TippingPoint Security Management System Threat Insights is an aggregation portal that takes events from TippingPoint NGIPS, vulnerability scanners, and sandboxing solutions and displays them in one place to prioritize, automate, and consolidate network threat information. This allows multiple security groups to have a common framework for evaluation and resolution. By automating the aggregation of threat data from multiple security tools, Threat Insights assists security professionals by prioritizing incident response measures for breaches or potential vulnerabilities, and highlights preemptive actions already taken to protect your network.

Key Benefits:
- Provides a single-pane-of-glass view for network security
- Provides visibility to prove that your NGIPS is providing proactive protection
- Prioritizes security response based on threat data
- Automates potential threat forwarding and analysis
- Integrates with Trend Micro portfolio and third-party security solutions
- Available anywhere from your mobile device
PRIORITIZE

With thousands of events created each day by your security solutions, it can be a challenge to determine where to start or how to respond. Threat Insights will help you prioritize your response by showing you:

- Which breached hosts require the most attention
  - Based on the number of times a host has been breached
  - Based on the number of times a threat has been detected
- What vulnerabilities you have and which Digital Vaccine® (DV) filters can be applied to provide protection
- See vulnerabilities currently protected by DV filters or virtual patches and those vulnerabilities that may have a DV filter available, but not applied
- Which zero-day threats have been detected
- Determine if undisclosed zero-day DV filters fire, requiring your immediate attention

A single portal gives you a centralized view of your network security, enabling you to respond rapidly to seek out, isolate, and mitigate threats.

AUTOMATE

Automation is key to a smooth-running security stack and reduces time to secure. By having our security tools work together to automatically pass tasks or threat responses between each other, security effectiveness and security staff efficiency can be improved. Via the TippingPoint SMS, the TippingPoint NGIPS will automatically submit identified potential threats to the TippingPoint Advanced Threat Protection Analyzer for further evaluation. Once detonated, monitored, and analyzed, the sandbox will automatically send the threat information back to the SMS where it is aggregated and viewed in the “Discovered Suspicious Objects” tile in Threat Insights. This tile will give you a view of the suspicious (IP or DNS address) URL, severity, and whether it was protected.

INTEGRATE

A single-vendor security solution may have a strong flagship product, but weak add-ons leave critical gaps in protection. Consolidating vendors who provide integrated security solutions will enable you to be more efficient with incident response via automation. Trend Micro is not just focusing integration on our own portfolio, but making sure we integrate with third-party security solutions, providing automatic workflows and putting relevant information together in summarized views.

Threat Insights provides a single location to view these integrations. From the portal you can see suspicious objects that have been automatically passed between NGIPS and the sandbox. The integration between the NGIPS and sandbox gives you increased security effectiveness by broadening protection from unknown threats.

Vulnerability scanners can be a great security tool, but can also require a lot of attention to ensure protection of discovered vulnerabilities. SMS matches vulnerability scan data with existing DV filters. With a few clicks, these vulnerabilities can be addressed to avoid potential catastrophe. Threat insights displays the vulnerability scan data, matching DV filters, and the number of times the vulnerability had been successfully attacked or blocked. This gives you a prioritized view of the vulnerabilities you need to address and the preemptive protection provided by the TippingPoint NGIPS.

Threat Insights is powered by XGen™ security, a cross-generational blend of threat defense techniques that is smart, optimized, and connected. Threat Insights provides smart protection with exclusive vulnerability information from the Zero Day Initiative (ZDI) and zero-day threat protection, is optimized with third-party integration, and connected through the integration with the TippingPoint NGIPS and Advanced Threat Protection solutions.