DEMISTO AND PREEMPT FOR IDENTITY-BASED THREAT PREVENTION AND AUTOMATED REMEDIATION

Benefits

- Automate threat prevention, event enrichment, investigation, and policy enforcement 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.

Compatibility

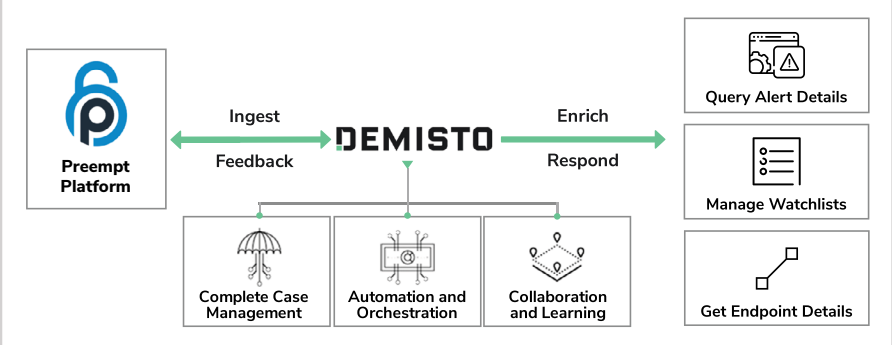
- Products: Demisto Enterprise, Preempt Plat form v2.4 and above

In today's constantly evolving cybersecurity landscape, a singular focus on perimeter security is no longer sufficient. There needs to be a shift towards more continuously adaptive identity and behavior-based threat prevention that takes situational context into account. Equally important is the need for prevention measures to coordinate with other security operation processes. Isolated security measures, however effective, will result in a ballooning of alerts and repetition of low-level tasks by security teams.

To meet these challenges, users can combine the adaptive threat prevention capabilities of Preempt Platform with the security orchestration and automation features of Demisto to accelerate incident response and reduce business risk.

Integration Features:

- Ingest Preempt Platform alert data into Demisto to create incidents and trigger playbooks tied to those incidents.
- Bi-directional event enrichment and adaptive enforcement that adapts based on situational context.
- Automate enrichment of alerts as playbook tasks: add or remove users from watch lists, get alert and endpoint details, get time-based activities,and so on.
- Leverage hundreds of Demisto product integrations to further enrich Preempt Platform alerts and coordinate response across security functions.
- Run thousands of commands (including for Preempt Platform) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



USE CASE #1 AUTOMATED THREAT ENRICHMENT AND RESPONSE

Challenge: The fragmented nature of threat prevention and incident response tools can make it tough for SOC teams to track the lifecycle of an incident due to moving between screens, fragmented information, and the lack of single-window documentation. Incident response will also often involve a host of important but repetitive actions that analysts need to perform, leaving them time-strapped for actual problem-solving and decision-making.

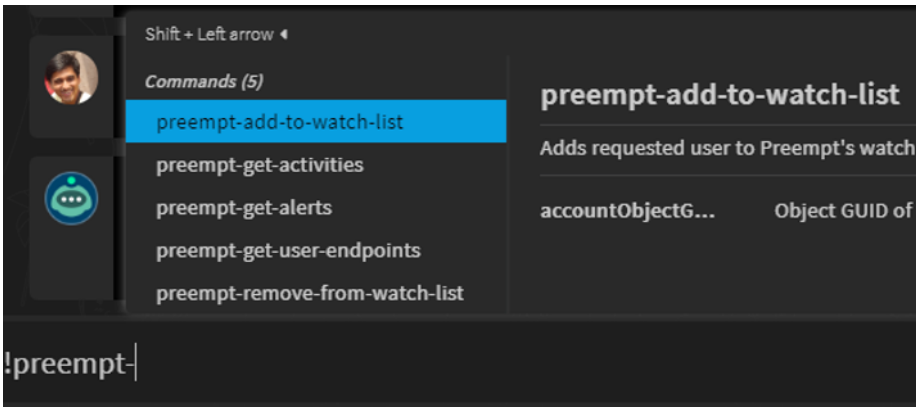
Solution: SOCs using the Preempt Platform for threat prevention and Demisto Enterprise for security orchestration and automation respectively can automate incident creation and trigger playbooks in Demisto for specific alert types in Preempt Platform. This playbook will orchestrate investigation actions across the entire stack of products that a SOC uses in a single screen and seamless workflow.

For example, analysts can leverage Preempt Platform to enrich alert details, endpoint details, and add users to watchlists as automatable playbook tasks.

Benefit: Demisto playbooks coupled with Preempt Platform actions can standardize and speed up triage and resolution of security alerts. Analysts get a comprehensive view of the incident's lifecycle, access documentation from a single source, and forego the need to switch between screens while performing investigation actions.

USE CASE #2 INTERACTIVE, REAL-TIME INVESTIGATION FOR COMPLEX THREATS

Challenge: Apart from running automated actions, attack investigations usually require additional real-time 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 gain greater visibility and new actionable information about the attack by running Preempt Platform commands in the Demisto War Room. For example, if playbook results throw up user details, analysts can get the list of endpoints accessed by that user in real-time by running the respective Preempt Platform 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.

Benefit: The War Room allows analysts to quickly pivot and run unique commands relevant to incidents in their network from a common 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.

About Preempt

Preempt protects organizations by eliminating internal threats and security breaches. Threats are not black or white and the Preempt Platform is the only solution that delivers identity and access threat prevention that continuously preempts threats based on identity, behavior and risk. This ensures that both security threats and risky employee activities are responded to with the right level of security at the right time. The platform easily scales to provide comprehensive identity based protection across organizations of any size. The company is headquartered in San Francisco, CA. Learn more about us at **www.preempt.com**.

About Demisto

Demisto is the only Security Orchestration, Automation and Response (SOAR) Platform that combines orchestration, incident management and interactive investigation into a seamless experience. Demisto's orchestration engine automates security product tasks and weaves in human analyst tasks and workflows. Demisto Enterprise, powered by its machine learning technology, acquires knowledge from the real-life analyst interactions and past investigations to help SOC teams with analyst assignment suggestions, playbook enhancements, and best next steps for investigations. The platform (and you) get smarter with every analyst action. Demisto is backed by Accel with offices in Silicon Valley and Tel Aviv. For more information, visit **www.demisto.com** or email **info@demisto.com**.