Q1 Labs®
Total Security Intelligence

IT EXECUTIVE GUIDE

To Security Intelligence

Transitioning from SIEM to Total Security Intelligence

WHITEPAPER

Q1 Labs®

Total Security Intelligence

IT EXECUTIVE GUIDE TO SECURITY INTELLIGENCE

Security Intelligence is Smart Business

Table of Contents

Executive Summary Security intelligence, built on the same concepts that have made business intelligence an essential enterprise technology, is the critical next step for organizations that recognize the importance of information security to their business health.

Too often, the response to new security threats is a "finger in the dam" approach with a particular point technology or reactive new policies or rules. This is in large part because a unified security program, based on automated analysis of unified information from across the IT infrastructure, is costly, complex, difficult to implement and inefficient. As a result, most organizations lack accurate threat detection and informed risk management capabilities.

In this white paper, you will learn how security intelligence addresses these shortcomings and empowers organizations from Fortune Five companies to mid-sized enterprises to government agencies to maintain comprehensive and cost-effective information security. In particular, we will show how security intelligence enables critical concerns in five key areas:

1. **Data silo consolidation**
2. **Threat detection**
3. **Fraud discovery**
4. **Risk assessment/risk management**
5. **Regulatory compliance**

Introduction

Why Security Intelligence?

High-performance enterprises excel in business in large part because they know how to put their information to work. Aided by the automated use of business intelligence technology, they apply analytics to extract maximum value from the massive amounts of data available to them.

The same approach should be applied to securing that information by implementing a security intelligence program. Just as business intelligence helps enterprises make decisions that maximize opportunities and minimize business risks, security intelligence enables them to better detect threats, identify security risks and areas of non-compliance, and set priorities for remediation.

The case for business intelligence is compelling. It enables organizations to support their critical decision-making by automating the data analysis processes at a level that manual analysis can scarcely approach. By applying computer-based business analytics to their unique environments, successful organizations derive the greatest possible value from their amassed terabytes and petabytes of data, from sales revenue and customer demographics to the cost of shipping and raw materials. Consider this from a 2010 article in the Economist ("Data, Data Everywhere"): "Data are becoming the new raw material of business: an economic input almost on a par with capital and labor. 'Every day I wake up and ask, 'how can I flow data better, manage data better, analyze data better?" says Rollin Ford, the CIO of Wal-Mart.'"

The case for security intelligence is equally, if not more, compelling. Enterprises and government organizations have vast quantities of data that can help detect threats and areas of high risk, if they have the means and the commitment to collect, aggregate and, most importantly, analyze it. This data comes not only from point security products, but also from sources such as network device configurations, servers, network traffic telemetry, applications, and end users and their activities.

Security intelligence reduces risk, facilitates compliance, shows demonstrable ROI and maximizes investment in existing security technologies. By analogy to business intelligence, the goals of security intelligence are to:

- Distill large amounts of information into an efficient decision-making process, reducing a billion pieces of data to a handful of action items
- Operationalize data collection and analysis through automation and ease of use
- Deliver high-value applications that help organizations derive the most benefit from their data to understand and control risk, detect problems and prioritize remediation
- Validate that you have the right policies in place
- Assure that the controls you have implemented are effectively enforcing those policies

Organizations have a long way to go in understanding their IT security environment. Consider a 2010 survey by CSO magazine, sponsored by Deloitte, which reported that seven in 10 security incidents are never reported. According to Deloitte, indications are that in most cases the victim organizations are not even aware they have been compromised.

In addition, the 2010 Verizon Data Breach Investigations report revealed that more than a third of the data breaches investigated go undiscovered for months. And, three-fifths of the discoveries are by third parties, not the victim organization. The report also cites "unknowns" as factors in 43% of the breaches: Unknown assets; data that was not known to exist on a particular asset; assets that had unknown network connections or accessibility; unknown user accounts or privileges.

Defining the Problem

The security model of 10-12 years ago is no longer adequate to meet contemporary challenges, as "Internet hooliganism" has given way to organized criminal activity. It is outmoded and does not scale in the face of today's threats and IT environment. Perimeter-based security has evolved to a highly distributed model, as employees, partners and customers conduct business remotely across the Internet and criminals exploit new attack vectors and misplace user trust.

Government and industry regulatory mandates emerged and/or were given "teeth" through stronger penalties and more diligent enforcement.

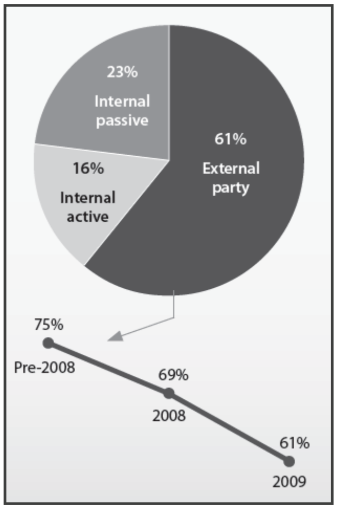
The security industry has responded with new and enhanced products to meet each threat. All of these tools add value to overall enterprise security, but they are, in effect, islands of security technology. They are not conducive to a risk-based enterprise-wide security program, and the overall effort tends to be fragmented.

In many cases organizations have to deal with incomplete data because a given security tool may not recognize a threat or risk for what it is without correlation from other data sources. On the other hand, even when data is collected from disparate sources, analysts are challenged by the sheer volume, making it extremely difficult to distill actionable information.

Security intelligence addresses these problems across the spectrum of the security lifecycle, centralizing data from disparate silos, normalizing it and running automated analysis. This enables organizations to prioritize risk and cost-effectively deploy security resources for detection, prevention, response and remediation.

Simplified breach discovery methods by percent of breaches

Source:
2010 Verizon Data Breach Investigations Report



Moving Beyond Log Management and SIEM

The concept of security intelligence is partially realized in security information and event management (SIEM) tools, which correlate and analyze aggregated and normalized log data. Log management tools centralize and automate the query process, but lack the flexibility, and sophisticated correlation and analysis capabilities of SIEM and, ultimately, security intelligence.

But SIEM should be regarded as a way point rather than a destination. The end goal is comprehensive security intelligence. SIEM is very strong from an event management perspective and plays a particularly important role in threat detection. Comprehensive security intelligence must encompass and analyze a far broader range of information: it requires continuous monitoring of all relevant data sources across the IT infrastructure and evaluating information in contexts that extend beyond typical SIEM capabilities.

Security intelligence should include a much broader range of data, leveraging the full context in which systems are operating. That context includes, but is not limited to: security and network device logs; vulnerabilities; configuration data; network traffic telemetry; application events and activities; user identities; assets, geo-location and application content.

This produces a staggering amount of data. Security intelligence provides great value in leveraging that data to establish very specific context around each potential area of concern and executes sophisticated analytics to accurately detect more and different types of threats.

A key value point for security intelligence, beyond SIEM, is the ability to apply context from across an extensive range of sources.

This reduces:

1. **False positives**
2. **Tells you not only what has been exploited but what kind of activity is taking place as a result**
3. **Provides quicker detection and incident response**

For example, a potential exploit of a Web server reported by an IDS can be validated by detection of unusual outbound network activity detected by network behavioral anomaly detection (NBAD) capability, and vice versa.

Or, you have a report that a server has a potential vulnerability that has just been disclosed. But it's one of hundreds in your organization, so how do you evaluate the threat for this particular server? Security intelligence can analyze all available data and tell you:

- The presence or absence of the vulnerability
- The value the organization assigns to the asset and/or data
- The likelihood of exploit based on attack path threat models
- Configuration information, which may indicate, for example, that the server is not accessible because a default setting has been changed
- The presence of protective controls, such as an IPS

Or, consider the insider threat. The 250,000 diplomatic cables given to WikiLeaks were obtained by a user, Pfc. Manning, who was acting within his authorized privileges. Chances are any given security mechanism would fail to detect this kind of action, but analysis of correlated data, applying contexts from multiple sources, may have stopped the leak before it could cause damage.

The Business Value of Security Intelligence

One of the most compelling arguments for security intelligence is operational efficiency: better use of people, time and infrastructure. It's the ability to incorporate several security and network technologies into an integrated system rather than products operating independently.

The focus on security intelligence is particularly relevant as operational responsibility for security is increasingly being placed in the hands of the network operations teams. It makes sense to mirror this consolidation of operational responsibilities with consolidation at the intelligence layer. Think in terms of enabling multiple tasks in single platform and cross-functional development of skills across the organization, then to deploy access based on roles

Further, security intelligence adds value in other areas of IT, such as troubleshooting system problems, network issues, and user support and authorization analysis.

Security intelligence enables organizations to use integrated tools across a common framework, and leverage a unified data set to address problems along the entire security spectrum. This can be illustrated in five of the most prominent use cases in which security intelligence provides high value.

1 Consolidating Data Silos

Without automated technology, business intelligence analytics are difficult to execute. The data to enable you to understand inventory returns, supply chains, etc., is available, but is siloed in different applications and databases. It falls upon the analyst to compile data from all those sources and pour them into spreadsheets or databases to perform manual analysis. Security analysis poses similar problems, and security intelligence provides similar efficiencies. From a security perspective, data can exist in three types of silos:

- Data locked up in disparate security devices, applications and databases
- Data that's collected from point products, applications, etc., creating, in effect, yet another silo. It's another database where that data is stored, but there's no communication, no coordination between, for example, your configuration database
- Organizational silos of data segregated by business unit, operations group, department, etc.

In the first two cases, security intelligence breaks down the silos by integrating data feeds from disparate products into a common framework for automated analysis across different security and IT technologies. From a security perspective, this brings in all the enhanced detection and risk assessment capabilities the consolidated telemetry of security intelligence can deliver. From a CIO perspective, the reduction of these silos enables the rationalization of security products that would otherwise have to be managed on a point product basis. The third case requires considerable cooperation among groups that are typically separated, meaning a realigning of processes and responsibilities, and perhaps, some pressure exerted by management.

The crushing cumulative volume of all this disparate data exacerbates the problem exponentially. Each of these silos can create enormous volumes of data, in different formats, for different purposes and, in some cases, different policies, and even compliance requirements. Only automated security intelligence can effectively manage petabytes of security-related data and analyze it across organizational and operational silos.

2 Threat Detection

In a few short years, as enterprises have opened themselves to Internet-based commerce and remote users, security has moved from a perimeter-based model with all policy centered on the firewall to distributed security. Security is now focused on hosts, applications and the content of information moving out of the organization.

Moreover, we're seeing growing incidence of highly targeted attacks, such as the attacks on NASDAQ and other high-profile companies. Sophisticated, targeted intrusions are typically multi-staged and multi-faceted, difficult to detect and very difficult to eradicate; advanced persistent threats (APT) are characterized by the tenacity of the attackers and resources at their disposal.

An over-arching intelligence should be applied to the diverse security technologies that have been developed in response to the evolving threat landscape. As noted in the discussion of security context, an activity that appears innocuous to one part of an infrastructure may be revealed as a threat when that data is correlated with other sources. So, for example, an attacker may disable logging, but can't shut down network activity. Proprietary applications may not produce logs; some parts of the network may be without firewalls. Security intelligence can still identify the applications and services running between that host and the network in these cases and flag a potential threat.

3 Fraud Discovery

Security intelligence is absolutely essential for effective fraud detection. The key ingredient, in addition to network telemetry, data from the switching and routing fabric, and the security device enforcement layer is an understanding of the users and the application data.

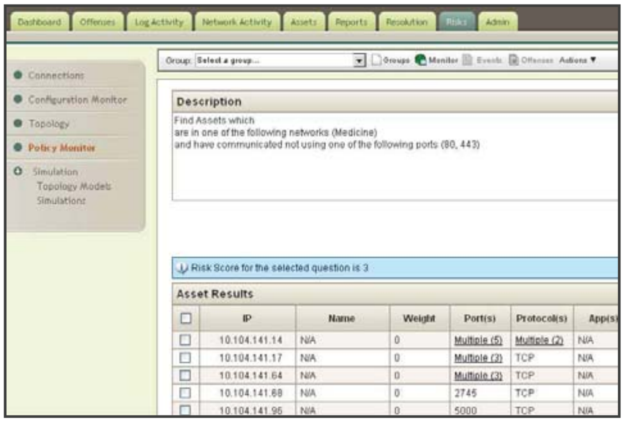
Fraud detection requires monitoring of everything that goes on across the network: network activity and events, host and application activity, and individual user activity. Security intelligence allows you to bind the user to a particular asset, By tying together network, DNS server and application activity with directory information, for example, security intelligence can tie a specific user, to a specific IP address for a specific VPN session.

4 Risk Assessment/Risk Management

Security intelligence provides the backbone for risk management through impact analysis and threat modeling. It is the difference between reacting to attacks on the network and proactively protecting your most important assets.

Impact analysis is based on the value an enterprise assigns to a particular asset and negative consequences to the business if it is compromised. Security intelligence addresses this by asset and data discovery and classification to identify critical assets. Further, it answers questions such as: How exposed is the asset? Does it have direct access to the Internet? Does it have known vulnerability for which there are known exploits?

Threat modeling takes all these factors into account and more¸ identifying not only vulnerabilities on the target system, but possible attack paths based on exploiting weaknesses between the target and the Internet -- poorly designed firewall rules, badly configured router ACLs, etc.



Description

Find Assets which
are in one of the following networks (Medicine)
and have communicated not using one of the following ports (80, 443)

Risk Score for the selected question is 3

Asset Results

□	IP	Name	Weight	Port(s)	Protocol(s)	App(s
□	10.104.141.14	N/A	0	Multiple (5)	Multiple (2)	N/A
□	10.104.141.17	N/A	0	Multiple (3)	TCP	N/A
□	10.104.141.64	N/A	0	Multiple (3)	TCP	N/A
□	10.104.141.68	N/A	0	2745	TCP	N/A
□	10.104.141.96	N/A	0	5000	TCP	N/A

Prioritize Risk - Query for Risk Scoring

5 Regulatory Compliance

Compliance is a foundational use case for security intelligence. It addresses many compliance requirements, particularly all aspects of security monitoring. So, for example, security intelligence doesn't meet all your PCI requirements, but it does meet all you PCI monitoring requirements in a way that SIEM and log management alone cannot. Security intelligence provides the data that serves as a foundation to deliver and demonstrate audit requirements for all regulations.

By monitoring broadly across IT infrastructure – events, configuration changes, network activity, applications, user activity, -- security intelligence consolidates compliance capabilities in a single product suite, rather than relying on multiple point products, each delivering its own piece of the audit puzzle.

Addressing the Bottom Line

Security intelligence, like business intelligence, enables organizations to make smarter business decisions. It enables organizations to process more information, more efficiently across the entire IT infrastructure. Applying business intelligence technology literally enables organizations to do more with less: Instead of having analysts devote expensive hours manually poring through a fraction of the available data, business intelligence automates analysis across all available data and delivers role-based information specific to the task.

Information technology is after all, about automating business processing –for purchasing, logistics, ERP, etc. Security intelligence is about automating security: understanding risk, monitoring the infrastructure for threats and vulnerabilities, and prioritizing remediation.

By centralizing security tools and data from the IT infrastructure, security intelligence enables consolidated management and more efficient use of resources devoted to security. Organizations improve their security posture without additional operational and personnel costs and the expense of purchasing, maintaining and integrating multiple point products.

Security intelligence yields key benefits in business cost and efficiency:

- Reduces cost associated with deployment and operation. Rather than add people, you free them to make security relevant to the business.
- Makes product acquisition simpler and cheaper. Enterprises purchase a single platform, rather than multiple products.
- Facilitates deployment through a unified platform rather than multiple products, which have to be integrated to even approach an acceptable security intelligence capability.
- Gives a broad class of organizations security capabilities that were formerly possible only for the most sophisticated enterprises.
- Automates the collection, normalization and analysis of massive amounts of security data from technical and organizational silos. This capability applies rich context to every analysis.
- Enhances threat detection, applying context to detect possible attacks that might go unnoticed by a particular security technology.
- Improves incident response through accurate and quick detection.
- Realizes staffing ROI. Organizations can implement new security

services, such as world-wide threat monitoring, without additional manpower.

- Empowers enterprises to run highly robust security programs, processing billions of records daily and producing a score or so of high-priority action items every 24 hours.

Q1 Labs Enables Security Intelligence

Q1 Labs QRadar Security Intelligence Platform provides a highly integrated set of solutions designed to help enterprises achieve total security intelligence implemented on a unified operating system and managed through a single console.

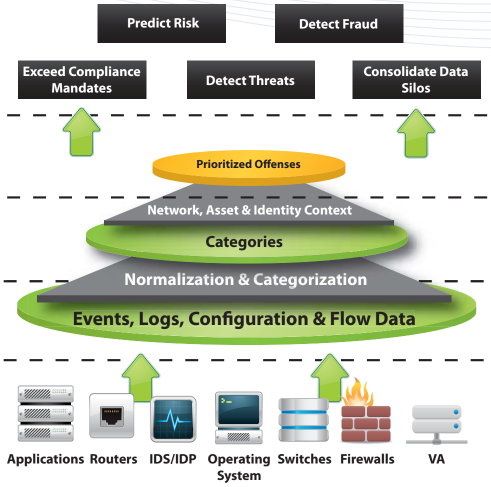
Anchored by a powerful SIEM, QRadar presents a unique security intelligence capability, integrating a set of high-value security and network-monitoring applications into a unified solution that empowers enterprises to deploy security and network operations resources based on analysis of a comprehensive set of data sources.

The QRadar solution is built on Q1 Labs' Security Intelligence Operating System, which enables Q1 Labs to deliver a set of common services around data integration, normalization, warehousing and archiving, and analytics. This unified structure produces a uniform workflow, reporting, alerting and dashboarding capability. These support organization-wide policies and processes, rapidly identify threats and assess risk, and support audit-, operational-, managerial- and executive-level security information and response requirements.

On top of strong core SIEM and log management capabilities, QRadar QFlow technology provides deep network monitoring with sophisticated behavior anomaly detection capabilities that add rich context to analyses that might otherwise rely solely on log data. QRadar application-aware network monitoring enables stateful information about all conversations at the application layer.

Further, QRadar Security Intelligence Platform extends its security intelligence capabilities into virtual network environments with its QRadar VFlow technology, assuring a high level of threat detection and risk management in support of data center consolidation and private and public cloud initiatives.

The risk assessment module, QRadar Risk Manager, provides detailed configuration auditing that adds risk posture context that SIEM alone cannot provide. QRadar Risk Manager evaluates risk and models potential threats against high-value assets, determining possible attack paths based on the wealth of data it draws upon.



Delivering Total Security Intelligence

The Security Intelligence Operating System provides a platform to continue to add new security modules to accommodate new use cases around the intelligent securing and intelligent risk assessment of the enterprise infrastructure. This eliminates the burden of new data integration layers, different storage requirements, new analytics engines, and different reporting infrastructure to accommodate new security applications and potential data sources.

Conclusion

Forward-thinking organizations have recognized and embraced the value of business intelligence technology, as their success is predicated on the ability to analyze and act upon the essential information derived from staggering volumes of data. Similarly, security intelligence is essential because information security is integral to doing business in the 21st century. Powerful, automated analytics of centralized data from sources that cover the entire spectrum of the IT infrastructure make a high level of cost-effective security not only possible, but indispensable.

Q1 Labs
890 Winter Street, Suite 230
 Waltham, MA 02451 USA
1.781.250.5800, info@Q1Labs.com

WPEGSI1011