RISKIQ®

partnered with

DEMISTO

Think Outside the Firewall™

Orchestrating Digital Threat Intelligence

Benefits

- Orchestrate threat discovery, intelligence, and mitigation actions through playbooks.
- Reduce time to resolution by using one platform to collaborate, investigate, and document.
- Shorten decision-making cycle by automating key tasks with analyst review.

In today's rapidly changing digital landscape, a major challenge faced by security teams is the difficulty in reconciling internal IOC and event data with external threat actor behavior and assets. With many attacks originating from outside the firewall, analysts spend inordinate amounts of time combing through multiple data sources to gain additional context into attacks. Users need a platform that unifies intelligence across data sources to accelerate incident response.

Users can now leverage the multi-source threat intelligence capabilities of RiskIQ PassiveTotal™ with the security orchestration and automation features of Demisto Enterprise for repeatable and scalable incident response that coordinates across different security measures.

Integration Features

- Automate enrichment of alerts as playbook tasks: passive DNS information, SSL certificate data, WHOIS data, IOC intelligence, and so on.
- Run search and query operations on WHOIS, SSL, and OSINT data based on keywords and metadata.
- Leverage hundreds of Demisto product integrations to further enrich RiskIQ data and coordinate response across security functions.
- Run thousands of commands (including for RiskIQ) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.

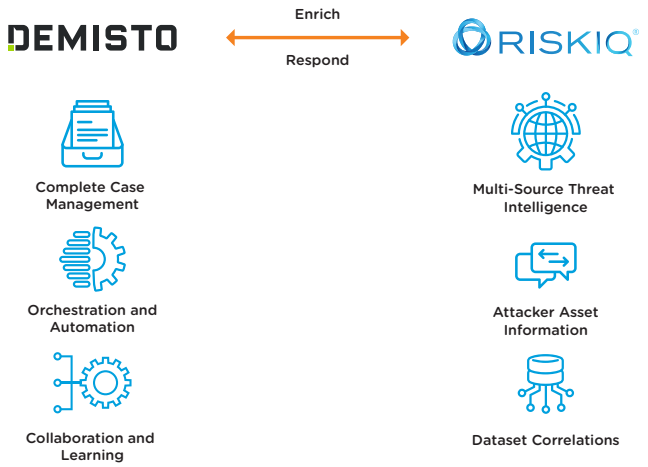

Fig 1 - Demisto's integration with RiskIQ

Use Case #1: Automated Phishing Enrichment and Response

Challenge

There is often a mismatch between the high-volume nature of phishing attacks and analyst agility in responding to them. Phishing attack identification, triage, reputation checks, and response involves switching between multiple screens, mundane and repeatable tasks, and tunnel vision that precludes knowledge of larger attack campaigns that encompass a phish mechanism.

Solution

Security teams can use the RiskIQ integration to automate multi-source enrichment of and response to phishing attacks via playbooks. Once alerts have been ingested into Demisto, playbooks can query RiskIQ's platform to get data from WHOIS, SSL certificates, passive DNS, host pairs, and internal IOCs, among others.

Playbooks can also orchestrate across other security products to execute actions such as sending users an email, opening a ticket, quarantining an endpoint, and detonating a file hash in a sandbox. Security teams can also choose to have bottlenecks before important tasks that give them manual oversight to verify preceding information and guide playbook progression.

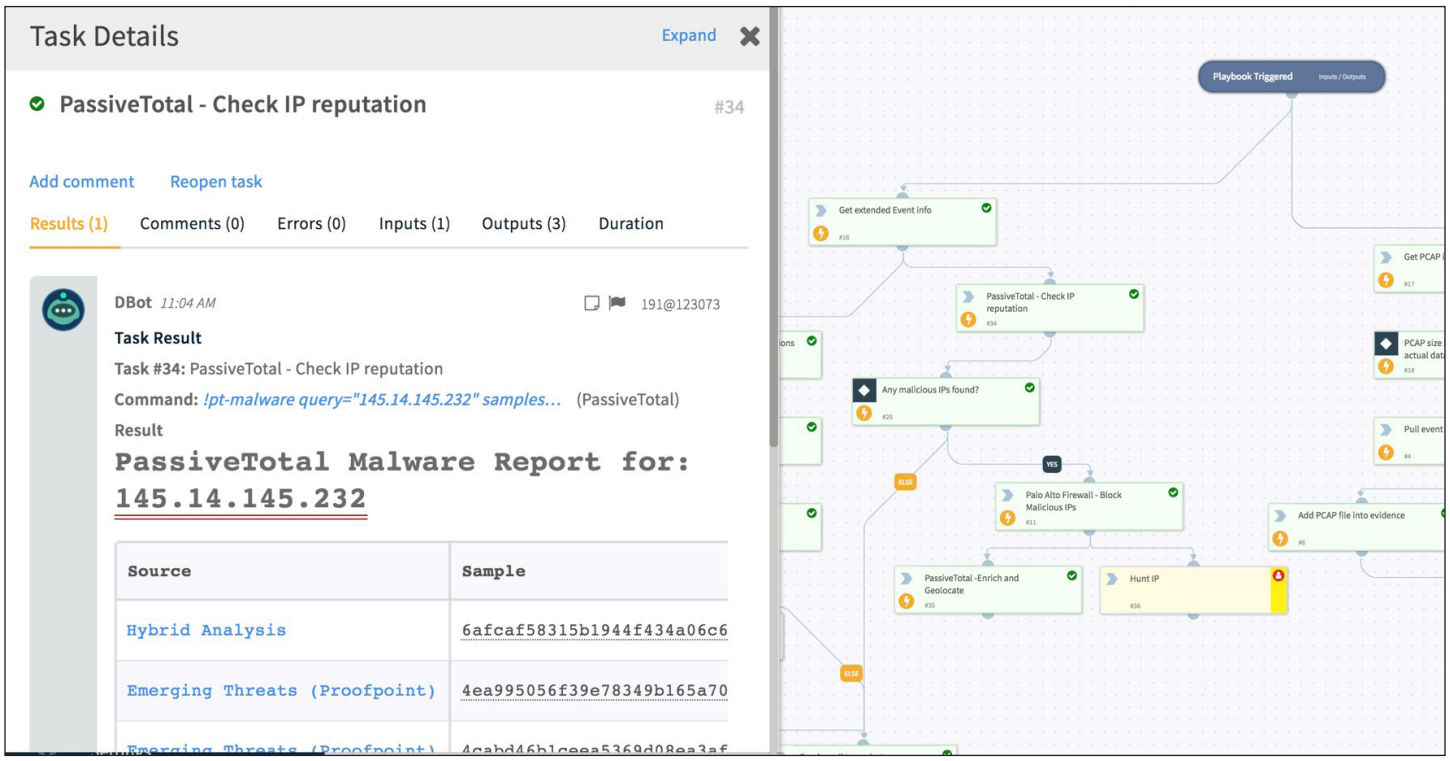

Fig 2 - Screenshot of a Demisto playbook querying RiskIQ's platform

Benefit

Enrichment and response playbooks automate a host of actions across products so that analysts have a wealth of information at their fingertips while starting incident investigation. Automating RiskIQ lookups can save screen switching time and execute repeatable tasks. Orchestrating actions across products in one window can help analysts coordinate across security functions for richer and deeper incident context.

Use Case #1: Interactive, Real-time Investigation for Complex Threats

Challenge

While standardized, repeatable playbooks can automate commonly performed tasks to ease analyst load, an attack investigation usually requires additional tasks such as pivoting from one suspicious indicator to another to gather critical evidence, drawing relations between incidents, and finalizing resolution. Running these commands traps analysts in a screen-switching cycle during investigation and a documentation-chasing cycle after investigations end.

Solution

After running enrichment playbooks, analysts can then gain greater visibility and new actionable information about the attack by running RiskIQ commands in the Demisto War Room. For example, if playbook results throw up alert details, analysts can get host pairs, subdomains, and DNS data tied to that alert in real-time by running the respective RiskIQ command. Analysts can also run commands from other security tools in real-time using the War Room, ensuring a single-console view for end-to-end investigation.

The War Room will document all analyst actions and suggest the most effective analysts and command-sets with time.

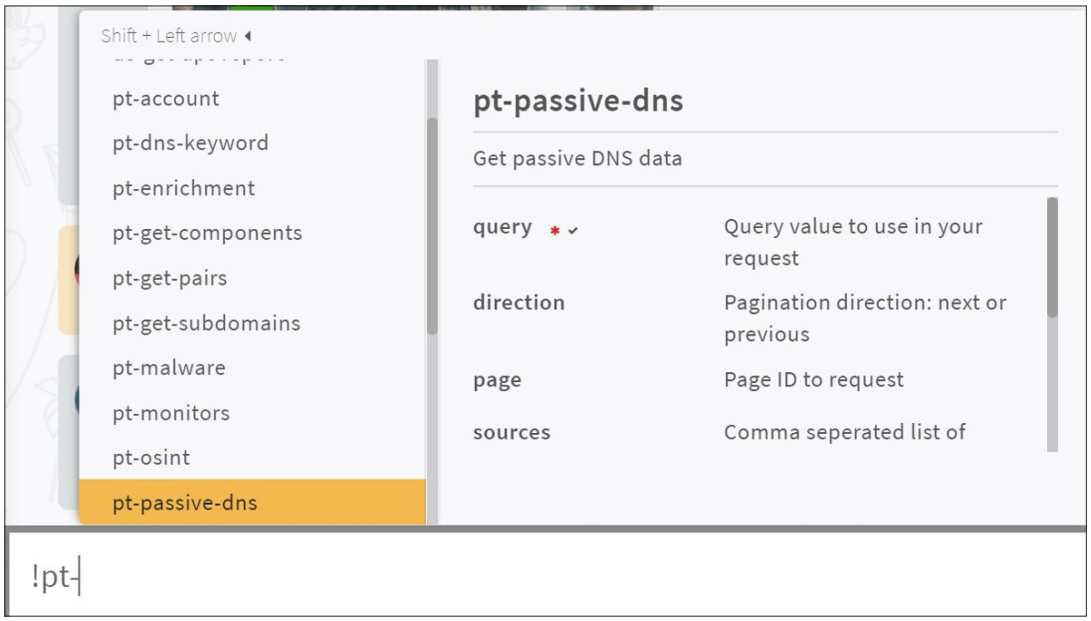

Fig 3 - Screenshot of Demisto War Room

Benefit

The War Room allows analysts to quickly pivot and run unique commands relevant to incidents in their network from a single window. All participating analysts will have full task-level visibility of the process and be able to run and document commands from the same window. They will also prevent the need for collating information from multiple sources for documentation.

RISKIQ

RiskIQ provides comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. RiskIQ's platform delivers unified insight and control over external web, social, and mobile exposures. Thousands of security analysts use RiskIQ to expedite investigations, monitor their attack surface, assess risk, and remediate threats.

Learn how RiskIQ could help protect your digital presence by scheduling a demo today.

22 Battery Street, 10th Floor
San Francisco, CA. 94011

sales@riskiq.net RiskIQ.com
1 888.415.4447 @RiskIQ