DEMISTO
A PALO ALTO NETWORKS® COMPANY

PRISMA PUBLIC CLOUD

Automated Cloud Threat Response and Remediation

Benefits

- Correlate alerts across public clouds and on-premise security products.
- Leverage automated workflows for real-time response within an agile cloud environment.
- Standardize incident response processes across hybrid cloud environments.

Compatibility

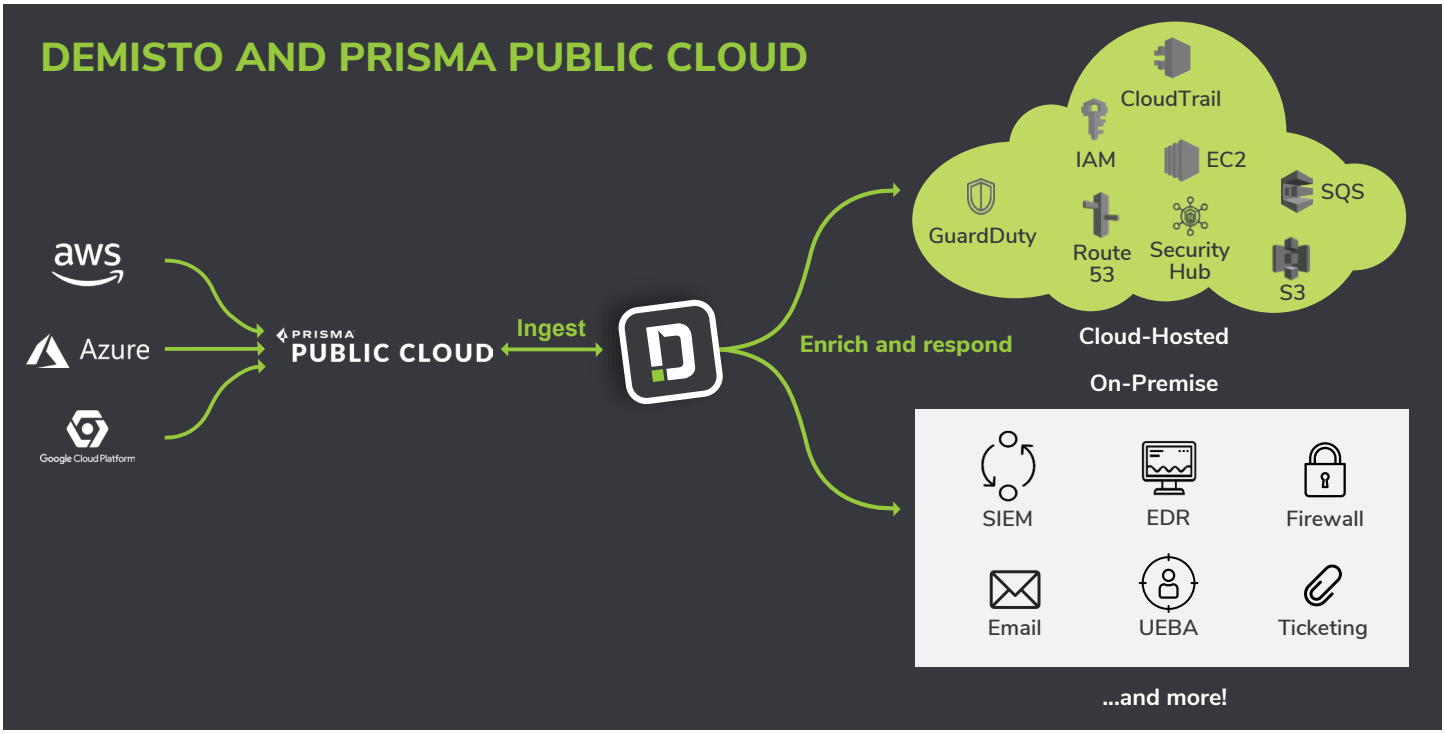
- Products: Demisto Enterprise, Prisma Public Cloud
- Platform: Platform independent

Increased cloud adoption has improved organizational agility, reduced product time-to-market, and leveled the playing field. However, cloud adoption has also expanded the threat surface for organizations, creating disparate ecosystems that hamper visibility into security vulnerabilities across the network. In addition, cloud provisioning and usage is often managed by business units outside the purview of the security team. Security teams need both visibility and agility to keep pace with this dynamic and constantly changing cloud environment.

This integration combines Prisma Public Cloud's comprehensive cloud monitoring and compliance capabilities with Demisto's security orchestration and automation to help security teams unify security functions across cloud and on-premise environments and accelerate detection and response to behavioral anomalies.

Integration features:

- Ingest and enrich Prisma Public Cloud alerts by querying other threat intelligence tools and orchestrating response across cloud and on-premise security products.
- Trigger task-based workflows or playbooks to orchestrate actions across cloud computing platforms and case management products.
- Leverage hundreds of Demisto product integrations to coordinate response across security, DevOps and IT functions.
- Run thousands of commands (including for Prisma Public Cloud) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.

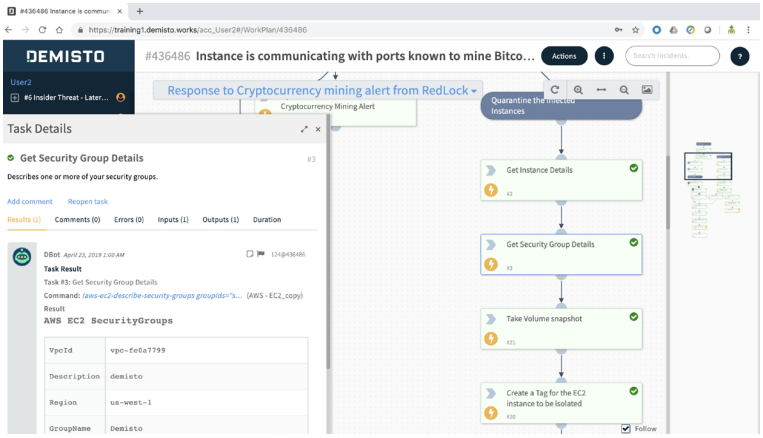


USE CASE #1

AUTOMATED CLOUD SECURITY ALERT INGESTION, ENRICHMENT AND RESPONSE

Challenge: In dynamic cloud environments, visibility and agility are critical to security teams. They need to monitor a broad geographical expanse that covers “shadow IT” and fluid network perimeters. A disconnect between cloud and on-premise environments also hampers security efforts for day-to-day operations and incident response.

Solution: Prisma Public Cloud alerts can be ingested into Demisto and trigger playbooks that further enrich indicator details with threat intelligence correlated from other security product integrations. Alerts indicating malicious behavior such as cryptocurrency mining can also trigger a host of automated incident response actions such as opening tickets, going to the AWS EC2 instance (or GCP or Azure) to check security groups, revoke user access, or quarantine compromised instances. An email notification can also be sent to an analyst for manual review.

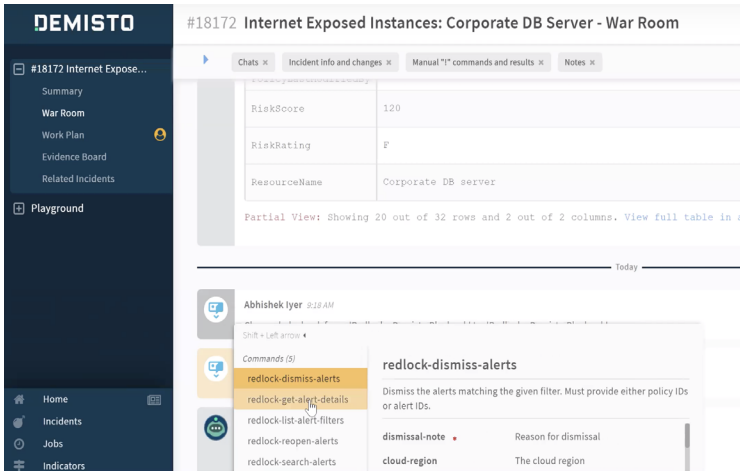


Benefit: The solution will give analysts the visibility to better monitor line-of-business cloud activities. With the help of automated playbooks, repetitive manual tasks are eliminated so analysts can focus on critical threats and reduce their MTTR from hours to minutes.

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

Challenge: While playbooks can automate commonly performed tasks to ease analyst load, an attack investigation usually requires additional tasks to be performed in real-time. Actions such as pivoting from one suspicious indicator to another to gather critical evidence, drawing correlations between incidents, and finalizing resolution result in analysts constantly switching between systems and consoles throughout the investigation lifecycle. This far from seamless experience also makes post-incident reporting an onerous task.

Solution: After running enrichment playbooks, analysts can review task details and run security commands from other security tools in real-time within the Demisto War Room for end-to-end investigation. Keys pieces of data can be tagged as evidence for future review. The War Room documents all analyst actions and suggest the most effective analysts and command-sets over time. A Chatbot interface facilitates cross-functional collaboration so security teams are better aligned with DevOps and business owners to fix vulnerabilities early as they happen versus remediating after the fact.



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 Palo Alto Networks Prisma Public Cloud

Prisma Public Cloud provides continuous visibility, security, and compliance monitoring across public multi-cloud deployments. Powered by machine learning, it correlates data and assesses risk across the cloud environment. Starting today, customers can further reduce their attack surface with two new free services; a vulnerability scanning service and an infrastructure-as-code template scanning service. Find out more about Prisma Public Cloud at https://www.paloaltonetworks.com/cloud-security.

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.