Log Sources v1.1 12/2023

Log Source	Volume[9]	IOC Matching	Threat Hunting	Audit Trail[7]	APT Detection[8]
Antivirus	Low	-	++[3]	+	+++
Windows & Sysmon	Medium[6]	++[1]	+++[4]	++	++
Cloud	Medium	+	+	+++	+
Proxy	Medium	++[2]	+[5]	++	+
IdP	Medium	-	+	+++	+[10]
NIDS/NSM	Medium	+[2]	+	+	+
DNS	High	++[2]	+[5]	+	+
Linux (auditd)[12]	Medium	+	+	++	+
Mail[6]	Medium	+	-	+	-
Firewall	High	+[2]	-	++	-

1 – E.g. File hash values (MD5, SHA1, SHA256), file names, C2 IPs, Mutex values
2 – C2 IP addresses or domain names in the logs
3 – see „Antivirus Event Analysis Cheat Sheet" for detailed information https://www.nextron-systems.com/?s=antivirus
4 – Sigma rules can help make sense out of the log data https://sigmahq.io/
5 – Patterns (URL, hostname), suspicious TLDs
6 – Volume depends on audit policy (use Microsoft Baseline) and Sysmon configuration

7 – Audit Trail is useful for reconstructing events
8 – APT Detection assesses log utility in identifying persistent threats (reconnaissance, backdoors, lateral movement)
9 – Log volume is primarily dependent on the utilized audit policy, hence it is a rough estimate
10 – With deception technology – honey tokens / credentials
11 – Identity Providers like Okta, Entra, Ping, JumpCloud, etc
12 – Laurel improves the usability a lot with concatenated command lines https://github.com/threathunters-io/laurel