Useful Smartlog Queries

Generic Queries

Research	SmartLog Query
Search for E-Mail Subject Note: Search without quotation marks and wildcard works for email_subject	*email_subject:*TEXT**
Application Control Proxy Log	*blade:"Application Control" AND appi_name:"Web Surfen" AND *part-of-hostname**
Every logs of a specific rule	*{ABC12345-ABC1-ABC1-ABC1-ABC123ABC12}*
Security Management Log Server : when logs were not able to be sent to it	*"were not sent to log server"*
Filter Logs by Geo-Location	*src_country:"Germany" AND src:<ip-address>*
Alert on GW	*type:Alert AND origin:<fw-gwname>*
FW Control Messages (Failover etc.)	*type:Control*
ClusterXL Control Messages, Cluster Switch over Messages	*type:Control ClusterXL*
DHCP Messages	*service:dhcp*
Address Spoofing	*address spoofing*
Find aggressive aging events	*aggressive aging*
Any TCP state errors listed in [sk101221](#)	*tcp (fin OR syn) NOT "both fin" NOT "established"* In the query field, type "*tcp state*" (without quotes) or any relevant text (e.g., "*syn_sent*", "*both fin*")
Global Broadcast	*dst:255.255.255.255*
HTTPS Inspection CRL or OCSP errors	*blade:"HTTPS Inspection" crl OR ocsp*
Certificates: any alert regarding crl (Certification Revocation List) or certificates (see [sk104400](#)for more details)	*type:alert (certificate or CRL)*
Potential network configuration problem messages in log - See [SK63160](#)	*"Engine Settings - TCP"*
IPS Bypass Messages See discussion here: [Checkmates: IPS bypass](#)	*blade:IPS NOT(action: (prevent OR block)) OR "IPS Bypass Engaged" OR "IPS Bypass Disengaged"*

Threat Extraction / Emulation

Research	SmartLog Query
Threat Extraction	*blade:"Threat Extraction" AND action:Extract*
Threat Extraction Search for E-Mail Subject	*blade:"Threat Extraction" OR blade:"Threat Emulation" AND email_subject:" TTTTT" OR email_subject:"TTTTT"*
Threat Extraction show last activity	*blade:"Threat Extraction" AND "Content Removal" OR "Conversion to PDF"*
Threat Emulation show errors	*blade:"Threat Emulation" *"ended with verdict Error"**
Threat Emulation show found threats	*blade:"Threat Emulation" AND severity:Critical NOT type:Correlated*

Endpoint Security & Remote Access

Research	SmartLog Query
Seeing tunnels activities	*tunnel_test or action:"Key Install" or action:"Failed Log In" OR action:"Log In" OR action:"Log Out" OR action:reject OR action:Update*
Connection Errors	*blade:vpn AND action:Reject ("endpoint" OR "user" OR "Office Mode")*
Errors Authenticating Users	*"Could not obtain user object" "IKE failure"*

Revision #8
Created 20 October 2020 13:55:08
Updated 13 September 2023 08:48:46 by Peter Baumann