Sysmon × Splunk: Six Short Detections

Author : Vlassov Vladislav | Date: 08.20.2025

Each section: SPL, a brief interpretation, and the original result screenshot from the provided file.

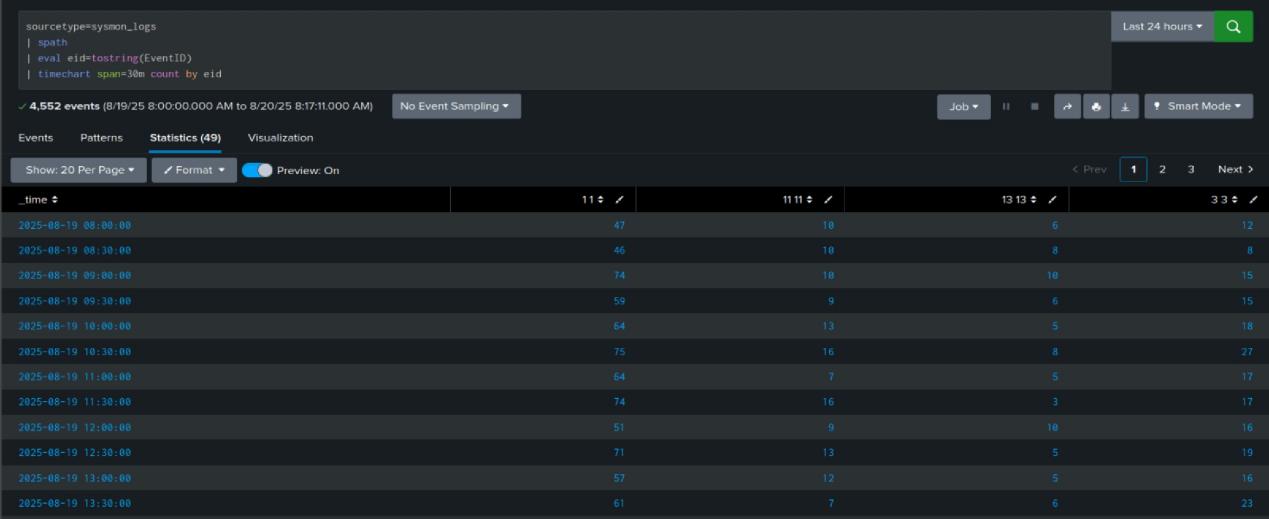
# 1. Baseline and EventID Trends

SPL:

sourcetype=sysmon\_logs | spath | eval eid=tostring(EventID) | timechart span=30m count by eid

Analysis: Focus on anomalies by host, parent-child, frequency, and egress. Validate against maintenance windows.

Conclusion: Flag unusual process behavior or network patterns for triage.



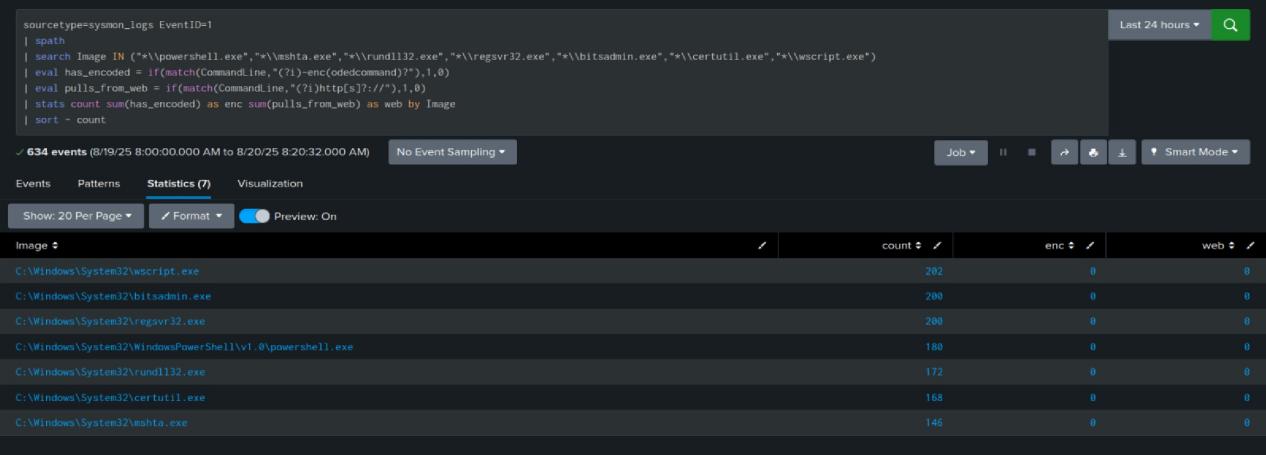
# 2. LOLBin and Suspicious Commands

SPL:

sourcetype=sysmon\_logs EventID=1 | spath | search Image IN ("\*\\powershell.exe","\*\\mshta.exe","\*\\rundll32.exe","\*\\regsvr32.exe","\*\\bitsadmin.exe","\*\\certutil.exe","\*\\wscript.exe") | eval has\_encoded = if(match(CommandLine,"(?i)-enc(odedcommand)?"),1,0) | eval pulls\_from\_web = if(match(CommandLine,"(?i)http[s]?://"),1,0) | stats count sum(has\_encoded) as enc sum(pulls\_from\_web) as web by Image | sort - count

Analysis: Focus on anomalies by host, parent-child, frequency, and egress. Validate against maintenance windows.

Conclusion: Flag unusual process behavior or network patterns for triage.



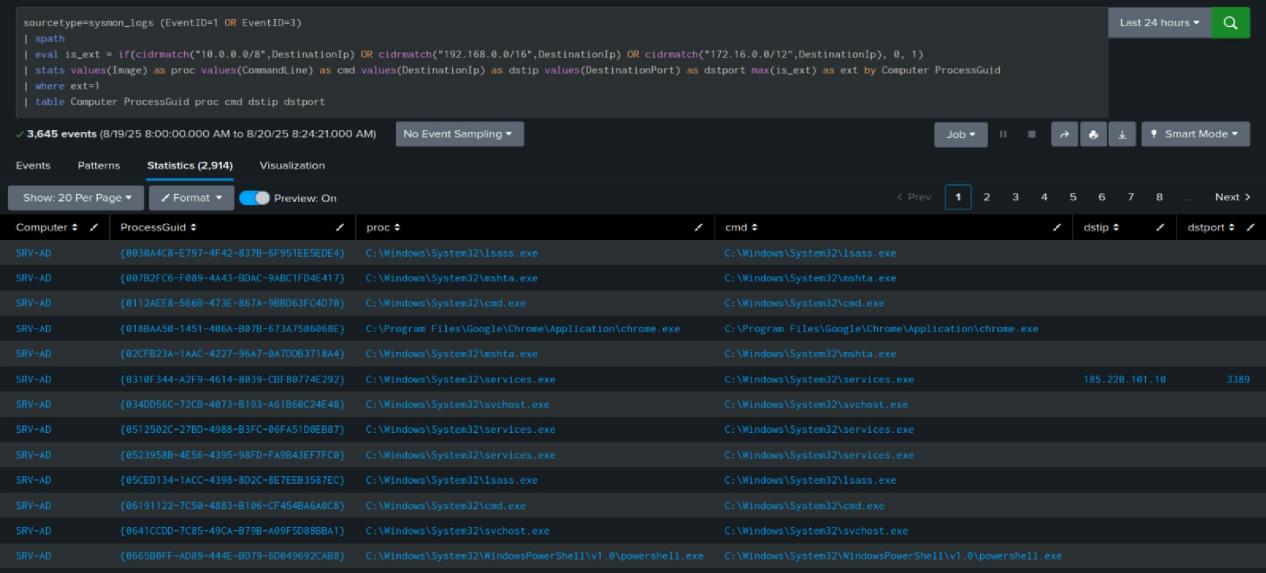
# 3. Outbound Connections by Process

SPL:

sourcetype=sysmon\_logs (EventID=1 OR EventID=3) | spath | eval is\_ext = if(cidrmatch("10.0.0.0/8",DestinationIp) OR cidrmatch("192.168.0.0/16",DestinationIp) OR cidrmatch("172.16.0.0/12",DestinationIp), 0, 1) | stats values(Image) as proc values(CommandLine) as cmd values(DestinationIp) as dstip values(DestinationPort) as dstport max(is\_ext) as ext by Computer ProcessGuid | where ext=1 | table Computer ProcessGuid proc cmd dstip dstport

Analysis: Focus on anomalies by host, parent-child, frequency, and egress. Validate against maintenance windows.

Conclusion: Flag unusual process behavior or network patterns for triage.



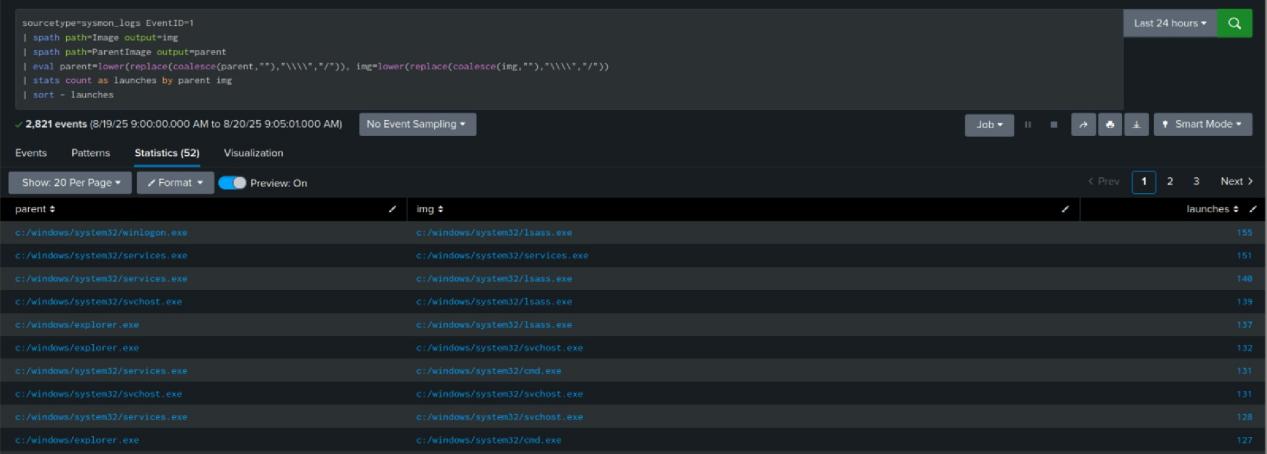
# 4. Parent–Child Process Outliers

SPL:

sourcetype=sysmon\_logs EventID=1 | spath path=Image output=img | spath path=ParentImage output=parent | eval parent=lower(replace(coalesce(parent,""),"\\\\","/")), img=lower(replace(coalesce(img,""),"\\\\","/")) | stats count as launches by parent img | sort - launches

Analysis: Focus on anomalies by host, parent-child, frequency, and egress. Validate against maintenance windows.

Conclusion: Flag unusual process behavior or network patterns for triage.



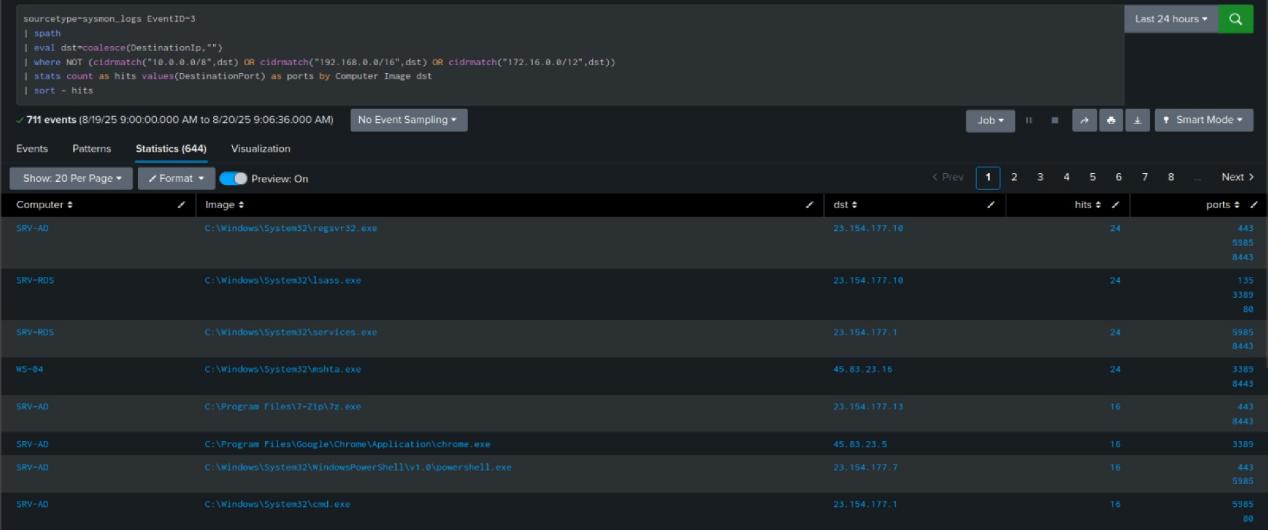
# 5. Public IP Beacons and Ports

SPL:

sourcetype=sysmon\_logs EventID=3 | spath | eval dst=coalesce(DestinationIp,"") | where NOT (cidrmatch("10.0.0.0/8",dst) OR cidrmatch("192.168.0.0/16",dst) OR cidrmatch("172.16.0.0/12",dst)) | stats count as hits values(DestinationPort) as ports by Computer Image dst | sort - hits

Analysis: Focus on anomalies by host, parent-child, frequency, and egress. Validate against maintenance windows.

Conclusion: Flag unusual process behavior or network patterns for triage.



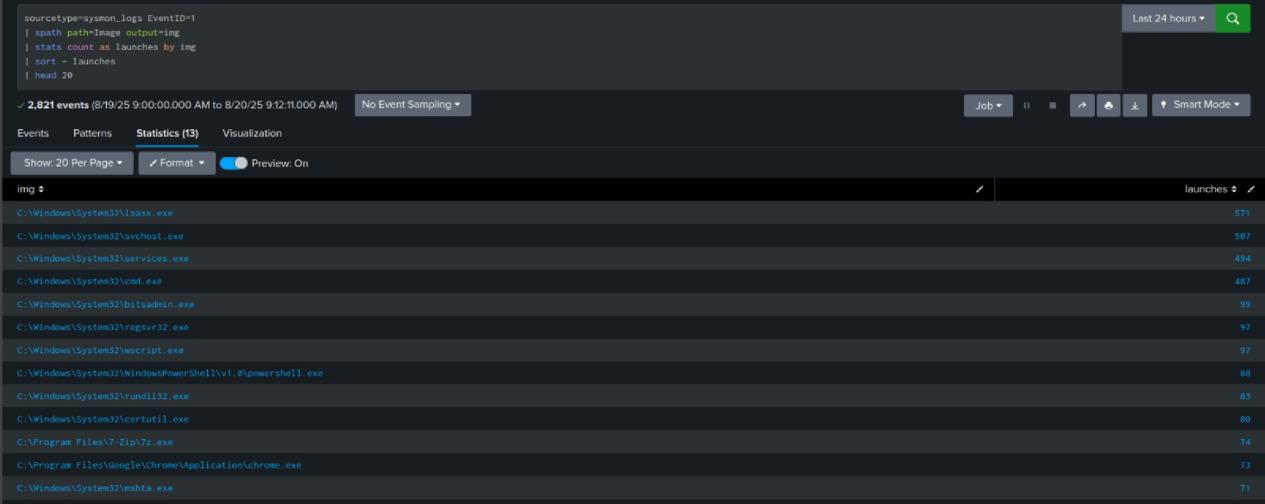
# 6. Top Executables by Launch Count

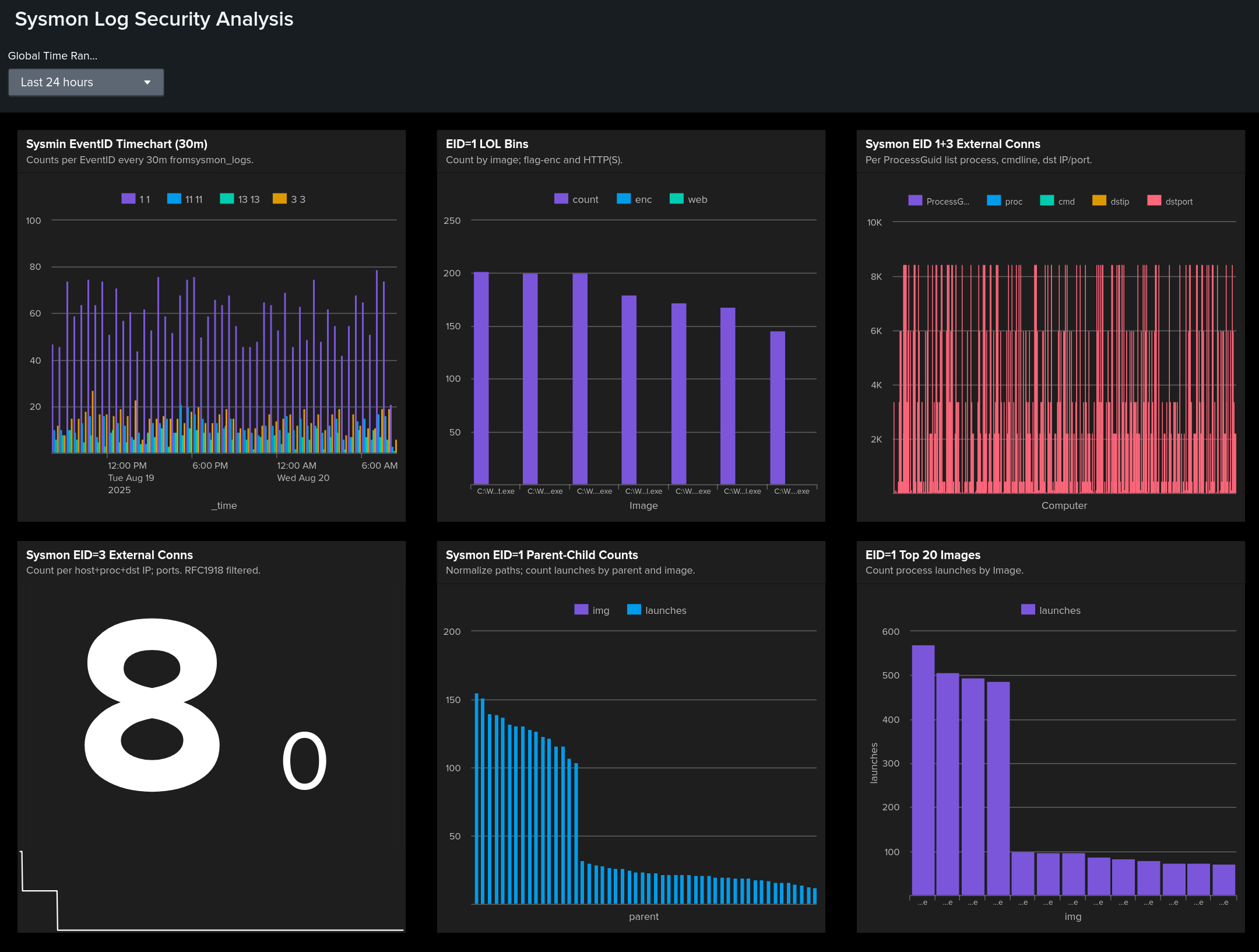
SPL:

sourcetype=sysmon\_logs EventID=1 | spath path=Image output=img | stats count as launches by img | sort - launches | head 20

Analysis: Focus on anomalies by host, parent-child, frequency, and egress. Validate against maintenance windows.

Conclusion: Flag unusual process behavior or network patterns for triage.



**Dashboard Overview — Sysmon Log Security Analysis**  


This dashboard provides a 24-hour view of Sysmon activity. The top row shows EventID trends for baseline anomalies, LOLBin executions with encoded/web flags, and a per-process view of external connections. The bottom row highlights the total count of external conns, uncommon parent→child launch pairs, and the top executables by launch volume. Investigate spikes, rare parent–child chains, and processes egressing to public IPs; pivot to host, command line, and destination context for triage.

Figure: Sysmon Log Security Analysis dashboard (last 24 hours).

**Overall Analysis:**  
The six detections give layered coverage across execution, abuse of signed binaries, parent–child outliers, and egress. Baselines expose spikes in EventIDs and process frequency. LOLBins with encoded commands or web pulls are highest risk. Uncommon processes talking to public IPs and repeated beacons are strong C2 signals. Findings need enrichment with DNS, WHOIS, hashes, and parent trees to reach confidence.