Demisto And RSA

For Automated Security Analytics And Ticket Management

Benefits

- Automate triage and response for NetWitness alerts and Archer tickets.
- Enrich investigation data with rich context, packet captures, and correlations.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

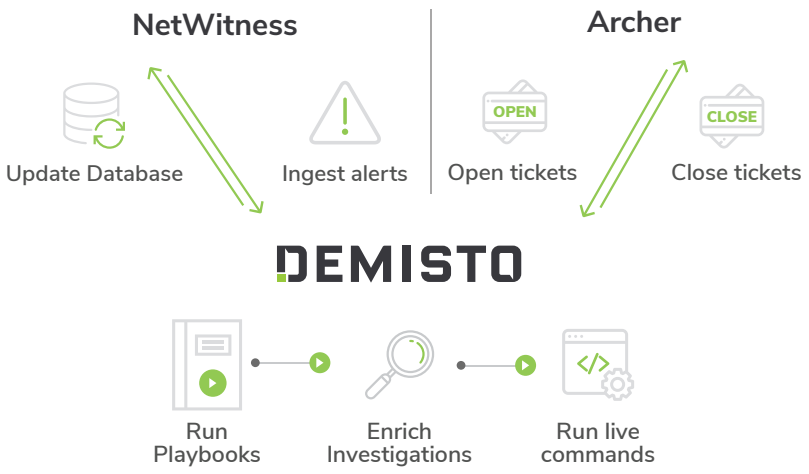
- Products: Demisto Enterprise, RSA Archer GRC, RSA NetWitness
- Product Versions: Demisto Enterprise v3.x, RSA Archer 6.2, RSA NetWitness 10.6.3
- Platform: Platform Independent

Security teams face unique challenges in today's data-heavy landscape with sophisticated attackers and vast threat surfaces. Separating insights from noise, battling a growing number of alerts, and coordinating between multiple security products all weigh heavily on the security analyst's mind.

To help meet these challenges, users can now enhance the ticket management features of RSA Archer and the security analytics suite of RSA NetWitness with Demisto's security orchestration, case management, and collaboration capabilities.

RSA and Demisto integration features:

- Ingest NetWitness alerts data and/or Archer ticket data into Demisto Enterprise.
- Trigger playbooks for enrichment and resolution of NetWitness alerts and Archer tickets.
- Leverage 140+ Demisto product integrations to enrich NetWitness and Archer database.
- Run 160+ NetWitness and Archer commands interactively via a ChatOps interface while collaborating with other analysts and Demisto AI.

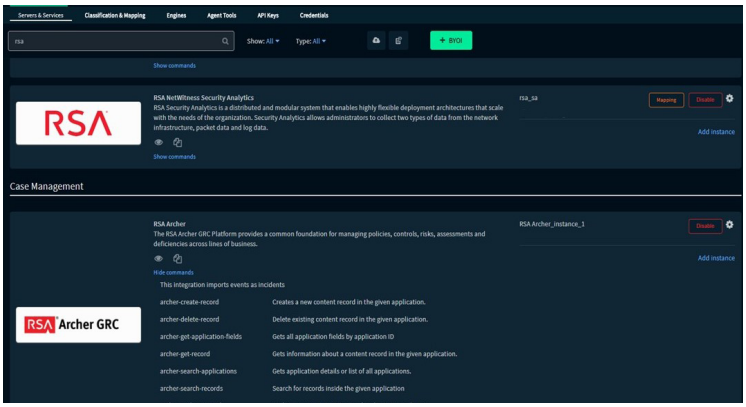


USE CASE #1 EXTRACTING CONTEXT FROM INVESTIGATION DATA

Challenge: During investigations, analysts need to check indicators, find out whether they are malicious, and weave a contextual thread through the endless holes of data at their disposal. Faced with many indicators sans context, this can be a repetitive and time-consuming process.

Solution: After ingesting alert data from NetWitness, analysts can leverage actions from 140+ security products to enrich the NetWitness database. They can pull and add packet captures from external sources using Demisto orchestration. Demisto also uses hypersearch to give analysts critical context about the indicators associated with an incident. Analysts can view indicator malice, repeating patterns, and cross-correlations at a glance in both the work plan and war room windows.

Benefit: Contextual viewing of data allows for quicker identification of remediation procedures and running the respective playbooks/actions to curtail the incident. Orchestrating security actions from multiple products in one window saves screen switching time, gives a better visual representation of alert data in one place, and enables further enrichment of individual sources through bi-directional integrations.



USE CASE #2 AUTOMATED TICKET MANAGEMENT AND RESPONSE

Challenge: If a security analyst uses different platforms for incident management and ticket management respectively, it can be tough to track the lifecycle of an incident due to flitting between screens, fragmented information, and lack of single-window documentation.

Solution: If SOCs use RSA Archer for ticket management and Demisto for incident management and security orchestration, they can trigger actions for specific ticket types in Archer to create an incident in Demisto and vice versa. Ticket resolution can also be streamlined by automatically running playbooks upon ticket creation in Archer.

Benefit: Demisto playbooks and investigation toolkits can gather additional information needed for triage and resolution of Archer tickets. Analysts can align ticket management with an incident's lifecycle, can access documentation from a single source, and forego the need to switch between screens.

About RSA

RSA, a Dell Technologies business, offers business-driven security solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and, reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high risk world. For more information, go to **rsa.com.**

About Demisto

Demisto Enterprise is the first and only comprehensive Security Operations Platform to combine security orchestration, incident management, machine learning from analyst activities, and interactive investigation. Demisto's orchestration engine automates security product tasks and weaves in the human analyst tasks and workflows. Demisto enables security teams to reduce mean time to resolution (MTTR), create consistent incident management process, and increase analyst productivity. Demisto is backed by Accel and other prominent investors and has offices in Silicon Valley and Tel Aviv. For more information, visit **www.demisto.com** or email **info@demisto.com.**