DEMISTO
A PALO ALTO NETWORKS® COMPANY | pagerduty

Automated Digital Operations Management and Incident Response

Benefits

- Leverage PagerDuty's personnel management and scheduling features within Demisto for coordinated incident oversight across security and IT teams.
- Further enrich PagerDuty data with intelligence from other security tools via Demisto's orchestration to achieve unified context for cross-functional processes.
- Improve team efficiency by centralizing collaboration, investigation, and documentation.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

- Products: Demisto Enterprise, PagerDuty

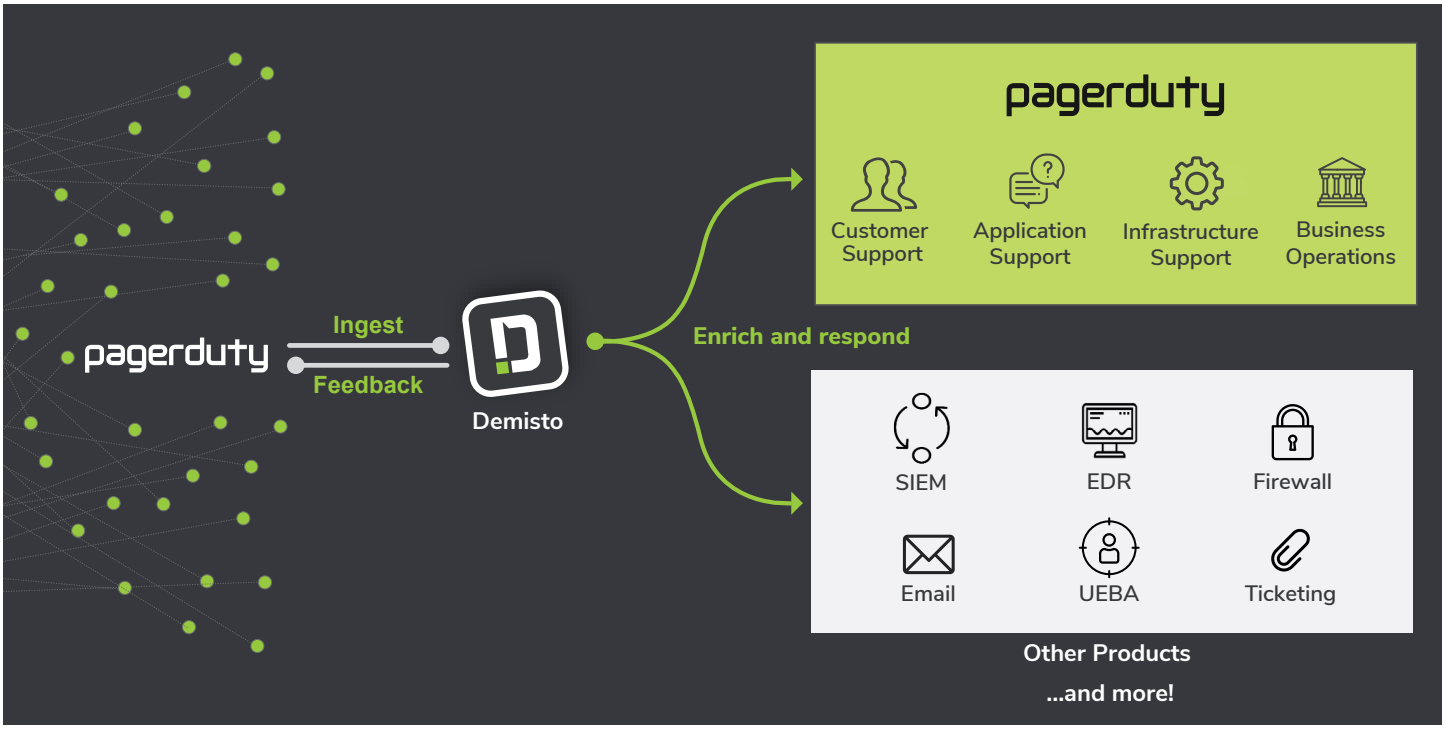
The new age of business and technology is marked by rapid product development and personalized user experiences. But these developments have brought with them an expanded threat landscape and a set of security hurdles to overcome.

From an incident response standpoint, security teams and IT teams are usually isolated, leading to console-switching, repetitive manual actions, and a lack of visibility during incidents that require joint response. From a DevSecOps point of view, it's also tough to reconcile traditional security measures with the agile, proactive, and iterative nature of DevSecOps processes.

To meet these challenges, Demisto integrates with PagerDuty to provide automated digital operations management and central incident oversight across security and IT teams.

Integration features:

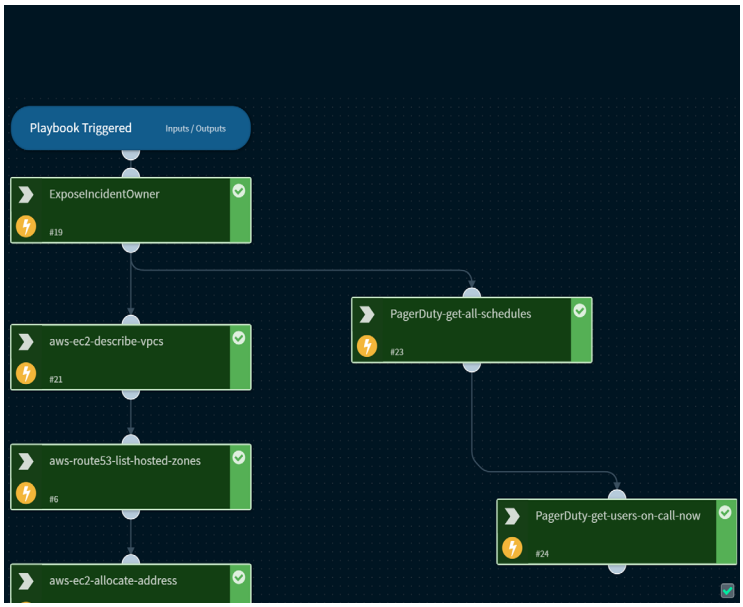
- Automate ingestion of PagerDuty events within Demisto for playbook-driven enrichment and response.
- Submit and resolve PagerDuty events from within Demisto, either as an automated task or in real-time.
- Get call schedules, users on call, contact methods, and notification details from PagerDuty within Demisto for improved incident oversight and cross-departmental coordination.
- Leverage hundreds of Demisto product integrations to further enrich PagerDuty events and coordinate response across security and IT functions.
- Run thousands of commands (including for PagerDuty) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



USE CASE #1 AUTOMATED AND COORDINATED INCIDENT RESPONSE ACROSS SECURITY AND IT TEAMS

Challenge: IT and security incident response usually have different definitions, processes, and escalation patterns, resulting in both teams working in isolation. This creates issues in enforcement and response to threats that concern both security and IT teams. Internal processes and lack of critical knowledge sharing prevents unified incident handling, leading to information asymmetry across teams, piecemeal processes, and a lack of accountability.

Solution: Teams can use the bidirectional integration between PagerDuty and Demisto to access IT events that need security participation and vice versa. To illustrate one of the two alternatives, PagerDuty event data can be ingested into Demisto to trigger standardized and automatable playbooks. These playbooks can enrich the event with more details from PagerDuty as well as coordinate actions across other products to gather wider context without the need for screen switching and manual repetition.



For example, if security and IT teams need to coordinate response to a cloud security incident, a Demisto playbook could query PagerDuty to get scheduling data and access the list of users on call while also gathering intelligence from AWS tools in parallel.

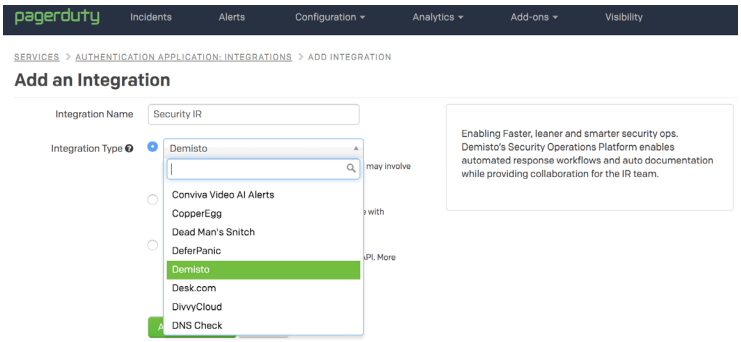
Within PagerDuty, users can leverage defined rule-sets to notify specific personas depending on incident severity and context. For example, while handling a breach notification process, users can notify on-call IT team members, legal advisors, and representatives from the executive team respectively.

Benefit: Leveraging PagerDuty's personnel management and scheduling along with actions from other products through a common playbook helps unify response processes across security and IT teams. Playbooks also minimizing screen switching, manual reconciliation of data, and repetitive work for security teams.

USE CASE #2 ENABLING AGILE SECURITY WITHIN A DEVSECOPS TOOL STACK

Challenge: Organizations with a DevSecOps mindset are defined by agile product development, rapid cross-team collaboration, and quick iteration on a security front. Weaving security into the entire product lifecycle puts the onus on teams to be proactive, work together, and ensure that their tool stack displays robust interconnectivity. Organizations on a DevSecOps journey will need to prevent isolated tools, teams, and processes.

Solution: Demisto's security orchestration combined with PagerDuty's granular escalation features provides a vital connective layer across the vast number of tools that are used within DevSecOps. Demisto playbooks utilizing PagerDuty actions can ensure rapid enforcement across tools while also alerting the appropriate team members for further investigation.



For example, a playbook can be triggered due to vulnerabilities detected by a vulnerability management tool. This playbook can automate deprovisioning of AWS cloud instances, close vulnerable ports if required, and leverage PagerDuty to inform the personnel on-call to take over.

Benefit: DevSecOps is a journey without an end-state, and Demisto's integration with PagerDuty provides teams with the agility, cross-team visibility, and standardized response to security issues to continue that journey with confidence.

About PagerDuty

PagerDuty is the leading digital operations management platform for businesses. We empower DevOps, IT operations, support, security, and business leaders to turn any signal into insight and real-time action across any operational use case. When revenue and brand reputation depend on customer satisfaction, PagerDuty helps teams prevent and resolve business-impacting incidents and deliver exceptional digital experiences.

About Demisto

Demisto, a Palo Alto Networks company, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Demisto, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit www.demisto.com.