

Security Threat Management (STM):

A Proactive and Automated Strategy for Addressing Increasingly
Complex Threats to Critical Information

CRA Reports

*This report was prepared by
CRA Reports, an independent
Reporting agency based in
Washington, DC.*

Copyright © 2005
All rights reserved

**Security Threat Management (STM):
A Proactive and Automated Strategy for Addressing
Increasingly Complex Threats to Critical Information**

Part 1. Introduction/Market Overview 3

Part 2. Operational Impact Analysis..... 5

Part 3. Technical Impact Analysis..... 10

Part 4. Financial Impact Analysis 13

Part 5. Conclusion..... 16

Part 6. About the Sponsor: High Tower Software, Inc. 17

Editorial Director
Lane F. Cooper

Research Associate
Tom Moore

PART 1:

Introduction/Market Overview

*This White Paper explores trends that are creating requirements for a proactive and automated approach to managing threats to critical information assets. It introduces the concept of **Security Threat Management (STM)** as a critical component of an integrated lifecycle management framework for effective security management. It demonstrates how a more strategic approach to managing information about security events can elevate the security posture of organizations while reducing the operational costs associated with security management. Finally, it describes the technological requirements for implementing STM to achieve organizational security objectives in a rational manner.*

Three major trends are converging to fundamentally alter how organizations that depend on their information systems maintain their operations defend themselves. These trends are putting more demands on the technical skills of security professionals protecting critical information assets. More importantly, however, they are elevating the role of sound business process management in day-to-day security operations. Consider the following:

- **The volume of threats to critical information assets is rising exponentially.** While it is difficult to quantify the precise number of attacks that are unleashed every year, attack automation, self-replication and proxy-server launches are triggering record numbers of security events. And many of them are successful. According to the Oakbrook Terrace, Ill.-based Computing Technology Industry Association, two of every five organizations have experienced a major information-technology security breach. (These data points come from a 2005 survey of 490 professionals from the public and private sectors.)
- **Blended attacks are becoming more sophisticated.** Security professionals in both the private and public sectors have been victims of a chain of attacks that start with one kind of attack (a virus for instance) that sets up a subsequent denial of service (DoS) attack or phishing scam designed to capture confidential information (such as personal data that can be used for identity theft). According to the most recent Computer Security Institute/FBI Cyber Crime and Security Survey, both virus attacks and DoS outpaced internal theft of proprietary information as the main source of security breach-related costs. The rising sophistication of attacks not only highlights the “intellectual arms race” between hackers and security professionals; it also reflects the profit-motive that is driving a growing percentage of attacks against organizations.
- **Enterprise security infrastructures are becoming increasingly complex, labor intensive, and difficult to manage.** In response to rising threats, organizations continue to make extraordinary investments in information security technology. According to the Freedonia Group, U.S. organizations will boost spending on security technology at a rate of 19 percent a year through 2008. Security professionals must consequently contend with an increasingly confusing array of firewalls, intrusion detection systems, patch management systems and other security technologies developed by the vendor community. This has

introduced a level of complexity that is not only overwhelming security analysts, but is also creating an incident response task list that is swamping IT staffs. In many cases, the high number of false alarms diverts IT professionals from mission critical operations. In others, the sheer volume of incidents results in un-investigated and therefore un-remediated events that can lead to significant harm.

The status quo in security event management is clearly not tenable. While the discreet security technologies developed in response to these trends are getting increasingly sophisticated, the way most organizations manage these tools is outdated.

...A Time for Change

It is the position of this report that the current state of security management is not optimized to address these converging trends. It concludes that new security technology developments must be matched with better, more automated and proactive management strategies that correlate and integrate information from a wide array of security solutions.

Armed with this new management strategy, organizations will be able to better identify, prioritize and efficiently respond to the most important threats to the most critical assets in a timely and cost-effective fashion.

Since it is the goal of all security teams to shorten the time and distance between awareness of critical security incidents and organizational response, security teams will have to adopt Security Threat Management (STM) strategies.

...STM Defined

Security Threat Management refers to the automated aggregation, correlation and integration of threat event information reported by multiple security systems (i.e. firewalls, IDS, anti-virus, routers, etc.) to quickly identify incidents and then prioritize, take action and track them from their first manifestation through to their remediation and resolution.

STM is designed to provide executives that have technical, operational **and** strategic responsibilities with comprehensive insight into the security posture of their organization.

"The need to integrate and correlate security event data is critical to all organizations. If you cannot integrate information from various security reporting devices on the enterprise network, then that means that human resources will have to be allocated to visit each box on the network to gather log data. That is very inefficient. Having gathered all of the log data of security events, if you cannot then effectively correlate the threats to vulnerabilities on critical information assets, then it is impossible to get a complete picture of your organization's exposure to risk." -- Eugene Schultz, Ph.D., CISSP, CISM, University of California, Berkeley Lab

PART 2:

Operational Impact Analysis

*"There are a lot of good point solutions for detecting problems at the firewall or on the host. But many people are overwhelmed with the amount of data, and struggle to distinguish between false positives and true high-priority risks. The result is information overload for security professionals." -- **Ames Cornish, Independent Security Consultant, Montebello Partners***

STM strategies replace the largely manual and labor-intensive operations, processes and procedures that currently characterize security incident response in most organizations.

Today, analysts manually gather data by inspecting logs and reports from various elements in the enterprise network and security infrastructure; they then review the data, and decide which incidents to address. In this model, as more security event data are generated by these systems, more analysts are needed to keep up with the volume of work. Since the volume and complexity of attacks on enterprise systems are expected to grow exponentially by the end of the decade, the cost implications of this model are unsustainable.

A significant amount -- perhaps even a majority -- of the security information reported in log files, intrusion detection system output, and reports produces false positives. In other words, a considerable amount of an analyst's time is spent on routine time-consuming activities designed to rule out reported incidents as actual threats. This diverts efforts away from addressing incidents that have the potential to disrupt operations or violate the integrity of the enterprise's key information systems.

Under prevailing management models, once security information is analyzed, the security team issues directives -- or recommendations -- on what actions to take in order to address the threats. Often the directives take the form of requests to general IT staffers, who must then time share remediation activities and other critical operational tasks.

The hand-off between security analysts and IT staffers often serves as an opportunity to lose track of how, when -- or even if -- appropriate remediation has taken place. This is because most large organizations tend to have separate organizational structures for their security teams and their IT departments.

*"Consequently, most organizations are not able to identify and address the growing number of attacks and potentially exploitable vulnerabilities on their networks. Moreover, they typically do not even have the means to compose a complete picture of their exposure levels." -- **Raj Patel, Vice President/Engineering, High Tower Software, Inc.***

...A Better Way

STM strategies recognize that security management is today a strategic operation. Indeed, security is seen by many as a critical utility that supports all strategic operations -- whether they directly support existing clients (Customer Relationship Management),

contribute to the generation of new revenue (Sales Force Automation), streamline the channel of distribution (Supply Chain Management), or support strategic partnerships (Collaborative Business Management).

Major organizations in both the public and private sector are investing time, money and significant intellectual resources to automate and optimize all of their critical processes. They are aggressively identifying inefficient manual operations that are labor-intensive and error-prone.

This perspective is being brought to bear on security operations. STM-based strategies provide a framework upon which the next generation of best practices can be developed to proactively protect critical assets and business processes.

From an operational standpoint, STM can be implemented in a phased process that consists of developing:

- An inter-disciplinary management team that will use STM data to optimize their operations.
- An enterprise-wide repository of security incidents that aggregates, integrates and correlates reports from across the organization.
- An automated support system for executing and monitoring responses to security incidents.
- A mechanism for capturing, storing and analyzing how the organization has responded to different events to learn from previous activities and develop new policies and best practices that continuously hone the security readiness of the organization.

...STM Impact Analysis

Given the strategic role of security in the enterprise today, it is neither necessary nor appropriate to limit information about an organization's risk exposure to the security and IT teams. Senior executives in line-of-business departments are increasingly interested in having a real-time insight into the threats to which their operations are exposed.

It may not be necessary to provide these non-technical executives with the granular levels of detail needed by IT and security departments. However, having high-level reports that advise them of potentially disruptive events based on analysis of prevailing threats to systems on which they depend can allow executives to develop contingency plans. It can also provide them with advance notice, giving them time to effectively shift into a contingency mode.

"Financial service organizations frequently face the threat of system downtime due to malicious or anomalous behavior. A security threat management system alerts users to threat activity that could disrupt the organizations online business operations. The organization can then be prepared to initiate contingency plans if necessary to allow customers to complete important transactions" -- Greg Kuiper, Information Security Manager, High Tower Software, Inc.

However, In order for these non-technical executives to use security event information gathered by an STM system, it is necessary to develop a common understanding of what security event data mean, how they were generated and how incidents indicated by these data may affect business operations. It is also important for the security and technical teams to appreciate when and how to communicate with non-technical business executives more effectively.

Therefore, a comprehensive map of how various elements in the enterprise system support specific business processes must be developed. An effective threat map, along with vulnerability analysis based on a detailed understanding of the prevailing business realities, requires that an inter-disciplinary team of executives work together closely in developing appropriate security plans and policies.

This phase of the STM process not only allows the organization to react and respond to threats more effectively from a business continuity perspective, but also provides the security and IT staffs with a common understanding how various elements in the enterprise system affect different parts of the organization. It keeps the technical teams on the same page, reducing the likelihood of misunderstanding or miscommunication concerning issues related to protecting critical assets.

...STM-Based Assessment: Setting the Stage for a Strategic Response

With a comprehensive enterprise-wide STM policy and impact analysis in place, the next phase is to automate the aggregation of threat data from the scores of devices and appliances on the network that are generating incident reports and logs.

It is critical at this stage to implement STM aggregation technology that can interact with a wide array of technologies developed by various vendors. It must also support multiple standards, formats and protocols. The key issues to address in this phase include:

- **Automated Aggregation.** STM aggregation systems must be able to automatically receive critical data from all elements on the enterprise network and bring all incident reports into a common repository, thereby eliminating the need to manually gather incident data from disparate security systems. In some cases it may be necessary for STM aggregation systems to poll other systems to receive critical data.
- **Automated Integration.** Having aggregated the raw security incident data, STM integration technologies must next automatically transform the data into a common format so that data from firewalls, intrusion detection systems, firewalls, etc., can be jointly analyzed. Automatic integration is a critical step. It not only saves a tremendous amount of labor, but it also reduces the likelihood of transposition errors that can occur when manually mapping disparate data types to a common format. Ideally, STM integration will generate exception reports when there is confusion about the data. This should significantly reduce the amount of raw data that must be handled manually, and also improve the productivity of security personnel.

- **Automated Correlation.** The final step in this phase calls for STM correlation technology to automatically associate the identified incidents -- and the threats that they represent -- with the known vulnerabilities of elements (this information is gathered during the STM Impact Analysis phase and is updated continuously) within the enterprise network that could be exposed to the attacks.

...Executing an STM-Enabled Response Strategy

With data now automatically aggregated, integrated and correlated with known vulnerabilities across the enterprise, security analysts can work with a comprehensive data set to make decisions and add value to the security management process in a way that machines and intelligent databases simply can not.

- **Strategic Prioritization.** By automating the initial aggregation and analysis of security incident data, security professionals can very quickly begin the process of weeding out false positives and low-priority incidents. STM-enabled prioritization processes allow more time for analysts to work on incidents that have the highest likelihood of causing real problems for the organization in the short term. A primary objective, in fact, is to spare the IT staffs from vetting false alarm activities; chasing "red herrings," after all, does not breed trust. If false alarms are kept in the security team's domain of activity, IT staffs have a higher level of confidence when responding to remediation requests from the security team.
- **Strategic Action Plans.** More time for high-priority incidents also means that analysts can develop more detailed and appropriate action plans for potentially disruptive incidents. Providing precise instructions in order of priority to the IT staffs helps ensure that the most pressing threats are immediately addressed. STM-enabled action plans also provide IT staffs with context about how to work remediation activities into their daily tasks. Most importantly, however, detailed and tailored instructions (as opposed to vague boiler plate entries generated from raw reports) remove opportunities for mixed signals that result in important threats going unchecked.
- **Tactical Tracking.** Follow-up analysis and tracking is probably one of the weakest areas of activity in most manual security management systems used today. Unless there are formal procedures requiring IT staffs to report on the results of remediation activities, there can be no guarantee that a threat has been addressed. Moreover, the status of all credible threats (including the mid- and low- priority threats) must eventually be addressed. An STM-based tracking system can be designed to establish parameters and tolerances so that threats that have not been immediately addressed (because they have been listed as low-priority issues) are eventually upgraded. This is an important function -- especially today, when blended attacks may initially manifest themselves as a series of low-impact attacks that set up more aggressive incidents later. In most manual management systems today, the avalanche of false positives and routine security activity requests results in many events being unaddressed. Yet, ignoring any credible attack can be dangerous in today's threat environment.

- **Strategic Reporting.** By strategically monitoring the status of an incident throughout its entire lifecycle in a granular fashion, security teams create a clear real-time window into the risks to which their organizations are exposed. But it is also important to develop data analysis capabilities that can provide meaningful insight to the *entire* community of interest that is working to mitigate an organization's exposure to risk. This means that the data should be mined to provide various types of executives -- whether they are non-technical line-of-business executives, IT administrators or security professionals -- with reports that contribute to their ability to manage human resources, business processes and critical technologies accordingly.

...Contributing to a Learning Repository

Most world class organizations recognize that they operate in dynamic environments in which the criteria for success and failure are constantly changing. The same is true in the security arena. Threats are constantly evolving, converging and reinventing themselves to compromise the integrity of their targets' information systems.

The final -- and perhaps most important -- role of an STM strategy is to provide a real-time library and information analysis center that ensures an organization is constantly optimizing its response to the changing threat matrix. An STM repository not only contains information about all of the important attacks to which an organization has been exposed, but also documents the actions that were taken to remediate them.

Security is as much an art as it is a science. Much can be learned from comparing how different analysts responded to the same attacks. The organization can then standardize on the most effective response.

The STM repository can also provide a longitudinal picture of how threats evolve. This provides security analysts with an opportunity to anticipate how new attacks may manifest themselves. This is especially important as organizations change their business processes in response to new competitive or regulatory requirements.

"New collaboration initiatives in the healthcare sector, for instance, may change the way hospitals share sensitive patient records. Often these new business processes will be pilot tested. An STM-based security management strategy should be implemented with these pilots, so that the security teams of the collaborative community of interest can immediately begin the never-ending process of optimizing the security posture of these new business processes." --
Raj Patel, Vice President/Engineering, High Tower Software, Inc.

PART 3:

Technical Impact Analysis

"Stove-pipes of security technology can become as big a barrier to a strategic response to threats and vulnerabilities as the actual attacks. Perspective and context must be built into the security process, if organizations are to effectively mitigate their exposure to risk." -- Alvin Mann, Engineer, High Tower Software, Inc.

In response to the operational and strategic imperatives that are driving demand for STM solutions, a new set of technical requirements is emerging. While the general automation and integration requirements -- which are discussed below with some specificity -- are now increasingly recognized by leading security thinkers across industries, there is a need to connect the dots between the technical tools that are available in the marketplace today and the strategic business requirements of organizations that hope to ensure the continuity of their operations. Thus, what follows is a non-technical summary of the specific elements that must be in place to ensure the successful deployment of an STM strategy.

There are seven basic elements to an STM strategy that must be integrated and optimized into enterprise operations to ensure a highly effective organizational risk management posture. These are:

- **Automated Aggregation.** In the security profession a lack of data is usually not as much of a problem as a plethora of data. Indeed, most security operations are overwhelmed by the avalanche of alarms and incident reports generated by a wide array of security point solutions (including firewalls, intrusion detection systems, routers, etc.) that monitor and react to potential threats. Today, many organizations still manually gather and process information from each of these devices.

One of the first technical steps to take in an STM-based environment is to automate aggregating so-called "syslog" data into a common repository. This means that an STM-based system must be able to interact and interoperate with multiple types of hardware, software and business process applications and gather appropriate threat data on as close to a real-time basis as possible. Given the nature of threats today -- with "zero-day" attacks now an increasingly common phenomenon -- organizations can no longer afford to wait for individuals to manually review syslog data on a weekly or even daily basis. STM requires technology that can reliably retrieve and interact with appropriate threat data from a wide-array of platforms. This not only provides the basis for accelerating the time to identify incidents but it also provides an important step forward in managing the complexity associated with working with a large number of security technologies that are focused on monitoring and protecting discreet threats and vulnerabilities.

- **Automated Integration.** A common repository makes it possible to create a common data structure so that security personnel and resources can engage in an "apples-to-apple" analysis of threat information.

STM-based strategies therefore require a capability that can automatically "map" various data formats aggregated from different technology platforms and applications into a common format. The technology must be intelligent enough to recognize common data types and harmonize their different manifestations (based on the devices that generated the data) into a "common expression." This is a prerequisite to meaningful analysis. And, again, the more quickly this integration step is taken, the sooner threats can be identified, prioritized and acted upon.

- **Automated Correlation.** The integration step enables the correlation function to take place. With data now available in a standard format for analysis, security resources can be applied to determine if the different security technologies are reporting on a related series of events. For example, the correlation function can determine whether the alarm reported by a firewall is part of the same phenomenon reported by the intrusion detection system.

Until recently correlation activity has typically been a labor intensive and manual process. An STMM environment, however, calls for technology that can automatically "connect the dots" between the reports of different security devices to identify trends or common anomalies that may indicate a serious series of events is converging to threaten organizational assets. In a non-STM environment the correlation process is separate and distinct from the aggregation and integration processes. But in the STM environment correlation activities must automatically categorize the nature of events (as malicious or reconnaissance-related for instance) by analyzing the results from all of the different reporting. It provides the foundation for minimizing the number of events to which security teams must respond, and is the basis for filtering false- or low-priority-alarms.

- **Strategic Prioritization.** Automated correlation is indeed a pre-requisite for developing a strategy for prioritizing the allocation of security resources. Many security organizations today respond to alarms generated by their various security monitoring and remediation tools on a "first-come-first-served" basis. A manual and un-integrated security environment provides no way to quickly distinguish between the high-number of low-impact events reported by their security resources and the handful of high-impact activities that can breach the integrity of an organization's information systems.

STM calls for technology that can quickly allow decision-makers to prioritize what, how and when to deploy security resources based, among other things, on:

- The nature of the threat (i.e. multiple security devices have confirmed that a threat is in fact manifesting itself in a certain way);
- The value of the targeted assets to the organization. This can be based on user-defined assessments of which databases, communications and networking elements are most critical to business continuity;

- The criticality of the business processes that may be under attack. For instance, non-critical administrative activities would have a lower priority than mission-critical transaction processing activities.

STM-enabled systems are able to suggest priorities to the security teams by correlating the nature of real-time events with user-determined business rules of engagement to create algorithms that generate risk scores associated with the monitored events.

- **Tactical Action Plans.** Based on the risk scores, an STM system can then generate an immediate tactical action plan by providing recommendations and tiered options for:
 - Deploying security resources;
 - Allocating available security and IT personnel;
 - Selecting appropriate tools for response;
 - Providing guidance on specific processes associated with deploying the security tools;
 - Providing guidance on how to manage specific processes to minimize disruption to ongoing business operations.
- **Tactical Tracking.** As people and resources are deployed, a case management file is opened so that the work-flow can be tracked.

STM requires technologies that can track and measure the progress of the response to threats against pre-determined performance parameters. Thus, if important high-priority activities begin to fall behind schedule, or people managing the remediation initiative fail to fulfill critical steps in the remediation process, user defined parameters can trigger an escalation report to bring these activities to the attention of team leaders as well as higher-level managers.

- **Strategic Reporting.** Many organizations see security management as a long series of search and destroy activities in which threats or vulnerabilities are identified and then minimized.

STM calls for a much more strategic approach to the mid- and long-term management of an organization's security posture. By having a comprehensive understanding of how the organization has responded to threats, STM can create a deeper context for the use of such data and information that can be extremely useful to:

- Security professionals
- IT staffs;
- Line of business managers; and
- Senior organizational executives.

The strategic reporting function provides the basis for linking threats and vulnerabilities to the strategic objectives of organizations so that there is a macro-perspective on how to optimize the allocation of security resources not only now, but also in the future.

PART 4:

Financial Impact Analysis

Most security cost justifications, such as for a firewall or intrusion detection system, focus on the cost of the breach, the cost of the appliance, the reduced risk of incurring a breach, as well as the business opportunity enabled by “opening” the network to the potential threats (sometimes referred to as the e-business “intensity”). This financial impact analysis does not go down this path. Rather it focus on the costs associated with managing the active network security devices in various sized networks through alternative means, as well as the cost and benefits of automating and tracking the incident response phase to resolve the threat.

A fully developed cost justification model should best be organized by separating the cost analysis into an incident identification phase and an incident response phase. The reason for this is that organizations may apply completely different technologies to the two phases, and different products exist on the market to handle one phase or the other.

STM-based solutions support both phases; a cost-benefit analysis should compare the possible alternatives of combining different solutions for each phase. For example, an organization could outsource its event monitoring, but manage internally the incident response function, or outsource both. But it can apply and use the principles of STM to automate or improve the response in both phases. For the purposes of this report, we define Phase One as consisting of:

- Aggregation;
- Integration; and
- Correlation

Further, we describe Phase Two as being made up of:

- Strategic Prioritization;
- Tactical Action Plans;
- Tactical Tracking; and
- Strategic Reporting

The two phases contain actions that require some combination of hardware, software and human interaction. (See Technical Impact Analysis on page 10.) A complete ROI model would outline the costs for the hardware, software and man-hours for the various alternative solutions. A purely manual approach would focus, for example, as shown below, exclusively on comparable man-hours.

...Phase One: Aggregation, Integration and Correlation of Security Event Data

For comparison purposes in evaluating Phase One, Datamonitor analysts report in their *Security Information Management* monograph dated December 2004, that organizations are using four techniques to currently monitor their security alerts. Those are:

- Log management tools from individual network security devices;
- Third-party event correlation tools;
- In-house proprietary solutions;
- Managed Security Service Providers (MSSPs).

These solutions could be considered at least a partial automation of a completely manual approach, which less sophisticated, smaller organizations may still be doing. The chart below lists the estimated man-hours for the continuing process of manual security event management.

Function	Description	Man Hours
Group One		Example:
Log Aggregation	Collection of logs from security devices	42 Man-hrs per week
Log Integration	Gathering logs in common format on single device	5 Man-hrs per week
Log Correlation	Association of log data with known threats	Up to 24 Hrs per day*

A fully developed financial impact analysis would look at the cost comparison, effectiveness, and efficiency of an STM-based solution to that provided by a point-solution provider of log aggregation tools, developing an in-house solution, and outsourcing the task to an MSSP.

...Phase Two:

Phase Two consists of prioritization, planning, tracking and reporting. Among the solution alternatives to managing the incident lifecycle are:

- Using an STM workflow management system;
- Using an external trouble-ticketing system;
- Using an MSSP;
- A manual process using post-it notes and email;

A complete ROI analysis for Phase Two would necessarily incorporate the costs of reporting on security remediation efforts for the purposes of compliance, the cost to respond to auditors, as well as the day-to-day costs of the security team. The chart below lists the estimated man-hours for the continuing process of managing the security lifecycle on a mostly manual basis.

Phase Two		
Strategic Prioritization	Prioritize security events	Up to 4 Hrs per day*
Strategic Action Plans	Define or recommend action plan	Up to 4 Hrs per day*
Tactical Tracking	Track security event lifecycle	Up to 12 Hrs per day*
Strategic Reporting	Provide reporting on security events	Up to 6 Hrs per day*

* 24x7x365

There are a great number of business processes in tracking and responding to security threats, many of which vary from industry to industry, making this an exceedingly complex comparison compared with the better understood process in Phase 1.

However, it's in Phase 2 that an STM solution targeted at compliance initiatives may have the greatest ROI justification. This is, among other reasons, is why external expertise needs to be brought in to conduct a detailed analysis of the alternatives.

PART 5:

Conclusion

In the past it was possible to manually inspect output of IDSs, firewalls, system auditing, and other sources, but many reasons now dictate that organizations adopt STM strategies. These strategies enable organizations to recognize threats faster and more efficiently; they also facilitate responding to them.

STM not only aids in dealing with security-related incidents that have occurred; it also enables an organization's information security practice to become more proactive by helping the organization to better understand applicable security threats and how they can be countered. Organizations are increasingly planning and implementing these strategies. Organizations that have not yet adopted an STM strategy are falling further behind the proverbial information security power curve; An appropriate STM strategy for any organization needs to be developed on the basis of a cost-benefit analysis; the particular strategy adopted will vary from one organization to another.

PART 6:

About the Sponsor

High Tower Software, Inc.

High Tower Software, Inc. is a privately held company based in Orange County, California. The High Tower® Security Threat Manager (STM) appliance was designed to simplify the security threat management process by analyzing extremely high volumes of security event data in real-time and then presenting the results in a comprehensive yet intuitive display. Its robust correlation rules and analytics are applied to event data streams to identify anomalous activity and provide important insight to the security operator.

High Tower STM provides a holistic view of the entire network and physical infrastructure, giving administrators quick access to detailed event information. The appliance correlates and analyzes data from a wide array of security devices in real time as events take place. And using patented technology, the system analyzes, and then filters out normal network activity and false positives to generate a clean, concise view of active threats.

Security alerts are displayed on High Tower's proprietary monitoring system and notifications can be sent to email, pagers, or cell phones - allowing security administrators to instantly respond to critical and anomalous events from around their network and expedite remediation. For more information:

High Tower Software
26970 Aliso Viejo Parkway
Suite 200
Aliso Viejo, CA 92656
Phone: 949-330-3080
Toll free: 877-HI TOWER (877-448-6937)
Fax: 949-330-3081
www.high-tower.com