opentext™

WHITE PAPER

Improve threat detection accuracy and SOC efficiency with multi-space analytics

See more. Detect faster. Respond with confidence.



Contents

The threat picture extends beyond your environment	3
Four perspectives answer different questions	4
Three essential perspectives inside the environment	6
Far space adds relevant external adversary context	8
Bring external signals into enterprise investigations	9
A legitimate account conceals an intrusion	10
From corroborated evidence to containment	11
Reduce exposure time through detection and reaction	12
Evolve the SOC around its most important visibility gaps	14
OpenText Multi-Space Analytics Framework	14

The threat picture extends beyond your environment

Security operations teams continually refine enterprise monitoring, correlation rules, behavioral detection, and log investigation. These investments improve the view of activity inside the organization. Yet, an adversary can develop infrastructure and conduct relevant activity beyond the environment that those tools observe. Further optimization of internal telemetry alone cannot supply that external perspective.

Multi-space analytics combines near-space telemetry from within the enterprise with relevant far-space telemetry from beyond it. Together, correlation, behavioral analytics, log investigation, and internet signal analytics provide complementary views of threats. These views inform one another, helping analysts connect observed activity with adversary context and build a better-supported basis for detection and response.

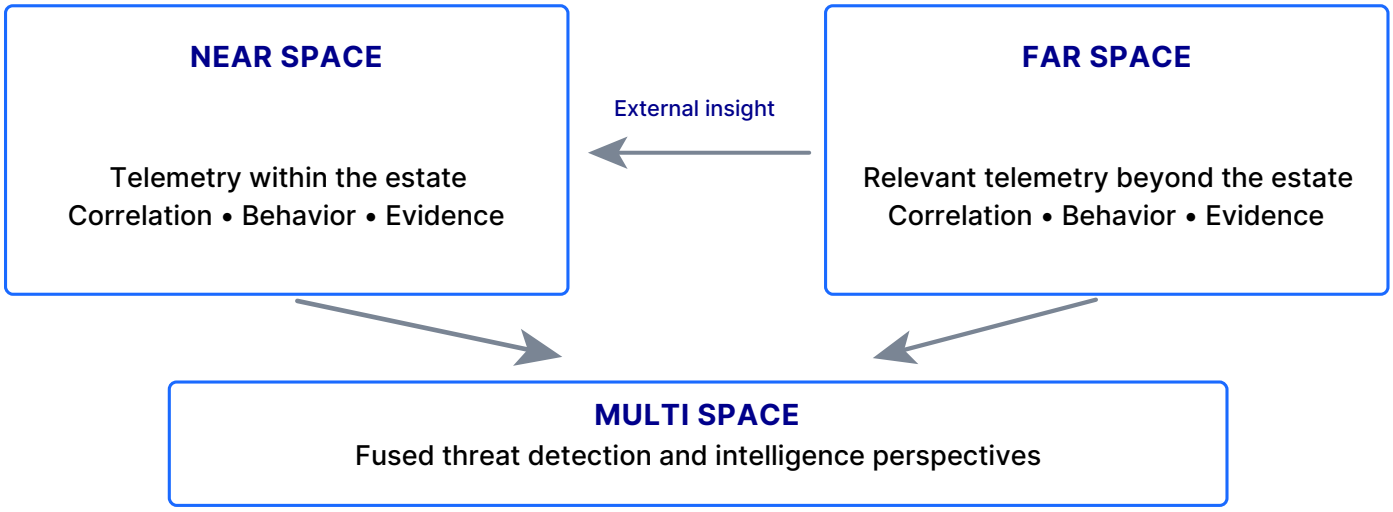


Figure 1 Similar analytic methods applied to different telemetry sources inform a shared threat picture. The fusion concerns threat detection and intelligence perspectives.

For SOC analysts, the practical benefit is more context for deciding what to investigate and how to respond. For security operations leaders, the objective is shorter exposure time through faster actionable detection and a better-informed, effective response. This paper explains the analytic roles, applies them to an illustrative incident, and shows how internal and external perspectives can inform one another.

Four perspectives answer different questions

Different analytic perspectives answer different security questions. The first three views below describe ways to examine enterprise telemetry; internet signal analytics adds the external perspective. Similar methods can operate in both spaces. The distinction between near space and far space is the source and visibility of the telemetry, rather than a separate class of algorithms.

Perspective	Security question	OpenText capability
Real-time correlation	What well-understood suspicious pattern is happening now?	OpenText™ Enterprise Security Manager
Behavioral analytics	What activity is abnormal for this user or entity?	OpenText™ Behavioral Signals
Log analytics	What does the underlying evidence show?	OpenText™ Security Log Analytics
Internet signal analytics	What relevant adversarial activity is occurring outside the enterprise?	OpenText™ Adversary Signals



Recognize familiar patterns and discover unfamiliar behavior

Correlation is strongest when suspicious relationships and sequences are well understood and can be expressed in detection logic. Its coverage becomes more limited when activity falls outside established detection logic. Behavioral analytics surfaces unexpected deviations and supplies context that can inform correlation. The methods cooperate across the threat spectrum.

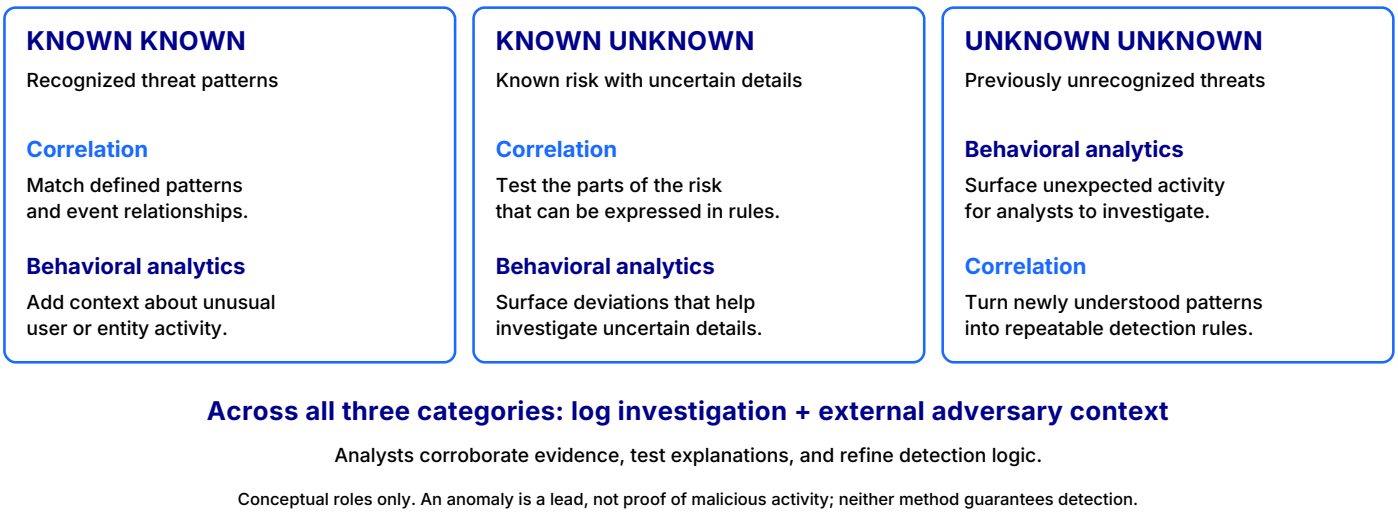


Figure 2 Complementary analytic roles across the threat spectrum. Log investigation and external context support all three categories.

Known-known threats have recognizable patterns. Known-unknown threats involve understood risks whose details remain uncertain. Unknown-unknown threats represent activity the SOC has not yet recognized as a threat. Behavioral AI and machine learning can help discover unexpected activity, while correlation can operationalize understood patterns. Neither method guarantees detection, and an anomaly by itself does not prove malicious intent.

Log evidence and external context remain useful across the spectrum. As analysts learn from an investigation, they can refine rules, hypotheses, and response procedures. This creates a continuing relationship between discovery and repeatable detection.



Three essential perspectives inside the environment

Real-time correlation recognizes meaningful event relationships

An isolated login failure, successful authentication, or administrative action may be routine. A combination of events can justify investigation. OpenText Enterprise Security Manager applies real-time threat analysis leveraging both correlation and simple pattern matching to help analysts recognize suspicious activity as events occur. Its contribution is to identify a meaningful pattern that the SOC has defined as important.

The quality of correlation depends on available telemetry, detection logic, and context. A rule that captures a known technique remains useful when an attacker changes tools. But known actions can also appear in combinations the SOC has not anticipated. As a sequence becomes less familiar, behavioral context and historical evidence help the analyst evaluate what the rules alone cannot explain.

Familiar techniques can form an unfamiliar attack

AI-assisted attacks can chain familiar techniques into a new sequence without requiring a novel exploit at every step. MITRE ATT&CK documents an AI-orchestrated campaign involving reconnaissance, valid-account use, data staging, and exfiltration.[1] Individual techniques may be recognizable while their combination is unfamiliar to the SOC. Correlation remains useful for known elements; behavioral analysis and log investigation help expose the relationship between them.

Behavioral context can inform correlation rules

A behavioral engine can maintain an evolving activity baseline for each user or entity, such as usual working hours. This gives the SOC context for interpreting events without maintaining separate static rules for every entity.

For example, a late-night login may be routine for a shift worker but unusual for a finance employee. When that entity context is available to a correlation rule, it can help determine whether the matched condition warrants an alert and which severity to assign. Analysts can also use it during triage. This illustrates how analytics can inform one another; the exact fields and automated handoff depend on supported integration.

Once investigation validates a previously unfamiliar sequence, analysts can translate what they learned into repeatable correlation logic. The behavioral engine continues to maintain changing entity context, while rules apply the detection conditions the SOC has established.

1 MITRE ATT&CK — *Anthropic AI-orchestrated Campaign*, C0062



Behavioral analytics identifies departures from expected activity

A compromised account may use legitimate credentials and permitted applications. Behavioral analysis asks whether that activity differs from the user's or entity's expected behavior. OpenText Behavioral Signals uses unsupervised machine learning to identify anomalies and generate prioritized threat leads. This provides an investigative starting point for activity that may not fit predefined detection logic.

How unsupervised machine learning supports detection

Here, AI means machine learning that analyzes observed behavior to identify patterns and deviations. It does not mean asking a generative large language model to write an answer. Unsupervised learning works with data that has not been labeled in advance as benign or malicious. It can identify unusual activity without requiring a labeled example of the exact attack. The output is an investigative lead, not a verdict.

OpenText Behavioral Signals specifically uses online unsupervised models that learn from incoming activity and adapt their baselines as the environment evolves. This reduces reliance on separate manual retraining to keep behavioral context current.

An unusual action can also have a legitimate explanation, such as a changed job responsibility or approved maintenance. Analysts must interpret a behavioral lead using surrounding evidence. This is where correlation and historical investigation help distinguish a meaningful security concern from a benign deviation.

Log analytics turns a lead into an evidence-based investigation

Once an analyst has a hypothesis, the next task is to establish what happened. OpenText Security Log Analytics supports log analysis and hypothesis-driven threat hunting through search and query capabilities. Analysts can examine relevant records, reconstruct the sequence, identify related activity, and assess the scope supported by the retained telemetry.

Historical evidence can support or challenge an alert. It can show whether a new destination appeared previously, whether additional accounts followed a similar pattern, or whether a suspected action was part of an approved process. Visibility remains bound by the sources collected and their retention. Missing logs are an evidence gap, not proof that an action did not occur.

Internal optimization still has a visibility boundary

Together, these three perspectives produce a richer view of enterprise activity. They remain dependent on what the organization can observe. An external infrastructure relationship or adversary activity beyond that view requires relevant outside-in evidence. Far-space analytics adds that dimension without replacing the internal methods already used by the SOC.

Far space adds relevant external adversary context

OpenText Adversary Signals analyzes malicious internet activity beyond organizational boundaries. This outside-in view supplies context the enterprise's own event records cannot independently provide. Relevance to an asset, destination, or investigation determines its value to the SOC.

Correlation, behavioral analysis, and examination of event history can be applied to both near-space and far-space telemetry, extending the evidence available beyond the enterprise's own visibility.

An external signal does not establish an internal compromise. Analysts connect it to enterprise activity, check timing and infrastructure relationships, and test whether it supports the incident hypothesis. Internal evidence helps establish whether the external lead matters to the organization.

Fuse internal and external threat perspectives

Multi-space analytics combines threat detection and threat intelligence perspectives from inside and outside the estate. External context helps analysts interpret internal activity, while internal evidence helps determine whether an external lead is relevant.

An investigation can begin with any lens. A correlated event can prompt a review of account behavior and external destinations. A behavioral lead can trigger historical searches. An external signal can prompt an internal hunt. A log-based discovery can lead analysts to check current correlated activity. The order follows the available evidence; it is not a mandatory four-stage pipeline.



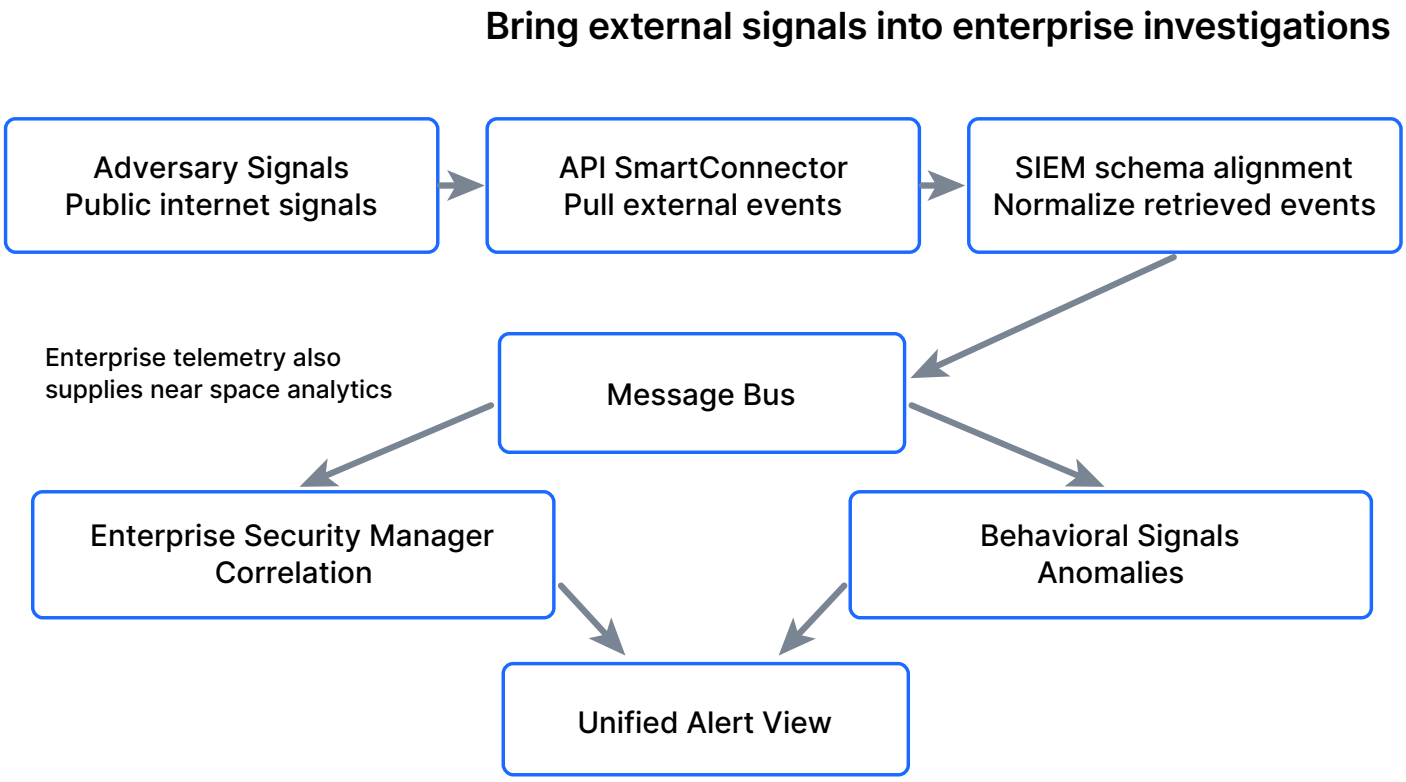


Figure 3 Conceptual integration flow connecting external adversary signals with enterprise detection and investigation. Deployment options depend on the supported product versions and configuration.

Figure 3 illustrates an integration approach in which an API-based SmartConnector retrieves Adversary Signals events and normalizes them to the SIEM schema. Relevant events pass through the Message Bus to Enterprise Security Manager and Behavioral Signals, with alerts and anomalies presented in the unified alert view. Analysts can review external insights in the Adversary Signals portal and investigate parsed SIEM events through Search UI where supported.

The illustrated flow brings external signals into the enterprise environment without sending private enterprise telemetry back to Adversary Signals. Security Log Analytics adds historical search and investigation. When planning a deployment, work with OpenText to confirm supported connectors, event routing, search access, and analyst workflows for your configuration.



A legitimate account conceals an intrusion

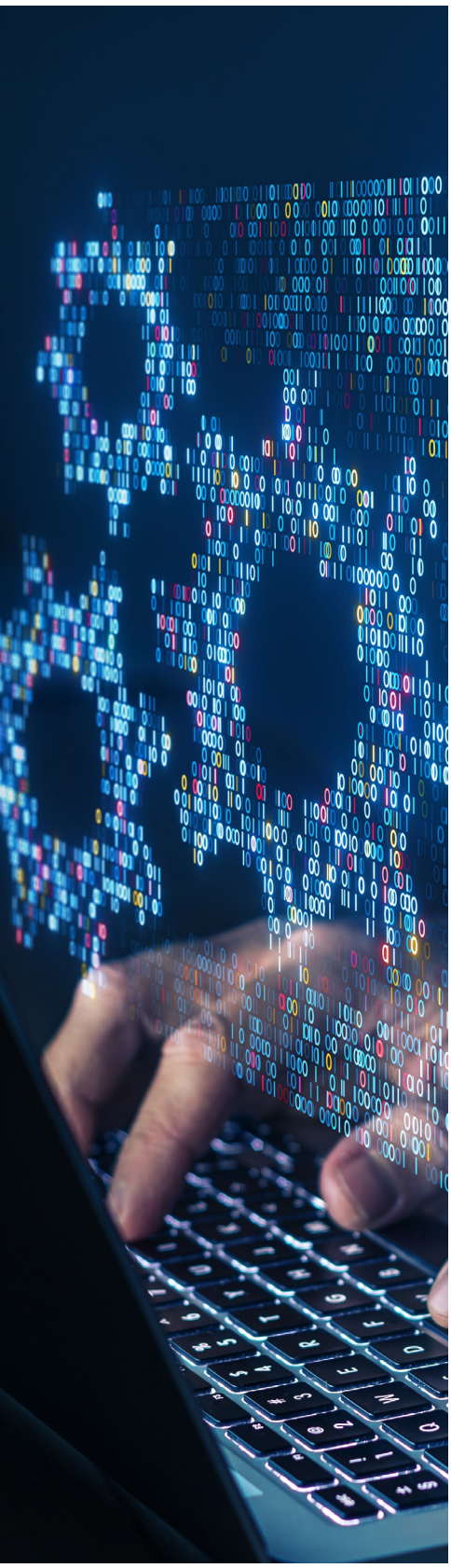
At 9:12 a.m., the SOC receives an alert involving a finance employee's account. Several failed sign-ins were followed by a successful login and access to a sensitive file repository.

The employee regularly handles financial documents. The activity could reflect a forgotten password followed by legitimate work, or an attacker using stolen credentials. Blocking the account immediately could interrupt a critical business process. Dismissing the alert could allow sensitive information to leave the organization.

This realistic illustrative scenario assumes relevant telemetry, configured detection rules, and supported integrations. Analysts still face delayed records, ambiguous infrastructure matches, and business constraints.

Four perspectives build the evidence

Analytic perspective	Evidence in this example	Contribution to the decision
Real-time correlation Enterprise Security Manager	A configured rule connects failed sign-ins, a successful login, and sensitive resource access within a short window.	Identifies a suspicious sequence. It does not establish who used the account.
Behavioral analytics Behavioral Signals	The account accesses substantially more files than usual and reaches a repository outside its established activity pattern.	Makes routine use a less convincing explanation and helps prioritize the investigation.
Internet signal analytics Adversary Signals	External analysis links malicious activity to infrastructure associated with a contacted destination. The initial match involves a shared IP address.	Prompts hostname, timing, and infrastructure checks. A shared IP match alone does not establish compromise.
Log analytics Security Log Analytics	Available identity, file-access, endpoint, and network records support a session and host timeline. Some endpoint records arrive late; transfer contents remain unknown.	Tests the approved-export explanation, connects observed activity, and identifies evidence gaps and possible scope.



From corroborated evidence to containment

The first external match is to an IP address on shared infrastructure, so the analyst does not treat it as proof. They check the contacted hostname, signal timing, and infrastructure relationship. The external context remains supporting evidence; the investigation must establish what happened inside the enterprise.

An approved finance export initially offers a benign explanation. The application owner confirms that its expected account and repository differ from the observed activity. The employee is unavailable, and some endpoint records arrive late. The analyst correlates available session, host, and timestamp evidence, accounting for clock differences, then adds the delayed records to the timeline.

The file-access spike, unexpected repository, archive creation, and outbound transfer support a suspected compromised-account incident with possible exfiltration. External context strengthens concern about the destination. The analyst escalates on the combined evidence without waiting for employee confirmation or treating any one signal as conclusive.

Network records show outbound traffic volume, not its contents. The analyst records possible exfiltration and investigates which files, if any, were transferred.

Act on the evidence and verify the result

Under the response procedure, the incident lead authorizes session revocation and account restriction. Because the workstation supports a critical finance process, the team coordinates isolation with its owner. Responders preserve available evidence and assess a narrowly targeted destination block to avoid disrupting unrelated services on shared infrastructure.

Responders verify that the suspicious session and transfer stop, then hunt for related accounts and hosts. A second host contacting the same IP is checked for the same hostname and behavior before being treated as affected. Monitoring continues for renewed activity.

Why the combined view matters

Correlation raises the initial alert; behavior prioritizes it; external context supplies a relationship to investigate; and logs test the sequence and scope. Shared hosting, an approved export, and delayed telemetry all require analyst judgment. The combined view helps the team work through these ambiguities and make a defensible response decision.

Multi-space analytics connects internal activity and external adversary context into a better-supported incident hypothesis, while keeping evidence gaps and alternative explanations visible.

The benefit is a clearer basis for prioritization, investigation, and containment. Better response quality means acting on corroborated evidence, targeting containment appropriately, preserving evidence, and verifying that activity stops while limiting avoidable business disruption. Assess the result through detection time, reaction time, analyst effort, and verified containment against the existing workflow.

Reduce exposure time through detection and reaction

Exposure Time is the sum of Detection Time and Reaction Time: Et = Dt + Rt. Detection Time runs from the defined start of malicious activity to an actionable detection. Reaction Time runs from that detection to effective containment. Use the same endpoints when comparing workflows so improvements reflect a shorter exposure window.

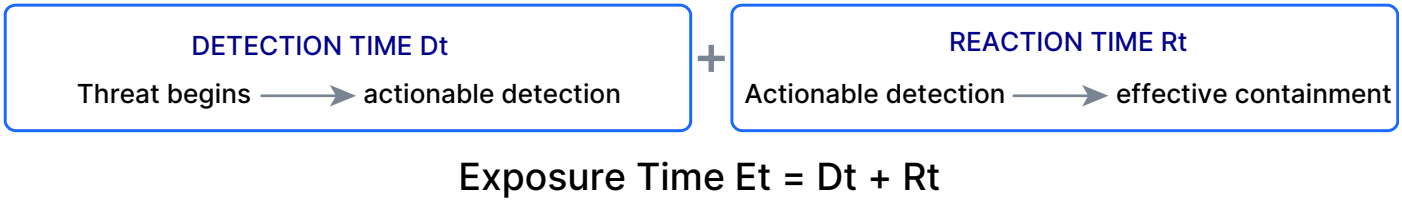


Figure 4 Exposure Time includes both detecting a threat and acting effectively to contain it.

Correlation and behavioral detection can contribute to actionable detection; relevant external activity may supply an earlier lead. Log investigation and corroborating context support a better-informed response. In the scenario, hostname checks help avoid an indiscriminate shared-IP block, and owner coordination limits disruption. Shorter exposure time requires both prompt detection and effective containment: an earlier alert alone does not prove an earlier or higher-quality response.





Evaluate the outcomes that matter to the SOC

Outcome	Contribution of the model	Suggested validation
Visibility	Internal activity plus relevant external context	Check which incident questions each source can answer
Detection speed	Patterns, deviations, and external leads	Measure Dt using a consistent threat start point
Detection accuracy	Corroboration and hypothesis testing	Compare adjudicated true and false positives
Analyst efficiency	More context available during investigation	Measure analyst effort per comparable case
Response quality and confidence	Corroborated evidence, targeted action, and verified containment	Measure Rt; verify containment, evidence preservation, and avoidable business disruption

Establish a baseline and compare equivalent scenarios after adding an analytic perspective. Track time and response quality together: faster action that fails to contain the threat or creates avoidable disruption is not an improvement. Results depend on telemetry, configuration, and operating practices.

Validate complementary value in your environment

A practical assessment should compare comparable incident scenarios with and without the added analytic perspective. Record available sources, analyst experience, configuration, retention, alert volume, and the response endpoint. Include missed detections and benign anomalies as well as successful cases. This helps determine whether additional context improves decisions rather than merely adding work.

Evaluate the connections between analytics as well as each individual capability. Behavioral context can inform alert severity; logs can validate a pattern; and external context can clarify a destination's significance. Measure whether these connections improve investigation and response while reducing analyst effort.

See more. Detect faster. Respond with confidence.

Contact us to see if a technical assessment can help determine how multi-space analytics can improve your security posture.

Evolve the SOC around its most important visibility gaps

Organizations can adopt multi-space analytics from different starting points. A SOC with established correlation may prioritize behavioral discovery or external context. A team with strong log retention may first need faster investigation workflows. The progression from telemetry to log analysis, correlation, behavioral analysis, and internet signal analytics is a conceptual maturity model, not a required implementation order.

Start with a threat scenario that matters to the business. Determine which questions existing tools answer, identify the missing perspective, and confirm the telemetry and integration needed to connect it to the investigation. Then establish a baseline for detection, analyst effort, and containment before expanding the workflow.

Assess whether your SOC sees the full threat picture

- Can analysts recognize meaningful suspicious event patterns as they occur?
- Can they identify abnormal user or entity activity beyond predefined detection rules?
- Can they reconstruct and test a hypothesis using retained historical evidence?
- Can they observe relevant adversarial activity beyond the enterprise environment?
- Can they use these perspectives together to reach an authorized response decision?

A gap in one answer identifies an area for assessment. The objective is to improve the evidence available for the most consequential security decisions while preserving the strengths of the existing SOC.

OpenText Multi-Space Analytics Framework

Harness the power of the OpenText SIEM portfolio to level up your cyber defense

Perspective	Security question	OpenText capability
Real-time correlation	What well-understood suspicious pattern is happening now?	Enterprise Security Manager
Behavioral analytics	What activity is abnormal for this user or entity?	Behavioral Signals
Log analytics	What does the underlying evidence show?	Security Log Analytics
Internet signal analytics	What relevant adversarial activity is occurring outside the enterprise?	Adversary Signals

Copyright © 2026 Open Text • 10.26 | 262-000247-001

opentext™