



Meeting Today's Complex Network Threats Head On

A white paper on the application of QRadar for
effective threat management

Overview

Over the past few years there has been a growing awareness in internet based threats that, if undetected, would have a significant negative impact the organization. This increased visibility has been driven through numerous embarrassing media stories where consumer data has been compromised and by numerous regulatory mandates that have emerged in the face of major corporate scandals. Compounding this problem further is a steady increase in insider theft of valuable corporate information by unscrupulous employees. To combat the broad spectrum of potential threats, organizations have invested heavily in targeted security solutions including firewalls, VPNs, intrusion detection and prevention systems, and vulnerability scanners. Unfortunately these solutions alone have not been able to completely protect organizations from the evolving landscape of threats. In recent years there has been a steady increase in the complexity of threats, including zero day attacks, worms and trojans, that span many systems and that are difficult to detect using existing point security solutions. In many cases companies are flying blind, in their ability to manage these threats, because they lack integrated visibility into the security solutions that are already in place. And, in the case of insider threats, companies lack the surveillance necessary to accurately pinpoint the actual individual or system that was responsible for malicious behavior. This white paper discusses in detail how QRadar, from Q1 Labs, provides an improved approach to threat management through the introduction of valuable and actionable surveillance that spans all facets of the enterprise IT environment.

The need for command and control

A major challenge for organizations, of all sizes, is how to extract useful information from the flood of network and security events that are generated on the network daily. Threats to an organization's information resources continue to evolve and become more sophisticated. Many of today's threats attempt to compromise confidential information for illegal financial reward and to utilize company computing resources to do harm to others. Many of threats may not be known to the existing security solutions and unfortunately go undetected resulting in immeasurable expense to the enterprise. Even when threats are detected by existing security solutions they may not be presented by the existing event monitoring and reporting solution because the events referencing the threat were not properly correlated and prioritized. Organizations are beginning to realize that they need centralized command and control that can more effectively manage the existing and emerging threats on their network that can be provided by an integrated network security management solution.

SIEM alone may not be enough

Many organizations have invested in a Security Information and Event Management (SIEM) solution to centralize their ability to monitor and correlate event signatures that are reported from the systems on the network. Although SIEM is a necessary tool for correlating network and security events, the jury is out on how well these solutions are working in practice to manage today's complex or insider perpetuated assaults. Inherent in traditional SIEM solutions is the ability to define rules that correlate a specific pattern of events. When rules have been properly written and tuned a SIEM solution can provide a valuable reduction in the number of items that are presented to a security specialist to address.

Unfortunately, this reduction is still leaves an overwhelming set of information to investigate for many reasons including:

- There is no context about the reliability of the alerts or prioritization based on the value of the targets
- The correlated results tell the security administrator that unusual activity is occurring, but lacks the ability to isolate the root cause.
- The information that is being correlated is tainted with misleading information, including false positives that are common amongst existing security solutions
- The SIEM solution lacks the ability to piece together information from all of the relevant data sources available, resulting in an inability to detect threats because of an incomplete picture of overall network behavior.

Organizations looking to improve their ability to improve overall security of information assets must look to a solution that has the ability to turn the flood of events and security focused management data into useful and relevant information for the network and security operation teams.

QRadar Network Security Management – Combining Silo'd Information

QRadar network security management platform, from Q1 Labs, takes an innovative approach to managing computer based threats in the enterprise. Recognizing that discrete analysis of security events is not enough to properly detect threats; QRadar was developed to provide an integrated approach to threat management that combines the use of traditionally silo'd information to more effectively detect and manage today's more complex "threats". Specific information silos that have been combined include:

Network events:

Includes events generated from networked resources including switches, routers, servers and desktops.

Security logs:

Includes log data generated from security devices like firewalls, VPNs, intrusion detection/prevention, anti-virus, identity management, and vulnerability scanners

Host and application logs:

Includes log data from industry leading host operating systems (Microsoft Windows, UNIX, and Linux) and from critical business applications (authentication, database, mail and web)

Network and application flow logs:

Includes flow data generated by networking devices from vendors including Cisco, Juniper, Foundry, HP, and Extreme. Information provides the ability to build a context of network and protocol activity.

User and asset identity information:

Includes information from commonly used directories including Active Directory and LDAP.

Many traditional SIEM solutions will only incorporate a subset of this information and typically lack the ability to leverage the valuable point of perspective that is provided by flow data, user and asset identity information. We cover many examples below where a combination of all of the aforementioned data sources is required to detect treats that will be missed by other solutions because they lack an integrated awareness of network, security, application, and user identity.

Detecting attacks other miss - zero day exploit

There are many threats on the network that are not yet known to existing security applications and can impact an organization at any time. These exploits leverage existing vulnerabilities to propagate harmful code.

Scenario: A user clicks on a link which takes them to a website. Embedded in this website is new malicious code that installs a backdoor onto the computer. The victim machine makes an IRC connection over a non-standard port in order to hide the connection from security devices. Once it connects to the IRC server it joins a channel and waits for a command to scan certain subnets for open mail servers (port 25) and return the results back to a chat room. Once the results have been returned, the attacker then sends a command to the back door telling it to send out mail to those hosts with open mail ports.

The firewall and IDS are effective at logging firewall accepts, some malformed headers and the scan for mail servers. QRadar correlation is required to tie these events together with the missing network behavior analysis that detects IRC on a non-standard channel (botnet) and the victim host sending mail. Without the additional application information provided by flow data this exploit would have gone undetected for some time.

Improved assessment of security incidents through asset profiles

Managing security incidents can be a significant challenge for organizations because of the dynamic nature of networked applications. Areas of the IT infrastructure where a continuous state of change is common include:

- Network addresses mapped to servers and hosts
- Applications running on a specific server
- Network ports used for specific applications

- Susceptibility of servers to known vulnerabilities
- Business criticality of specific servers and applications
- Ability of network and security systems to report security incidents accurately

It is important for a network security management solution to record all changes in these areas to assess the importance and relevance of observed events collected by the system. A key capability in QRadar is asset profiling that build a time-based record of important information about all assets that are present on the network. Metrics maintained in an asset profile include stateful snapshots of:

- Asset identity – Network addresses and resolved system identity
- User identities – User authentication requests, both successful and unsuccessful
- Vulnerability profile – Known vulnerabilities as reported by vulnerability scanners
- Asset weighting – Weighting metrics for an asset including: severity, credibility, and relevance

Asset profiles are valuable in many ways when trying to assess certain types of security incidents. Specific challenges that are solved through the use of information collected in an asset profile include:

- Detecting new servers and applications introduced on a network
- Tracking security incidents back to actual users and systems
- Validating or refuting potential false positives and false negatives
- Prioritizing security incidents based on business criticality

Although asset profiles are an extremely important capability provided by QRadar, it is complemented by advanced correlation of security incidents, called offenses, that leverages a network, application and identity context to greatly improve an organizations ability to correlate and prioritize security incidents on the network.

Cross-technology event correlation to identify complex, enterprise threats

A key capability in QRadar is the ability to correlate security events across multiple disparate device types. Many of today's enterprise threats are complex and span multiple systems. It is important to be able to connect the dots across all network and security events to improve the accuracy of threat detection.

Example: A single attacker launches a DoS within a network, and successfully executes a buffer overflow on one of the targets. The exploited host then performs reconnaissance on additional assets in the network, and attempts to escalate privilege on a mail server, which ultimately fails. While different security devices (i.e. firewall and IDP) will correctly report a flood of events spanning multiple targets and attack categories and different network devices will report a flood of events also spanning multiple categories it is important to synthesize all this activity into a single report of a denial of service attack that includes information on all systems that were affected.

Hidden in the deluge of events that can come from even moderate deployments of Firewalls, VPNs and IDPs on a high-traffic network are the piece parts of what constitutes a prelude to something much more damaging. Indeed attacks like this may take many days to evolve. While individual security devices normally do their part in flagging activity peculiar to the segment or traffic they are watching, greater

visibility is required across all devices incorporating network and security activity as well as the important contextual elements mentioned earlier that help prioritize the severity and relevance of threats.

Improved security incident notification with “Offenses”

When a security event is generated on the network it is difficult to determine the merits of the event without having a complete profile of all other events that have been generated by the infrastructure, both past and present. In addition, it's important to have a complete profile of all additionally relevant security, application, and identity related management information that is provided by the networking infrastructure.

As discussed earlier, many traditional log management and SIEM solutions lack the ability to integrate important network flow and identity information into their correlation engine resulting in a decreased ability to detect more complex threats. Many SIEM solutions attempt to reduce the number of events on the network by looking for specific patterns that might indicate abnormal behavior. Although pattern based correlation is important, if it is the only form of correlation provided by a SIEM solution network and security operators will still be faced with an unacceptable number of alerts that must be addressed. A more effective solution will provide a capability to confirm or deny the merits of any correlated alert against a historical baseline of past behavior across all collected network, application and identity information collected.

This improved capability is best shown by a simple example. Many SIEM solutions provide correlation rules looking for excessive failed login attempts to servers that maintain sensitive information. Suppose the defined rule is configured to generate a failed login notification if a system receives more than 5 login attempts in a one minute period. Any time a legitimate user of the system accidentally types their password wrong 6 or more times, because of bad memory or bad typing skills, will result in an alert that must be addressed by a security administrator. An improved correlation capability will recognize a successful login from the same host after the failed logins and that the user who successfully logged in was legitimate; this improved intelligence would have prevented a false alert from being generated.

QRadar provides an advanced correlation feature called “Offenses” that provides correlation that greatly improves the accuracy of the detection of security incidents. An offense provides the ability to join multiple pattern based rules in addition to a level of intelligence to verify or refute the merits of a correlation rule being triggered. This added validation leverages all relevant data sources including information maintained in an asset profile and historical network activity maintained by the solution. The result is a significant reduction of false positives and a greatly improved ability to provide only the most relevant information to the security operators.

Example: Events are received from a intrusion detection system indicating a Windows service attack and the target's asset profile indicates that the targeted port is open and that there is a vulnerability on the machine: QRadar performs network flow analysis for five minutes on all flows between the attacker and the target, as well as on other flows being sent out from the target of the

attack. The results will help determine the priority of that event as well as any chaining that has taken place between the original target and any hosts it is now attempting to infect.

Although pattern based correlation rules are an important feature of a security management solution, they lack an ability to significantly reduce the tens of millions of events that occur daily on enterprise networks into a manageable set of actionable information. QRadar's advanced correlation called "Offenses" provides a significantly improved ability to detect and notify security operators about the most pressing security incidents.

Verifying reported threats

A challenge too many users of a traditional SIEM face is that the solution is only effective if the events generated by the networked systems are accurate. Unfortunately many devices on the network can be poor at delivering accurate results. Poorly tuned security devices will generate an unacceptable number of false positives and false negatives. It is important to have a capability to verify or refute a particular event so that only accurate results are reported.

Scenario: Intrusion Detection Systems (IDS) have been implemented in an organization to detect rogue network behavior. Since it's deployment it has been continuously tuned and many false events have been eliminated. Unfortunately, with the changing dynamics of network use it still generates an unacceptable level of misleading events.

Many false positives reported by an IDS result from a lack of knowledge, by the IDS, about the vulnerability status of the systems on the network. If an IDS generates an event reporting an attack but the target of the attack is already protected then the false positive could have been prevented or suppressed. QRadar integrates other valuable sources information including vulnerability and flow data to validate or refute all events.

Prioritization of significant "Offenses"

It is difficult for a network security management solution to prioritize threats by relying on the information that is encoded in the events alone. There are external factors to consider when determining the impact of an event, including an asset's:

Severity – how susceptible is this system to an attack

Credibility – how accurate is this system in its reporting of security incidents

Relevance – how important is this system to the business (i.e. criticality)

These factors, when included in the analysis of security management information, provide the ability to prioritize security incidents based on their potential impact to the business.

Scenario: an enterprise is made up of 10's of thousands of networked resources. The network has an average of over 10 million network flows and over 4 million network and security events on a daily basis. The network includes roughly 1000 mission critical network resources that provide core business activities including database, e-Mail, voice, and networking. These critical resources are distributed across over 100 geographically dispersed locations, each of which has varying levels of importance to the organization. The organization is attempting to make sense of the flood of events from the entire organization based on overall impact to the business.

An important aspect of QRadar is the ability to synthesize millions of events into actionable “offenses”. An offense represents a single security incident that needs to be addressed by an organization. An offense represents automated intelligence that would have required hours, if not days, of manual investigation. The offense contains a historical context of all information relevant to the security incident and is prioritized by overall business impact. This organization would reap the benefit of QRadar's advanced correlation that would reduce the almost 800 million events and 14 million flows reported daily to 183 actionable offenses.

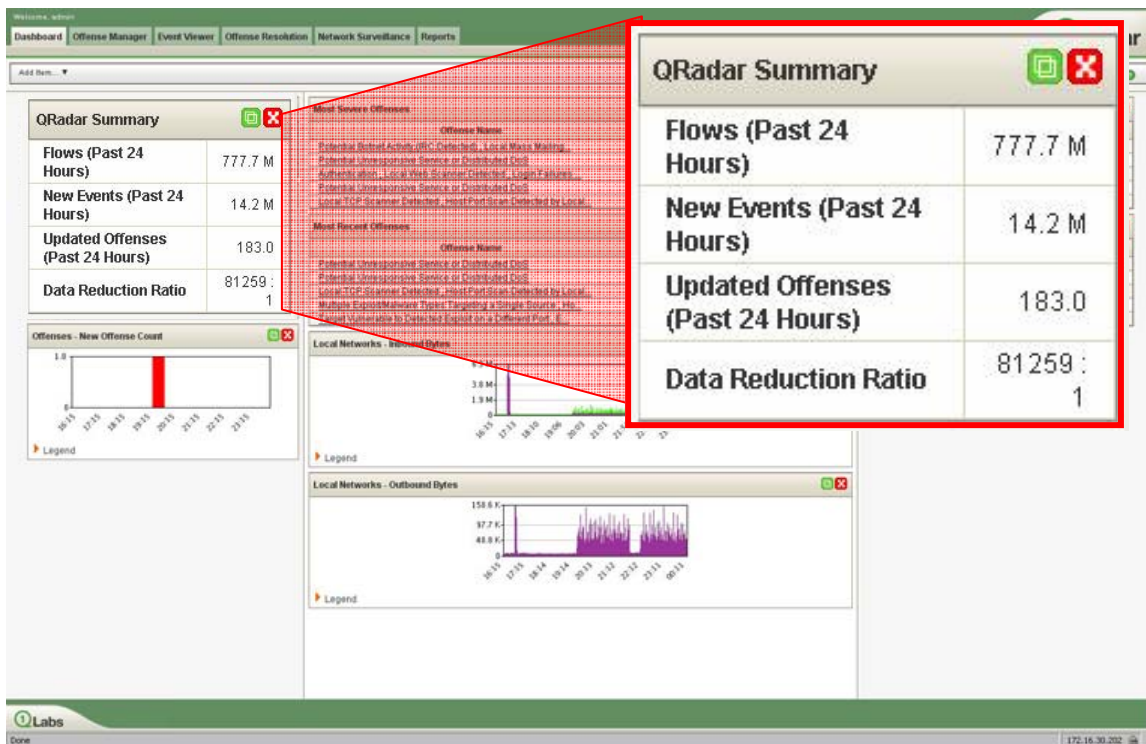


Figure 2: QRadar Offense Summary Dashboard

Protecting data with strong policy enforcement

Many security breaches, where sensitive information was compromised, could have been prevented through strong policy enforcement. Many security incidents occur because inappropriate access to protected information goes undetected by the systems in place.

The good news is that with a comprehensive network security management solution, like QRadar, organizations can better define policy to police access to sensitive information. Important capabilities in QRadar to enforce strong policy include:

- Ability to detect access to specific systems by inappropriate users or groups
- Ability to detect risky protocols like FTP and telnet
- Ability to monitor use bandwidth consuming applications like peer-to-peer and video
- Ability to detect connected systems from un-trusted networks
- Ability to detect data transfers that include sensitive information
- Ability to detect new systems and applications on the network that are not approved
- Ability to detect users on the network that are not known

As organizations look to tighten security controls an important capability is to extract value from information provided across all systems to enforce strong policies which will result in a much improved ability to protect sensitive information.

Summary

Organizations continue to struggle to stay ahead of the evolving threat landscape. Even after significant investment in a plethora of security solutions, security teams still face an enormous burden trying to extract relevant and actionable information about threats from their IT infrastructure. They also face enormous challenge trying to protect valuable corporate data assets. Traditional event management solutions may fall short because they require complex tuning and may not piece together all the pieces necessary to effectively correlate the information required to detect threats. QRadar, from Q1 Labs, provides an advanced network security management solution that bridges the gap across traditionally silo'd management areas to deliver unparalleled surveillance on the network to detect today's more complex and sinister threats, both internal and external, across the entire IT infrastructure.