

# Useful Smartlog Queries

## Generic Queries

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

# Threat Extraction / Emulation

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

# Endpoint Security & Remote Access

| Research                    | SmartLog Query   |
|-----------------------------|--|
| Seeing tunnels activities   | <b><i>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</i></b> |
| Connection Errors           | <b><i>blade:vpn AND action:Reject ( "endpoint" OR "user" OR "Office Mode" )</i></b>  |
| Errors Authenticating Users | <b><i>"Could not obtain user object" "IKE failure"</i></b>   |

Revision #8

Created 20 October 2020 13:55:08

Updated 13 September 2023 08:48:46 by Peter Baumann