THREATQUOTIENT ™

paloalto
NETWORKS®

THREATQUOTIENT™ AND PALO ALTO NETWORKS' MINEMELD

Timely processing of the potential risks to your business is critical to your security. This includes the rapid ingestion of millions of indicators at high frequency, along with the distribution of accurate and relevant intelligence to the systems and people that protect your assets.

The joint solution of ThreatQ™ and MineMeld by Palo Alto Networks® enables you to distribute third-party intelligence from ThreatQ's Threat Library™ and make them available for consumption by the Palo Alto Networks security platforms.

THREATQ BY THREATQUOTIENT™

ThreatQ is an open and extensible threat intelligence platform (TIP) to provide defenders the context, customization and collaboration needed for increased security effectiveness and efficient threat operations and management. ThreatQ accelerates the transformation of threat data into actionable threat intelligence by giving defenders unmatched control through a Threat Library, an adaptive workbench and an open exchange to ensure that intelligence is accurate, relevant and timely to their business. With ThreatQ, customers can automate much of what is manual today and get more out of existing security resources, both people and infrastructure.

ThreatQ is used to:
- Improve Situational Understanding
  – Understand threats through context and adversary profiling, enabling defenders to anticipate threats and proactively update security posture.
- Accelerate Detection and Response
  – Combine external and internal threat data to provide context and relevance, empowering better decision making and automated actions.
- Maximize Existing Security Investments
  – Automate intelligence distribution to your existing sensor grid to ensure the right intelligence is delivered to the right tools at the right time.
- Advance Team Collaboration
  – Enable your security teams to be more efficient and effective through greater information sharing and instantaneous knowledge transfer.

INTEGRATION HIGHLIGHTS

Provide security teams with a single Threat Library for all threat intelligence, both external and internal

Ensure threat intelligence is accurate, relevant and timely for your organization

Automatically distribute third-party indicators of compromise from ThreatQ to MineMeld to maximize the value of your threat intelligence

Automate enforcement of prevention-based controls for Palo Alto Networks Next-Generation Security Platforms
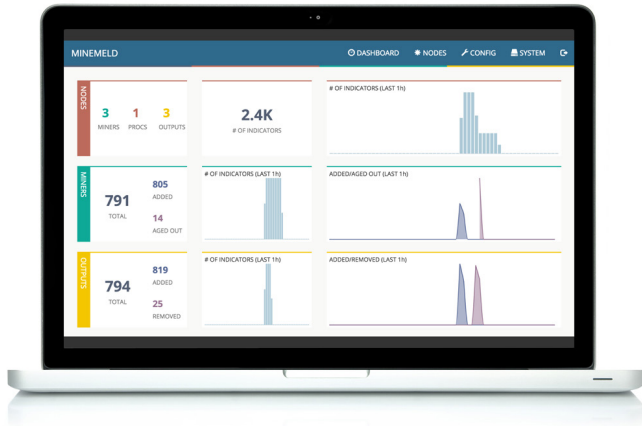
MINEMELD BY PALO ALTO NETWORKS

MineMeld, by Palo Alto Networks, is an extensible threat intelligence processing framework. Based on an extremely flexible engine, MineMeld can be used to collect and distribute indicators from ThreatQ to the Palo Alto Networks Next-Generation Security Platform for enforcement.

MineMeld natively integrates with Palo Alto Networks security platform to automatically create new prevention-based controls for URLs, IPs and domain intelligence derived from all sources feeding into the tool. Now, organizations can simplify their workflows for blocking indicators of compromise (IoCs) with external dynamic lists and dynamic address groups, without spending additional resources to manage block lists, including the automated timeout of expired indicators.

MineMeld further integrates with the Palo Alto Networks AutoFocus™ contextual threat intelligence service, allowing you to identify high-value, targeted indicators – in AutoFocus – and block them on your next-generation firewall with export lists and MineMeld.

INTEGRATION USE CASES

The integration supports a variety of use cases such as:

Centralize and enrich threat data feeds; profile adversaries and associated indicators.

Leverage MineMeld to enforce new, third-party prevention controls in Palo Alto Networks devices, including blocking malicious IPs and other IoCs.

Evaluate the value of a specific threat intelligence feed for your environment

Extract indicators from Palo Alto Networks device logs and share them with ThreatQ for use in its Threat Library.

ABOUT THREATQUOTIENT™

ThreatQuotient understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, empowers defenders to ensure the right threat intelligence is utilized within the right tools, at the right time. Leading global companies are using ThreatQ as the cornerstone of their threat intelligence operations and management system, increasing security effectiveness and efficiency.

For additional information, please visit threatq.com.

Copyright © 2017, ThreatQuotient, Inc. All Rights Reserved.

ABOUT PALO ALTO NETWORKS®

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets.

Find out more at www.paloaltonetworks.com.

THREATQUOTIENT™