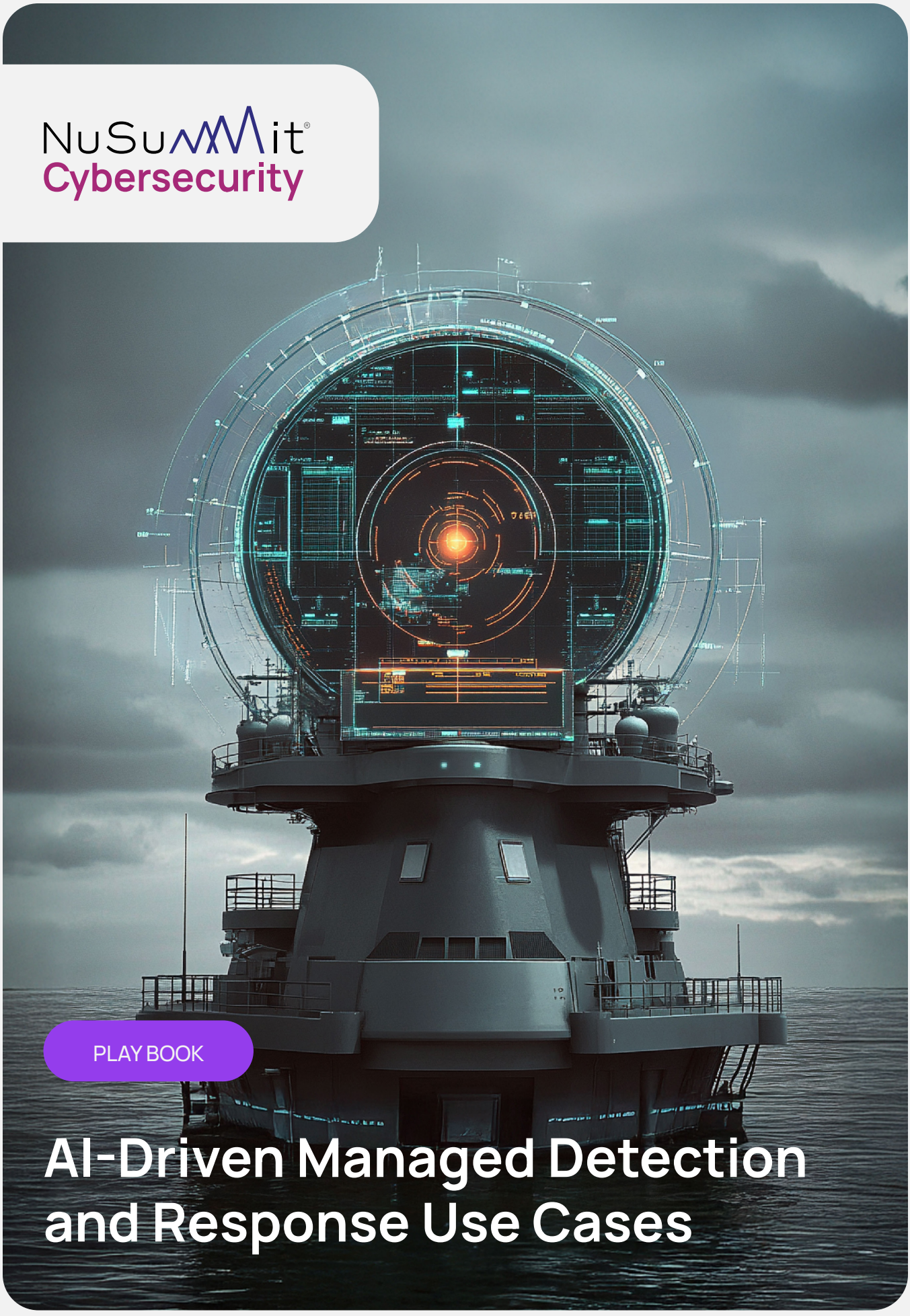
NuSummit Cybersecurity



PLAY BOOK

AI-Driven Managed Detection and Response Use Cases

Table of Contents

The Operational Reality of MDR

Modern enterprises generate a continuous stream of security telemetry from endpoints, authentication systems, networks, firewalls, cloud platforms, and applications.

All of this data converges within a Security Information and Event Management (SIEM) platform, which ingests logs, applies detection logic, and generates alerts when suspicious patterns are detected. However, detection alone does not secure an organization.

The real challenge of MDR is not generating alerts. It is interpreting them quickly and consistently enough to reduce risk before it escalates.

Security teams must repeatedly answer three operational questions:

- Does this alert matter?
- How urgent is it?
- What action should follow?

At enterprise scale, answering these questions manually becomes unsustainable. Alert volume grows, analyst fatigue increases, and decision quality begins to vary.

This is where AI strengthens MDR operations, not by replacing SIEM platforms or analysts, but by improving how alerts are interpreted, prioritized, investigated, and acted upon.

MDR Maturity Model

Organizations typically evolve through identifiable stages of MDR capability.

Reactive MDR

- Rule-based alerts
- Manual triage
- Manual response
- High analyst workload

Focus:
Respond after detection

Proactive MDR

- Threat intelligence integration
- Structured threat hunting
- Improved correlation

Focus:
Identify suspicious behavior earlier

AI-Optimized MDR

- Automated enrichment
- Risk-based prioritization
- Playbook-driven response
- Guided investigations
- Continuous improvement
- Automated reporting

Focus:
Scale detection and response without increasing analyst load

Where AI Fits in the MDR Architecture

A practical MDR architecture follows a layered operational flow:

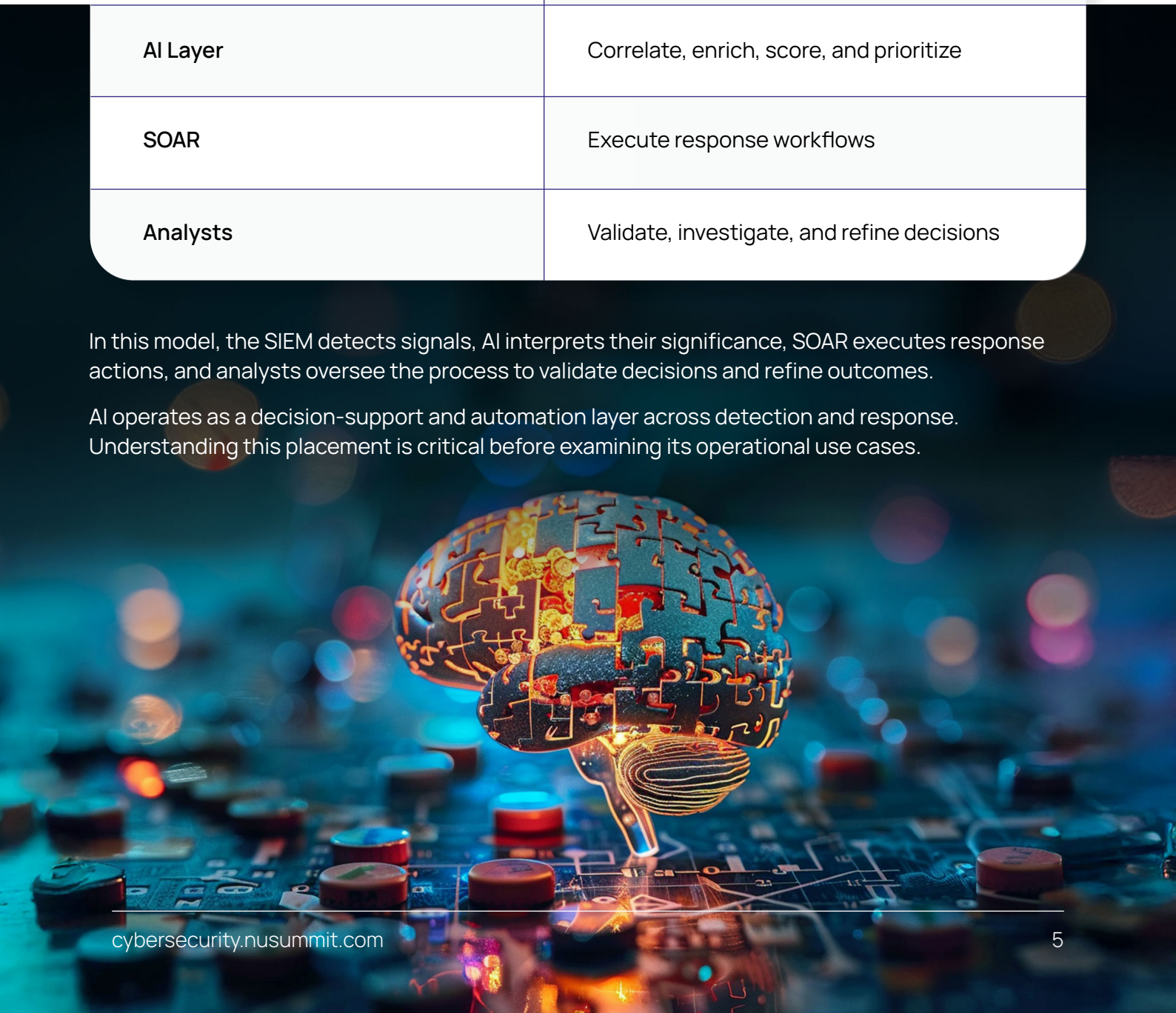
Telemetry Sources → SIEM → AI Analysis Layer → SOAR → Response

Each layer has a defined responsibility:

Layer	Role
Telemetry Sources	Generate raw activity signals
SIEM	Aggregate logs and detect suspicious events
AI Layer	Correlate, enrich, score, and prioritize
SOAR	Execute response workflows
Analysts	Validate, investigate, and refine decisions

In this model, the SIEM detects signals, AI interprets their significance, SOAR executes response actions, and analysts oversee the process to validate decisions and refine outcomes.

AI operates as a decision-support and automation layer across detection and response. Understanding this placement is critical before examining its operational use cases.



Automate Alert Triage and Enrichment

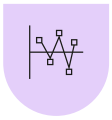
Alert triage is the first operational bottleneck in any SOC.

Every alert requires context before meaningful evaluation. Analysts must determine:

1. Asset criticality
2. User history
3. Device patterns
4. Geographic behavior
5. Related activity

Without automation, gathering this context requires pivoting across multiple tools, often taking longer than the investigation itself.

AI accelerates triage through three mechanisms:



Telemetry correlation links signals across identity logs, endpoint telemetry, network activity, and cloud events.

Behavioral baselining models establish normal activity patterns and identify deviations.

Risk scoring ranks alerts based on historical incident data, asset value, and threat intelligence inputs.

Example: Login Failure Analysis

Repeated login failures may indicate either a mistyped password or a credential attack. At the SIEM layer, both may produce identical alerts.

AI distinguishes them by evaluating geolocation consistency, device continuity, login timing patterns, behavioral history, and IP reputation. The alert is then assigned a contextual risk score before analyst review.

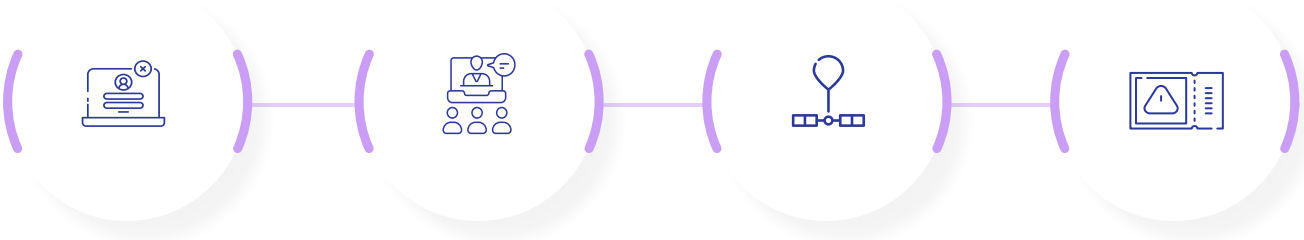
This reduces triage time and ensures consistent prioritization.

Automate Incident Response

An alert becomes an incident once it crosses a defined risk threshold. The speed of this transition directly affects the success of containment.

AI integrates with orchestration systems to execute response logic using structured playbooks. These playbooks encode agreed response procedures and conditional decision paths.

If risk indicators exceed the threshold and corroborating signals are present, the system can automatically trigger containment actions such as:



Suspending accounts

Revoking sessions

Isolating endpoints

Creating incident tickets

Example: Privileged Account Misuse

A privileged account logs in from a new country and executes administrative commands never previously observed. Individually, these actions may not appear critical. Evaluated together, they exceed the risk threshold. The session is immediately suspended and escalated for investigation.

Reducing response time by minutes can prevent lateral movement and privilege escalation.

Continuous Threat Investigation and Incident Analysis

Sophisticated attacks rarely produce a single obvious alert. Instead, they generate small anomalies across systems. An endpoint may show minor registry changes while the same device initiates connections to unfamiliar domains, and the associated user account accesses servers outside its normal scope. Individually these appear harmless. Correlated together, they form a pattern.

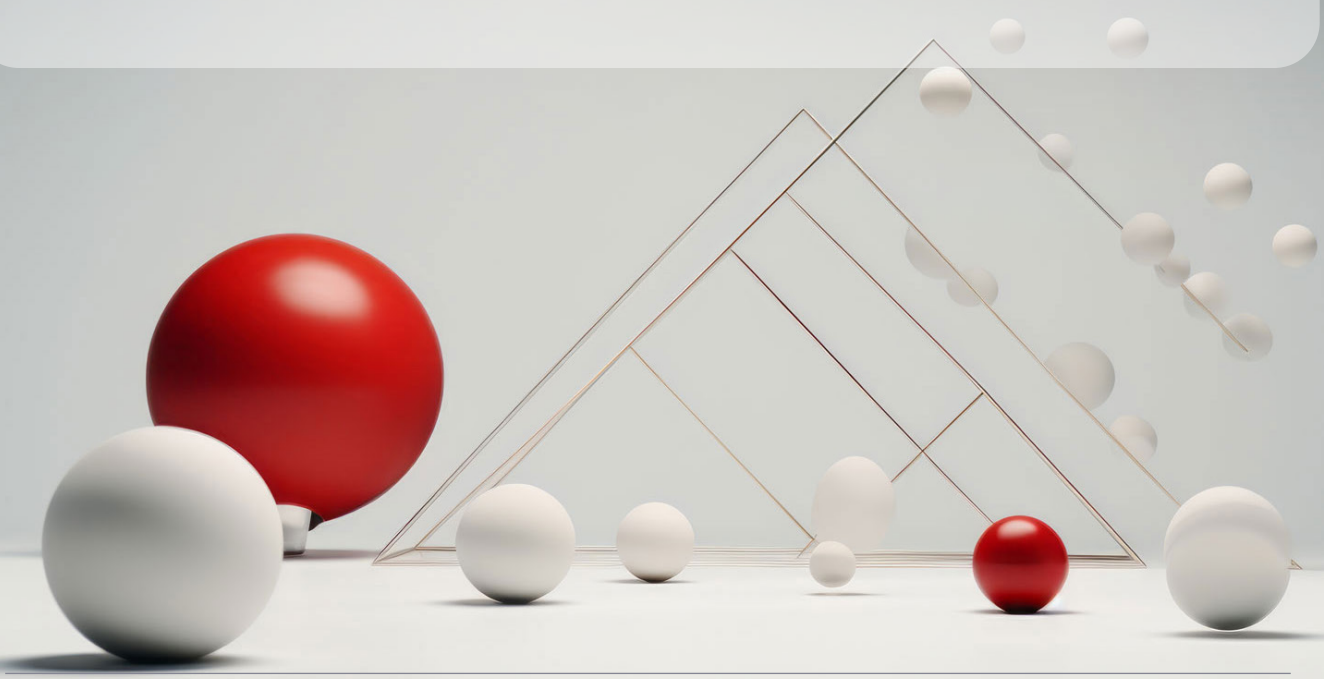
AI supports investigation by

- Analyzing activity sequences across time
- Clustering related anomalies
- Correlating signals across platforms
- Mapping relationships between entities

Example: Early-Stage Compromise

A registry modification alone may not be suspicious. Combined with unusual outbound traffic and abnormal server access, however, the system identifies a behavioral chain consistent with compromise.

Instead of reviewing alerts individually, analysts see the attack narrative. Root cause analysis becomes faster and more accurate.



Analyst Augmentation- Quality of Analysis

Investigation depth often varies based on analyst experience, shift timing, and workload. This variability can lead to inconsistent outcomes.

AI reduces inconsistency by embedding structured investigative logic into workflows. Investigation models aligned with incident types automatically recommend validation steps, queries, and correlation checks.

Example: Malware Detection

When malware is detected on one device, a minimal investigation might remove the file and close the alert. A structured investigation examines broader risk:

- Presence of the same indicators elsewhere.
- Persistence mechanisms.
- Lateral movement attempts.
- Suspicious outbound communication

By applying these checks systematically, investigations reach consistent depth regardless of analyst tenure.

AI does not replace analysts. It ensures investigations start from a complete baseline rather than a minimal one.

Playbook Adaptation- Automate SOP Creation

Security environments change constantly. Attack techniques evolve. Defensive assumptions must be refined.

AI-supported MDR platforms enable adaptive playbooks. Response workflows are modular and version-controlled rather than static.

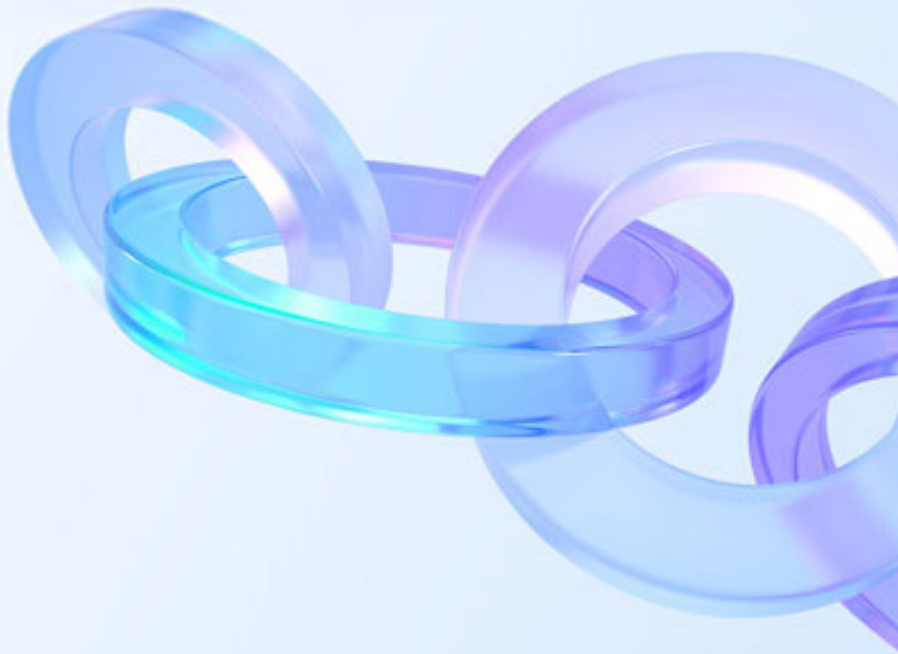
Example:Post-Incident Learning

After resolving an incident involving encoded PowerShell commands, analysts determine that future investigations should automatically check for obfuscated parameters. Once added, this validation step is applied to all similar alerts going forward.

This creates a continuous improvement loop:

Incident → learning → playbook update → improved future response

Operational maturity increases because improvements are embedded into the process rather than retained only in individual experience.



Dashboards and Reporting

Security operations must translate technical activity into actionable insight for operational teams and leadership.

Reporting typically requires assembling metrics such as:

- Incident trends
- Response duration
- Severity distribution
- Recurring threats
- Unresolved cases

Manually compiling these reports consumes analyst time and introduces inconsistencies.

AI continuously aggregates operational metrics directly from SIEM and ticketing systems, generating structured summaries and visual reports automatically.

Example: Pattern Detection Through Reporting

If reporting reveals repeated authentication anomalies from a specific region or tied to a particular application, leadership can quickly determine whether the pattern indicates targeted activity, configuration gaps, or policy weaknesses.

Visibility becomes continuous rather than periodic.

How Real Attackers Behave and Why These Stages Matter

Real attackers rarely trigger obvious alerts. They intentionally design activities to blend into normal operations:

Credential guessing spread across weeks

Low-volume data exfiltration

Threat Patterns

Administrative tools used instead of malware

Gradual privilege escalation

Because of this, detection rarely depends on one signal. It depends on pattern recognition across time and systems.

Attacker Behavior	MDR Capability That Stops It
Slow credential attacks	Generate raw activity signals
Living-off-the-land techniques	Aggregate logs and detect suspicious events
Privilege escalation	Correlate, enrich, score, and prioritize
Stealth persistence	Execute response workflows
Recurrent intrusion attempts	Validate, investigate, and refine decisions

Operational Impact

When AI is integrated properly into MDR workflows, improvements compound:

01 Reduced alert fatigue

02 Faster containment

03 Consistent investigations

04 Clearer reporting

05 Faster analyst onboarding

06 Systematic use of senior expertise

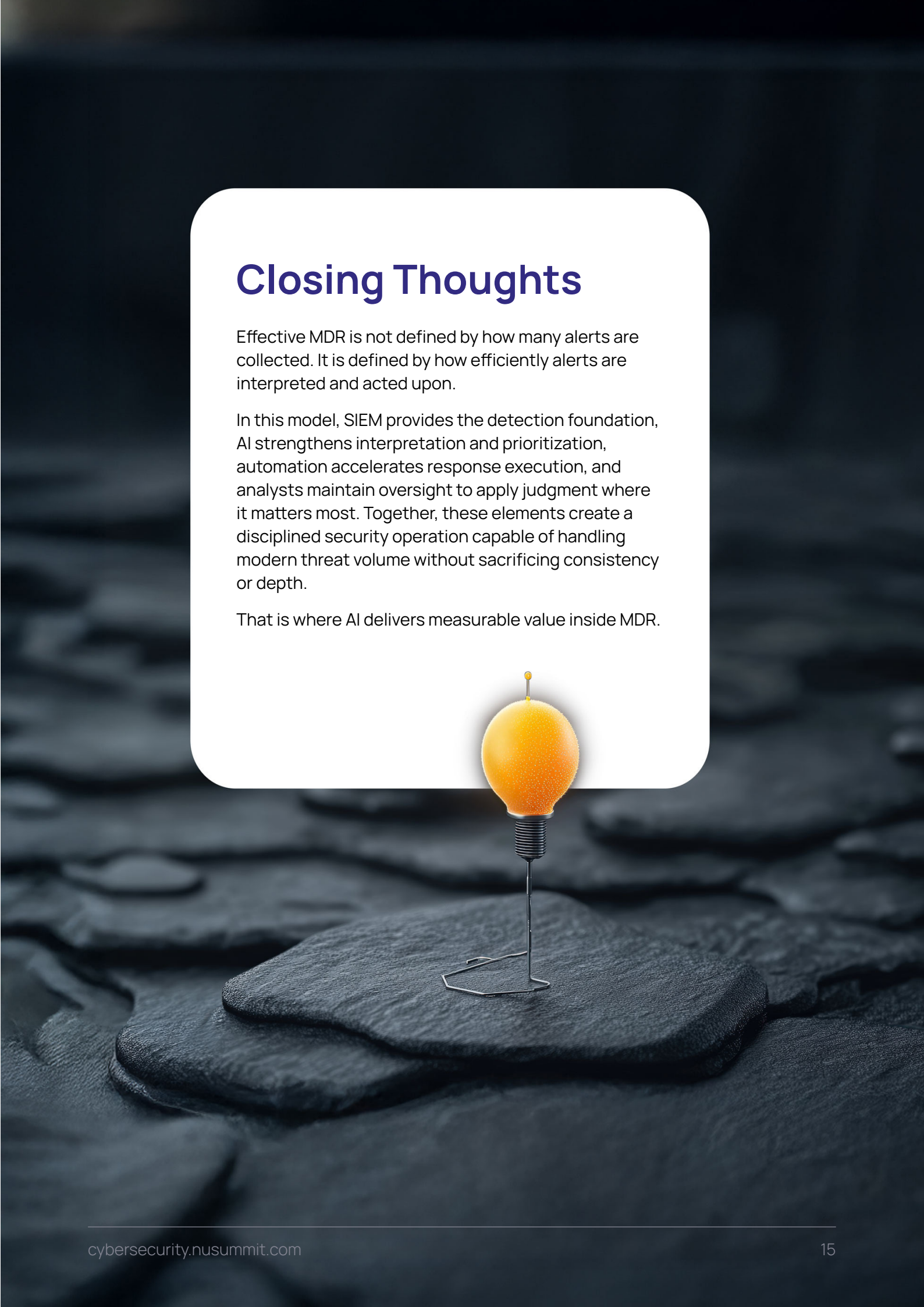
Most importantly, MDR becomes sustainable at scale. As alert volume grows, automation absorbs repetitive workload while analysts focus on complex and novel threats.

Closing Thoughts

Effective MDR is not defined by how many alerts are collected. It is defined by how efficiently alerts are interpreted and acted upon.

In this model, SIEM provides the detection foundation, AI strengthens interpretation and prioritization, automation accelerates response execution, and analysts maintain oversight to apply judgment where it matters most. Together, these elements create a disciplined security operation capable of handling modern threat volume without sacrificing consistency or depth.

That is where AI delivers measurable value inside MDR.



About NuSummit Cybersecurity

NuSummit Cybersecurity helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services.

Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at **cybersecurity.nusummit.com** or write to us at **cybersales@nusummit.com**

Dallas I Jersey City I Cupertino I Ottawa I Riyadh I Dubai Mumbai I New Delhi I Bangalore

Follow us at: