NETWORK SECURITY MONITORING VS. LOG SECURITY MONITORING

SKOUT CYBERSECURITY

SCOPING RESOURCE

	NETWORK SECURITY MONITORING	LOG SECURITY MONITORING
SIEM analysis	✓	✓
AI analytics engine	✓	✓
Behavior analysis	✓	✓
24x7 Security Operations Center access and monitoring	✓	✓
24x7 SOC-as-a-service	✓	✓
Unlimited devices per user, per site	✓	✓
Physical or virtual deployment	✓	✓
Multi-tenant dashboard view	✓	✓
Self-service reporting	✓	✓
Supports customer notification if critical incident	✓	✓
Satisfies key compliance controls (PCI, HIPAA, SOX, etc.)	✓	✓
Collaborative event resolution and remediation	✓	✓
Inspects live network traffic and alerts if IOCs are detected	✓	No
IDS event correlation and incident creation	✓	No
Network packet inspection for IOCs	✓	No
Ingests and Alerts on discovery of IOCs in system and security logs	No	✓
Log parsing and normalization	No	✓
Detects signs of business email compromise	No	Yes, through email SaaS integrations
Detects security risks outside your network	Through incoming and outging traffic	Through log sources
Detects security risks traveling on your network	Through live network traffic inspection	Through network log sources (like firewalls or IDS devices)
Detects signs of ransomware	Through incoming and outgoing traffic	Through logs

Use Cases

NETWORK SECURITY MONITORING		LOG SECURITY MONITORING	
Denial of Service (DoS) Attacks	Identifying unusual traffic from organization-owned IoT devices, which might be leveraged by an attacker to perform an attack.	*Access Control*	Monitoring who is accessing devices and where they connect to, and alert when source or target is unknown or suspicious.
Dataflow Monitoring	Many devices communicate over unencrypted protocols and can be used as a vehicle to transfer sensitive data. Network Security Monitoring can monitor unusual data flows to and from devices and alert security staff.	*Detecting Compromised User Credentials*	Log Monitoring can use behavioral analysis to detect anomalous behavior by users, indicating a compromise. For example, logins at unusual hours or at unusual frequency.
FTP and Cloud Storage	Monitoring network traffic over protocols that facilitate large data transfer, and alerting when unusual quantities or file types are being transferred, or when the target is unknown or malicious.	*Anomalous Privilege Escalation*	Log Monitoring can detect users changing or escalating privileges for critical systems.
Lateral Movement	Insiders conducting an attack may attempt to switch accounts, machines and IP addresses on their way to a target.	*Third-Party Violations*	Monitoring activity by external vendors and partners who have access to organizational systems, in order to identify anomalous behavior or escalation of privileges.
Command and Control Communication	Network Monitoring can correlate network traffic to discover malware communicating with external attackers. This is a sign of a compromised account.	*Correlating with Existing Products*	Merge data from your existing security tools with multiple sources to provide greater visibility and re-use existing investment.

getskout.com
info@getskout.com