Trustwave®
Smart security on demand

MANAGED INTRUSION DETECTION

IDENTIFY ATTACKS ON YOUR NETWORK ASSETS

Trustwave Managed Intrusion Detection delivers customized, comprehensive security for organizations that need data security experts to monitor network and application-layer traffic via an Intrusion Detection System.

THE MANAGED SERVICES ADVANTAGE

Perimeter defenses alone are not enough to secure your network. Round-the-clock, expert human analysis that complements investments in security technology and controls is essential to detect potentially malicious activity within your network.

An Intrusion Detection System (IDS) plays an integral role in supplementing other security measures in modern corporate networks. However, to be effective, an IDS implementation requires disciplined processes and experienced staff, carefully configured systems and consistent tuning and updates of the IDS device itself. That's why so many organizations entrust their IDS management to Trustwave.

- **Consultation and Design** Following an extensive network review and scoping exercise, Trustwave will recommend the most effective placement of IDS sensors within your network.

- **Configuration and Policy Development** Once Trustwave experts work with you to identify the subnets and VLANs you wish to monitor, they will tune the IDS to your environment and test and deploy the customized configuration. After initial deployment – and before the service becomes fully operational – Trustwave engineers will continue to monitor and adjust IDS policy to establish a baseline in order to optimize device performance.

- **Ongoing Device Management and Signature Updates** Trustwave network security engineers manage the IDS service remotely from our 24x7 Security Operations Center (SOC). Trustwave's attack-tracking libraries are regularly correlated, tested and updated by our own Trustwave SpiderLabs Signature Operations team to ensure emerging threats are monitored and brought to the appropriate parties' attention.

- **Continuous Event Identification** Events from your IDS logs are continuously reviewed to identify threats. To minimize false-positive events, qualified network security engineers will analyze event logs and notify you in the case of an actual or potential threat.

- **Timely Response and Escalation** When an issue arises, the Trustwave SOC will notify designated personnel within your company as a first step in your incident response policy.

- **Managed Intrusion Detection** Trustwave Managed IDS Service deploys sensors at key locations on your network to identify patterns of suspicious activity. Network security engineers then analyze event and traffic data 24x7 to assess a threat's potential to harm corporate assets.

- **Proactive 24x7 Notification** Notification is conducted in accordance with pre-approved policy. Security events are classified as "potential," "medium," "high" and "critical," and customers can tailor notification guidelines to their preference. Interaction with your staff is carried out in a secure manner— through strict authentication and confirmation protocols either through our TrustKeeper portal or over the phone.
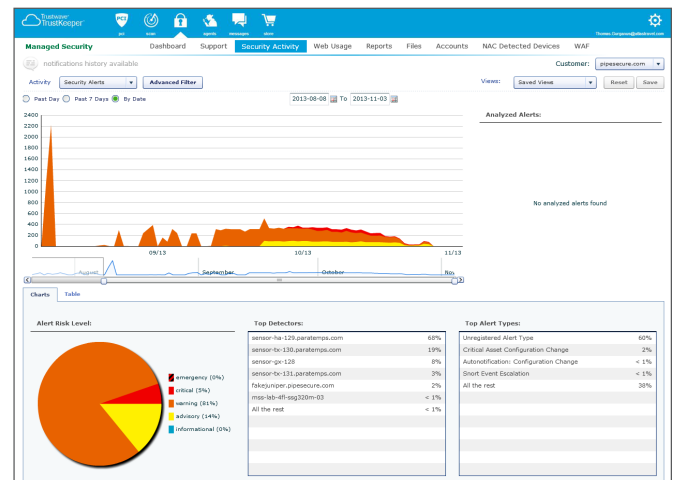
IDS Event Report Details

- **Dynamic Online Reporting and Documentation** A record of alerts is documented along with the actions taken in response to each attempted intrusion. Via a secure portal, you have round-the-clock access to all captured events and those that warranted additional action.

- **How it Works** Trustwave Managed IDS Service adheres to best practice standards. Following an initial consultation, Trustwave's network security engineers configure and thoroughly test the IDS sensors. Once the device is installed on the customer site, Trustwave engineers then perform further tuning on the device.

- **Why it's Effective** Trustwave IDS utilizes a combination of signature and anomaly detection to identify potentially malicious activity. Trustwave's network security experts respond to events triggered by policy exceptions based on signature match or observed traffic anomalies, such as malformed or atypical packets, to ensure that appropriate actions are taken.

- **Benefits** Trustwave Managed IDS provides a full-service solution that eliminates the following:
  - Hassles of in-house management
  - Costs associated with staffing a 24x7 operation
  - Recruiting, hiring and retaining qualified staff

- **Results Delivered** Unlike hardware or software-oriented solutions, the foundation of Trustwave Managed IDS Service rests upon expert human analysis. Through our online, secure portal, you have continuous access to reporting that includes real-time and historical event information (stored for an agreed upon length of time). To assist with internal control and compliance requirements, a record of attack events and their severity is automatically posted to the portal for review and assessment-support purposes.

- **Related Services** Trustwave Managed IDS Service can be deployed alone or in concert with other Trustwave data security and compliance services as required by your organization.

TRUSTWAVE IDS THREAT ANALYSIS AND ALERTING

Expert Threat Analysis

Automated Analysis & Normalization

Combination of automated & human analysis prioritizes alert events to determine actual threats for notification

Trustwave IDS inspects internal and external network traffic, and forwards alerts for potential malicious activity to Trustwave SOC

Actionable alerts detailed in Trustwave customer web portal for incident response support

Trustwave®
Smart security on demand

For more information: https://www.trustwave.com

Copyright © 2015 Trustwave Holdings, Inc.