

Continuous Monitoring: Turning Logs Into Ongoing Awareness

Mon, Aug 17, 9:00 AM EDT · <https://scottslab.io/posts/continuous-monitoring-and-analytics>



TL;DR

NIST defines continuous monitoring as maintaining ongoing awareness of vulnerabilities and threats to support risk decisions. Not a quarterly scan, but an always-on program aligned to your risk tolerance, adaptable, and actively managed. It runs a six-step loop (strategy → metrics → automate collection → analyze → respond → review) and leans on four analytics styles: anomaly, trend, behavioral, and availability. Endpoint monitoring and UEBA push it down to individual hosts and users.

Continuous monitoring is what all the logging and correlation is *for*. NIST's definition is worth quoting in spirit: maintaining ongoing awareness of vulnerabilities and threats so you can make informed risk decisions. The key word is ongoing. This isn't a scan you run each quarter and file, it's an always-on picture of where you stand. NIST frames three characteristics that keep it honest: it's aligned to your risk tolerance, it's adaptable as things change, and it has active management involvement, because a monitoring program nobody in charge looks at is just disk usage.

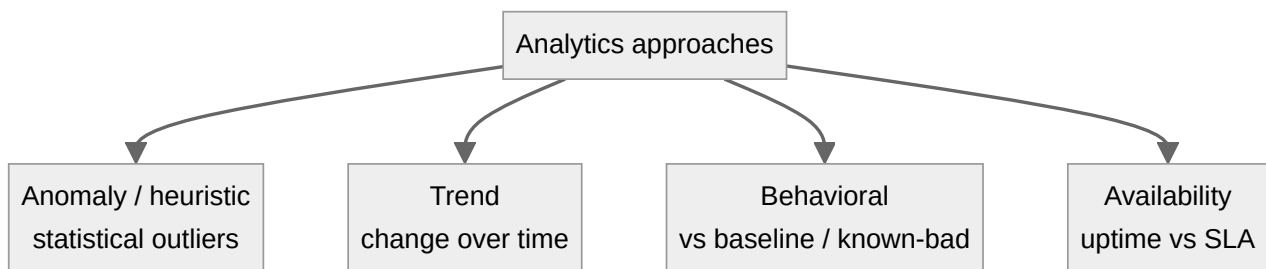
The program runs as a six-step loop. Define a strategy based on your risk tolerance. Establish metrics and how often you'll assess them. Implement automated collection and reporting. Automated, because humans can't sustain "continuous." Analyze and report the findings. Respond

by mitigating, avoiding, transferring, or accepting the risk: the only four things you can ever do with a risk. And review and update the program, because the last step feeds the first.



Continuous Monitoring: Turning Logs Into Ongoing Awareness

The analysis itself comes in four flavors, and good monitoring uses all of them. Anomaly (or heuristic) analysis flags statistical outliers: the bandwidth spike on January 13 that doesn't match any normal day. Trend analysis tracks change over time, and change is a signal in both directions: a sudden *drop* in account compromises is as worth a look as a spike, because it might mean detection broke, not that the attackers went home. Behavioral analysis compares activity against baselines or known-malicious patterns. And availability analysis watches uptime against your SLAs, because "is it even up" is a security question too.



Continuous Monitoring: Turning Logs Into Ongoing Awareness

Two things push this all the way down to the edges. Endpoint monitoring treats processor, memory, and file-system activity as security indicators: a process pinning the CPU or a sudden burst of file changes is often the first sign of ransomware. It folds malware protection, OS logs, and file-integrity monitoring back into the SIEM. And UEBA (User and Entity Behavior Analytics) builds machine-learning models of what normal looks like for each user and flags the deviations for an analyst, which is how you catch the compromised account that's authenticating perfectly but behaving like someone else. The whole point, from a single log line up to a UEBA model, is the same: know what normal is, so abnormal has somewhere to show up.