Detection rules to actively monitor existing and new variants of attack against the log4j vulnerability

Policy name	Functionality	Last Updated
Possible CVE-2021-44228 Exploitation Attempt Accountname Analytic	Web Server, Web Proxy, Web Application Firewall, Next Generation Firewall,Authentication / SSO / Single Sign-On, Cloud Authentication / SSO / Single Sign-On, Cloud Services / Applications, Authentication / VPN,	**NEW**
Possible CVE-2021-44228 Exploitation Attempt UserAgent Analytic	Web Server,Web Proxy,Web Application Firewall,Next Generation Firewall, Authentication / SSO / Single Sign-On,Cloud Services / Applications,Authentication / VPN, Cloud Authentication / SSO / Single Sign-On	**Updated Dec 21st for** additiaonl functionalities
Possible Cryptocurrency Mining CommandLine Analytic	Unix / Linux / AIX	**NEW**
Possible CVE-2021-44228 Exploitation Attempt URI Analytic	Web Server, Web Proxy, Web Application Firewall, Next Generation Firewall	Dec 20th
Possible CVE-2021-44228 Exploitation - Unusual Download Attempt From Log4j Logging Server Analytic	Web Server,Web Proxy,Web Application Firewall,Next Generation Firewall	Dec 16th
Network Application Port Mismatch Analytic	Web Proxy, Next Generation Firewall	Dec 16th
Potential Privilege Escalation SamAccountName Spoofing Analytic	Microsoft Windows	Dec 16th
Possible CVE-2021-44228 Exploitation - Unusual LDAPs Network Connection From Java Application	Endpoint Management Systems, Unix / Linux / AIX	Dec 18th
Log4j related signature detection	IDS-IPS, EDR, Cloud EDR, Web Application Firewall	Dec 16th
Unusual Download Attempt From Log4j Logging Server	Web Proxy, Next Generation Firewall	Dec 18th