



MAZU NETWORKS INTELLITACTICS

Enterprises have a number of security systems and devices in place, including firewalls, intrusion detection and prevention systems, anti-virus solutions, etc. Each of these addresses a specific range of security concerns. While Intellitactics provides for the central analysis and storage of events and logs, companies still struggle to protect their assets and applications.

So what's missing?

Behavior Analysis, Continuous Global Visibility, Integration with Existing Security Products

Behavior Analysis

Behavior analysis enables you to understand what's happening on the network and how a threat or event is affecting your systems and users. Without behavior analysis, it can be difficult to take action with confidence.

Continuous Global Visibility

Continuous global visibility is critical in today's complex network environment. There are so many places to watch for so many types of threats. The more visibility you have, the more confident you can be in the protection of your network.

Integration with Existing Network Management Products

Your ability to address and recover from an event is only as good as your response capabilities. In order to ensure maximum response with minimum damage and disruption, you need integration with the security products already deployed in your environment.

Mazu and Intellitactics Security Manager (ISM)

The Intellitactics Advantage

Intellitactics Security Manager (ISM) centralizes and stores security data from throughout the technology infrastructure so enterprises can automate log aggregation, correlation, and analysis, as well as recognize, investigate, and respond to incidents automatically. In addition, ISM allows enterprises to streamline incident tracking and handling, enable the monitoring and enforcement of policy, and provide comprehensive reporting for regulatory compliance efforts.

The Mazu Advantage

Mazu provides continuous global visibility into how users, applications, hosts, and devices are behaving on a network, and detects if there are meaningful changes from their typical behavior that indicate a network performance issue, a security threat, or an application problem. Through Mazu, enterprises understand usage patterns, consumption rates and dependencies between users, applications and network infrastructure.

A Powerful Combination

Mazu's Network Behavior Analysis (NBA) system and ISM have been integrated in two ways:

- 1) ISM can receive and correlate Mazu alerts
- 2) ISM users can easily link to Mazu for a network behavior perspective on any event

These two solutions combine to provide powerful analysis of the same environment from completely different and independent perspectives. Mazu uses the behavior analysis of network traffic flows while ISM correlates host and security device log files. Mazu's behavior analysis, providing detailed network activity information, can be accessed via ISM's user interface. This information on how an event is affecting the network and the services running on it enables enterprises to better understand the impact of event response actions.

MAZU NETWORKS

INTELLITACTICS

Continuous Global Visibility

Routers and switches are ubiquitous across the network. Because Mazu monitors flows from the routers and switches, integrating Mazu with ISM doesn't just add one more security device; it effectively adds every router and switch to the arsenal of data sources.

Typical Integrated Workflows

There are two typical workflows for an integrated solution in a Security Operations Center.

In the first workflow, ISM generates an alert. For example, through the analysis of firewall and Windows logs, ISM determines there are a dozen potentially compromised systems. As the SOC operator views the alert for each system, his first step is to generate a Mazu traffic report for the system directly from the ISM GUI. The Mazu traffic report provides a comparison of the traffic before and after the potential incident to typical behavior for that host. Evidence of deviation from normal behavior provides substantial corroboration of a compromised host. Mazu could then be used to remove that host from the network.

The second workflow is driven by an event generated from Mazu. The Mazu system will identify zero-day attacks and malicious behavior by credentialed users that often slip by other security solutions. When the Mazu alert appears on the ISM GUI, the SOC operator can easily drill down to the Mazu UI for a complete view of the potential problem and can see such information as user identity, switch ports, ports, protocols, applications, and traffic volume. Mazu presents mitigation plan for addressing the issue along with an analysis of the "collateral damage" to typical traffic if the mitigation plan is implemented.



Mazu Networks

125 CambridgePark Drive
Cambridge, MA 02140
Tel (617) 354-9292
Fax (617) 354-9272
www.mazunetworks.com



Intellitactics

1800 Alexander Bell Drive - Suite 500
Reston, VA, 20191
Tel (703) 620-3800
Fax (703) 620-3850
www.intellitactics.com

About Us

Mazu Networks

Mazu Networks provides continuous global visibility into how users, applications, hosts and devices are behaving on a network, and detects if there are meaningful changes from their typical behavior that indicate a network performance issue, a security threat, or an application problem. Through Mazu, enterprises understand usage patterns, consumption rates and dependencies between users, applications and network infrastructure. Only Mazu offers continuous global visibility, automatic and custom behavioral analysis benefits for network operations, and security and superior integration with network and security products. Mazu Networks' customers optimize their network operations, secure their internal networks and maximize application availability.

Intellitactics

Headquartered in Reston, VA, Intellitactics provides the world's leading enterprise security management solutions used by security analysts, operations, and risk officers to achieve cost-effective regulatory compliance; mitigate risk by automating security operations, and accelerate incident resolution to ensure the availability of critical business services. Intellitactics' products empower organizations to simplify security and compliance. The flagship product, Security Manager, combines event, alert, and incident management to mitigate exposure to cybercrime, with extensive automated analysis and reporting. A strong complement to Security Manager is Intellitactics™ SAM, which measures security value and features security assurance metrics™ on a configurable dashboard. Other products include Intellitactics for Compliance and Intellitactics for Enterprise Defense.