EXPANSE

Splunk Use Cases for Alerting | Expanse Technical Add-On

Use Cases Relevant to Alerting

Determine Risky Behavior Flows	
Description	*Returns risky flows to/from internal and external IPs based on a specified Behavior rule. In this example, we'll just alert on Tor traffic.*
Query	`index="<BEHVAIOR_INDEX_NAME>" eventtype=Expanse riskRule.name="Connections to Tor"`
Comments	Flow data will include information about the reason the communication was risky, the internal and external IPs and ports, and the internal domains associated with the IP. Expanse recommends setting up a single email event for this query per rule in order to avoid an excessive number of alerts.

New Critical Issue Appearance on Network Perimeter (On-Prem and Cloud)	
Description	*Returns all new Critical exposures for On-prem and Cloud.*
Query	`index="<ISSUE_INDEX_NAME>" eventtype="Expanse" severity="Critical" activityStatus="Active" value="Active"`
Comments	Different assets/exposure types may require varying paths for remediation. If you'd like to filter alerts further to only pertain specific issue types you can do so by filtering on the `description` field.

Certificate Expiration Compliance	
Description	*Tracks certificates observed by Expanse to enable proactive compliance with existing company policies.*

Query	`| inputlookup certificatescollection_lookup`
	`| eval expTime=strptime('certificate.validNotAfter',"%Y-%m-%dT%H:%M:%SZ")`
	`| eval yesterdayTS=relative_time(now(), "-1d@d")`
	`| eval nowTS=now()`
	`| where (expTime >= yesterdayTS AND expTime <= nowTS)`

Comments	Returns all certificates that expired in the last day. You can modify the expiration time frame to fit your desired warning interval.