

Time is essential for first line analysts. For them, receiving a timely, accurate alert that includes the full context of the threat is necessary to make a quick but informed decision. For these users, IBM QRadar offers several important capabilities.

First, IBM QRadar's approach to Offenses provides analysts with a single-pane-of-glass view into all activity related to a given threat. From the Offense screen, analysts can see a summary description of the suspicious activity that led to the Offense, the users and systems involved in the Offense, and all events and flows that contributed to the Offense.

Second, automatic risk scoring and prioritization help analysts identify which Offenses to investigate first. Because Offenses are continuously updated with new events and flows, and the magnitude score is adjusted based on this new information, analysts can clearly see when low-priority Offenses suddenly become higher-priority.

Third, IBM QRadar Advisor with Watson can help analysts quickly understand the full context of an Offense so they can make better and faster triage decisions. The solution enriches known observables with related IOCs and provides a visual knowledge graph that shows the full scope of the threat in the environment. These enriched insights help reduce the time spent on investigations and empower analysts to make faster, more informed decisions.

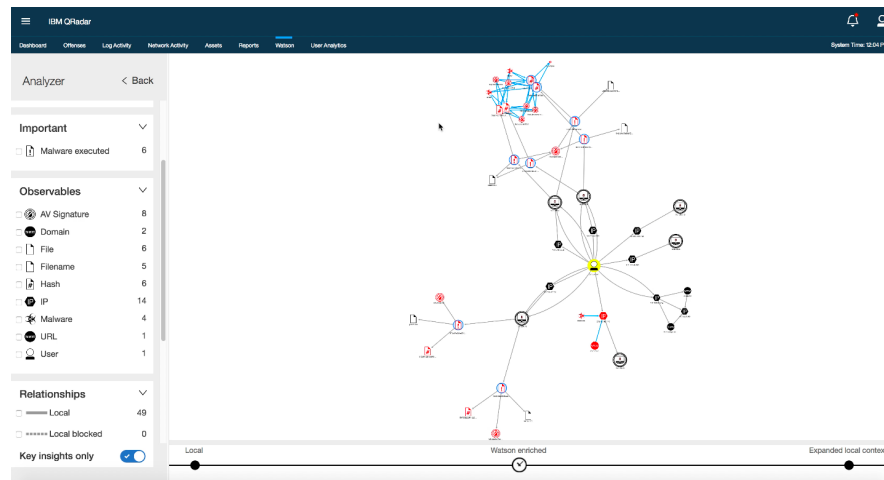


Figure 8: QRadar Advisor with Watson automatically creates a relationship graph that shows all observables related to an offense.

For investigators: Filtering and pivoting on suspicious activities

Investigators and advanced analysts often orient their searches around specific threats or risks, such as a suspicious user or asset, a known attack campaign or a calculated risk. Within IBM QRadar, users can create and run ad-hoc or scheduled AQL searches to look for suspicious behaviors. Search results can help analysts identify all users or systems impacted by a specific threat, and they can also be used to help show compliance with regulatory and audit requirements.

For example, a high-risk user has been identified by QRadar User Behavior Analytics. As a first step, the analyst can quickly search for the username and find all his logon/logoff activity to understand what the user accessed in the environment. By pivoting to the related systems, the analyst can now review all network protocols and filter for suspicious network connectivity, such as P2P traffic or abnormally high volumes of data transfers. Once a suspicious external host has been identified, the analyst can then verify which other internal systems have also connected to this suspicious host to gain a complete inventory of the systems potentially impacted by this event.

For deeper forensics investigations, IBM QRadar Incident Forensics can recover all network packets associated with an incident and reconstruct the step-by-step moves of an attacker. This provides investigators and responders with a crystal-clear picture of what malicious activity took place, where and when. Incident responders can view the infection paths and identify the root cause and other infected users or entities. They can also gain a complete forensic trail of what happened so they can take steps to prevent the incident from occurring again in the future.

For hunters: Searching for adversarial tactics

IBM QRadar offers a wide spectrum of behavioral and anomaly-based detection methods that can identify events that are common along the kill chain and provide unique starting points for threat hunting. Following are a few examples of activities that occur throughout the kill chain, can be detected by IBM QRadar and used by proactive threat hunters to uncover adversaries earlier in the attack cycle.

Suspicious processes: Using endpoint activity events, such as Sysmon events or data from EDR solutions, IBM QRadar can baseline endpoint configurations and processes to detect suspicious changes such as unusual or new processes, potential key loggers, malicious use of powershell or excessive use of system tools on a single machine.

Privilege escalation: IBM QRadar can detect if a command shell has been opened with escalated privileges. For example, if a regular user starts the command shell as a Windows System user, an event can be immediately generated.

Asset discovery: IBM QRadar continuously analyzes network data to detect new assets. It can automatically determine the new asset type based on attributes and behavior. Analysts can periodically review new assets to look for unexpected or suspicious systems.

Port scanning: IBM QRadar can track the normal number of connections between any given host and other systems on the network. An abnormally high number of connections or attempted connections may indicate a malicious port scan, which could be cause for further investigation into the host initiating the scan. Sanctioned vulnerability scanners can be added to known reference sets to eliminate noise caused by legitimate processes.

Lateral movement: Execution of remote commands from one endpoint to another may indicate an attempt of lateral movement. Using endpoint activity events and network flows, IBM QRadar can detect these attempts, even when the commands are encoded or obfuscated.

Data exfiltration: IBM QRadar Network Insights, which conducts full packet analysis and can provide insight into local DNS traffic, can be used to detect suspicious data within sessions, such as phishing emails that contain malware or the suspicious or unauthorized transfer of sensitive or private data.

The IBM QRadar Security Intelligence Platform

More than just a SIEM, the IBM QRadar Security Intelligence Platform offers organizations a broad set of automated and integrated security analytics, purpose-built to help eliminate blind spots and accelerate monitoring, detection and investigation workflows.

These pre-built analytics allow analysts across all tiers of security operations to gain the critical, actionable insights needed to speed up day-to-day processes, reduce the risks associated with extended dwell time, and improve the security posture of the organization. IBM QRadar comes with a wealth of hundreds of apps, content packs and integrations to help jumpstart a security analytics program.

Components of the IBM QRadar Security Intelligence Platform

IBM QRadar SIEM, at the core of the platform, helps security teams accurately detect and prioritize threats across the enterprise. It also helps provide intelligent insights that enable teams to respond quickly to reduce the impact of incidents.

IBM QRadar on Cloud is a SaaS offering that provides the benefits of IBM QRadar SIEM without requiring security teams to manage the underlying infrastructure of their SIEM solution. Analysts can focus on detecting, investigating and responding to threats without worrying about upgrades and maintenance.

IBM QRadar Advisor with Watson applies artificial intelligence to automatically investigate indicators of compromise, determine the root cause and scope of threats and accelerate the investigation cycle.

IBM QRadar User Behavior Analytics analyzes user activity to detect malicious insiders and determine if a user's credentials have been compromised. This solution is included in the IBM QRadar license and can be installed in minutes via IBM Security App Exchange.

IBM QRadar Network Insights analyzes network data in real-time to uncover an attacker's footprints and expose hidden security threats, often before they can damage your organization. The solution helps detect activities such as phishing e-mails, lateral movement and data exfiltration that may be missed when looking at logs alone.

IBM QRadar Vulnerability Manager identifies security vulnerabilities, adds context and helps prioritize remediation activities. Fully integrated with the IBM QRadar Security Intelligence Platform, it is designed to enrich the results of vulnerability scans to reduce risk and help organizations achieve compliance.

IBM QRadar Incident Forensics allows users to retrace the step-by-step actions of a potential attacker and quickly conduct an in-depth forensics investigation of suspected malicious network security incidents. The solution helps reduce the time needed to investigate Offenses, in many cases from days to hours—or even minutes.

IBM QRadar Data Store normalizes and stores both security and operational log data for future analysis and review. Users can optionally build custom apps and reports based on this data to gain deeper insights into the IT environment. The offering supports the storage of an unlimited number of logs without counting against the organization's Events Per Second (EPS) license.

Why IBM?

IBM Security offerings provide security intelligence to help organizations holistically protect customers, data, applications and infrastructure from security threats. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development organizations.

With IBM QRadar, you can gain comprehensive insights, quickly detect and prioritize potential threats, gain feedback to continuously improve detection, help address your security and regulatory risk, as well as report on compliance adherence.

For more information

To learn more about the IBM QRadar Security Intelligence Platform, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/qradar

January 2019

© Copyright IBM Corporation 2019.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at <https://www.ibm.com/legal/us/en/copytrade.shtml>, and select third party trademarks that might be referenced in this document is available at https://www.ibm.com/legal/us/en/copytrade.shtml#section_4.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:

QRadar®, Watson®



All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.