Mandiant

VARIABLES USED IN INTEGRATION QUERIES

This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview** (https://docs.mandiant.com/home/msv-integrations-overview).

The following table contains a list of Security Validation-provided variables that can be used in queries, and the type of queries where they can be used, if the integration supports that type of query.

Some integrations have special queries. For example, Splunk has a correlation query and Cisco Firepower has a file query and an Amp query. Rather than list these integration-specific queries separately, they are combined in one column.

TIP: If the integration in the platform doesn't have the query type indicated, you can't use that variable in a query. For example, %DOMAINS% can only be used by integrations that have a Malicious DNS Action Query.

	Query Type				
Variable	**General**	**Malicious DNS Action**	**Email Action**	**Host CLI**	Integration-specific
%DOMAINS%		✔			
%HOST_CLI_ACTOR_HOSTNAMES%				✔	
%ACTOR_IPS%	✔				✔
%END_TIME%	✔	✔	✔	✔	✔
%HOST_CLI_ACTOR_IPS%				✔	
%LAST_INDEX% (Splunk / Splunk ES)	✔	✔	✔	✔	✔
%RECIPIENTS%			✔		
%SENDERS%			✔		
%START_TIME%	✔	✔	✔	✔	✔