DEMISTO | luminate

Automated Cloud Access Management and Incident Response

Benefits

- Automate ingestion of Luminate alerts within Demisto for playbook-driven response.
- Further enhance Luminate's enforcement capabilities with intelligence from other security tools via Demisto's orchestration.
- Improve analyst efficiency by centralizing collaboration, investigation, and documentation, leveraging Luminate's unique audit trail of users' actions across all applications
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

- Products: Demisto Enterprise, Luminate Secure Access Cloud™

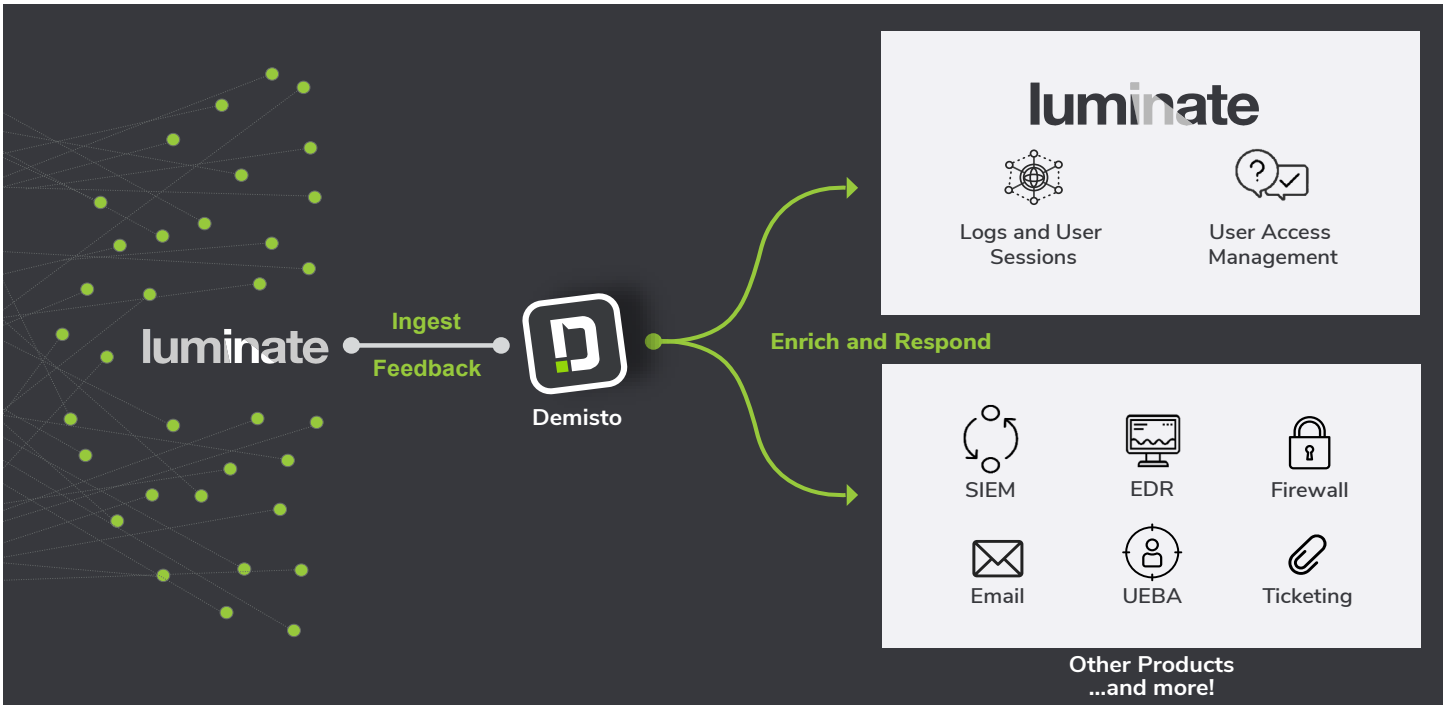
Cloud adoption has heralded a new age of business and technology, as organizations share compute, storage, and infrastructure resources to innovate and scale. But these developments have brought with them their own set of security hurdles to overcome.

From an incident response standpoint, cloud security data and processes are often isolated from traditional security measures, requiring multiple consoles to manage overall security posture. The disparate environments resulting from rapid cloud provisioning and multiple cloud security products also leads to a lack of visibility. It's also tough to reconcile traditional security access and compliance policies with the agile and globally dispersed nature of cloud applications and users.

To meet these challenges, Demisto integrates with Luminate's Secure Access Cloud™ to provide cloud compliance enforcement and incident response across cloud and on-premise infrastructures.

Integration features

- Receive incident data from Luminate within Demisto and trigger automated playbooks tied to those incidents.
- Block and unblock corporate user or contractor access through Luminate from within Demisto, either as automated playbook tasks or in real-time.
- Get Luminate's unique SSH, RDP and HTTP access logs within Demisto for further investigation and incident enrichment.
- Leverage hundreds of Demisto product integrations to further enrich IntSights 'digital footprint' intelligence and coordinate response across security functions.
- Run thousands of commands (including for Luminate) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



USE CASE #1 AUTOMATED ENRICHMENT OF AND RESPONSE TO CLOUD SECURITY INCIDENTS

Challenge: If cloud security consoles are isolated from other functions such as EDR, malware analysis, and threat intelligence, it becomes time-consuming and repetitive for security analysts to cross-reference alerts from cloud security tools, get further context, and coordinate containment and response. Processes diverge depending on the analyst that handles the incident, and this leads to differing response quality.

Solution: Security teams can use the Luminate integration to ingest incident data into Demisto and trigger standardized, automated playbooks for responding to each incident. These playbooks can enrich the alert with more details from Luminate as well as coordinate actions across other products to extract wider context without the need for screen switching and manual repetition.

For example, a playbook could query Luminate for HTTP and SSH access logs data, cross-reference that data with intelligence from SIEMs and treat intelligence tools, and query Luminate again to respond by blocking affected users' access to all sensitive applications, whether on-premise or in the cloud.

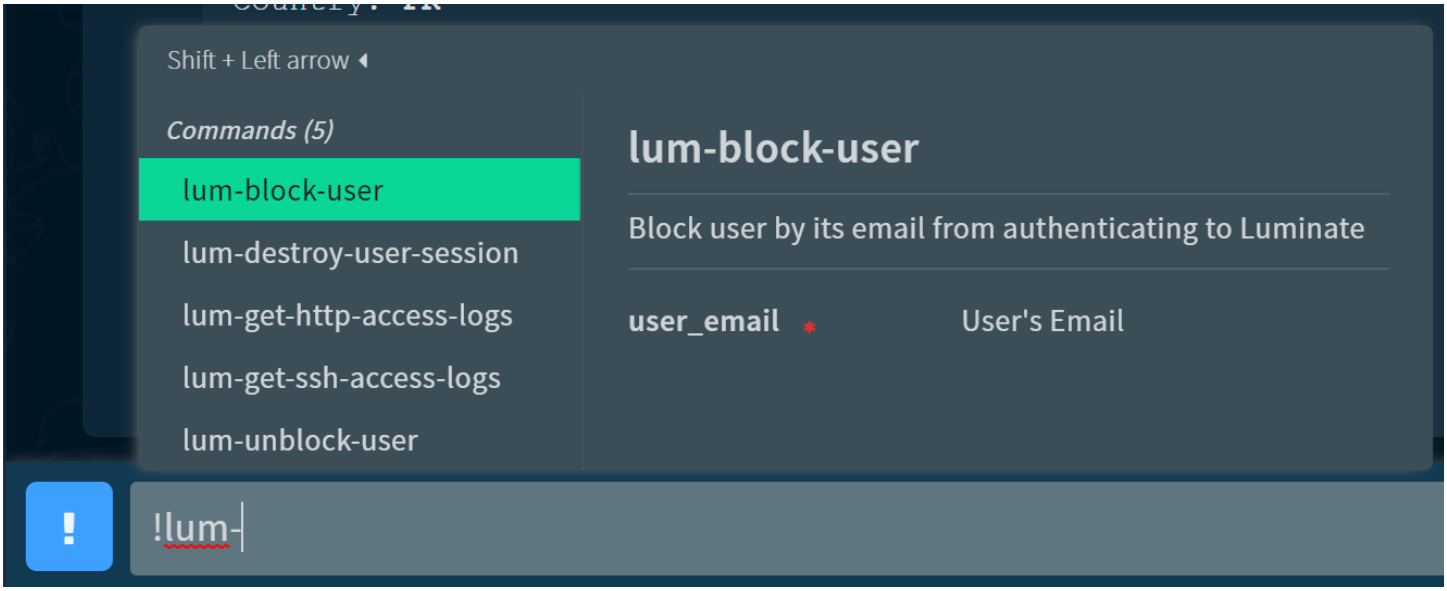
Benefit: Leveraging Luminate's unique audit trail of users' actions along with data from other products through a common Demisto playbook helps minimize screen switching, manual reconciliation of data, and repetitive work for security teams. Unifying and automating response processes across cloud and on-premise infrastructures also helps security teams gain central oversight and coordinate actions at scale.

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

Challenge: Standardized processes are not enough for responding to every security alert. 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. In a cloud-first world that's driven by agility, these lost seconds are precious.

Solution: After running enrichment playbooks, analysts can gain greater visibility and new actionable information about the attack by running Luminate commands in the Demisto War Room. For example, if incident data is ingested from Luminate into Demisto, analysts can run commands such as **lum-get-http-access-logs** and **lum-get-ssh-access-logs** to get more information about the alert in real-time. 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 Luminate

Luminate enables security and IT teams to create Zero Trust Application Access architecture without traditional VPN appliances. Its Secure Access Cloud™ securely connects any user from any device, anywhere in the world to corporate applications, on-premises and in the cloud, while all other corporate resources are cloaked without granting access to the entire network. This prevents any lateral movements to other network resources while eliminating the risk of network-based attacks. Deployed in less than five minutes, Luminate's Secure Access Cloud™ is agentless, and provides full visibility of users' actions as they access corporate resources, as well as real-time governance of these resources. To learn more, visit www.luminate.io or email info@luminate.io.

About Demisto

Demisto 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. Our orchestration engine coordinates and automates tasks across 100s of partner products, resulting in an increased return on existing security investments. Demisto enables security teams to reduce Mean Time to Response (MTTR), create consistent incident management processes, and increase analyst productivity. For more information, visit www.demisto.com or email info@demisto.com.