

Agentic SOC

The new operating
model for continuous
defense



An inflection point for the SOC

For decades, the security operations center (SOC) operating model has followed the same sequence: an alert fires, an analyst investigates, the case escalates, and the team responds. As teams and tooling matured, we got faster and more efficient at handling larger volumes of alerts and detecting more complex attacks.

Today's threat landscape has fundamentally broken this model. Attackers are using AI to map exposure, tailor payloads to your environment, and conduct thousands of operations a second. If they're blocked, the agent adapts and tries again—over and over. While defenders are triaging a queue of alerts, attacker agents have already moved ten steps further down the attack chain.

This asymmetry is structural. An operating model built around task efficiency cannot keep pace with adversaries operating at machine speed. We don't need to accelerate existing workflows. We need to redesign security operations around continuous protection—where attacks are disrupted automatically, specialized agents execute at scale, and defenders focus on directing outcomes.

The future SOC will not be measured by how much work it processes, but by how effectively it reduces risk. That requires a shift from managing tasks to governing outcomes—and from reacting at human speed to defending at AI speed.

The answer is not to work the list faster. It is to change what the SOC is built to achieve.

David Weston

Corporate Vice President

AI Security, Microsoft



Security has outgrown the task list

No matter how efficient security teams become at executing tasks, they're often optimizing for the wrong objective.

Modern security programs are remarkably good at executing tasks. They prioritize vulnerabilities, investigate incidents, respond to alerts, deploy controls, and remediate exposures at a scale that would have been unimaginable a decade ago.

The problem is that attackers aren't constrained by those same workflows.

An attacker doesn't care whether you've addressed the top 100 items on your vulnerability backlog if exposure number 8,031 still provides a path to their objective.

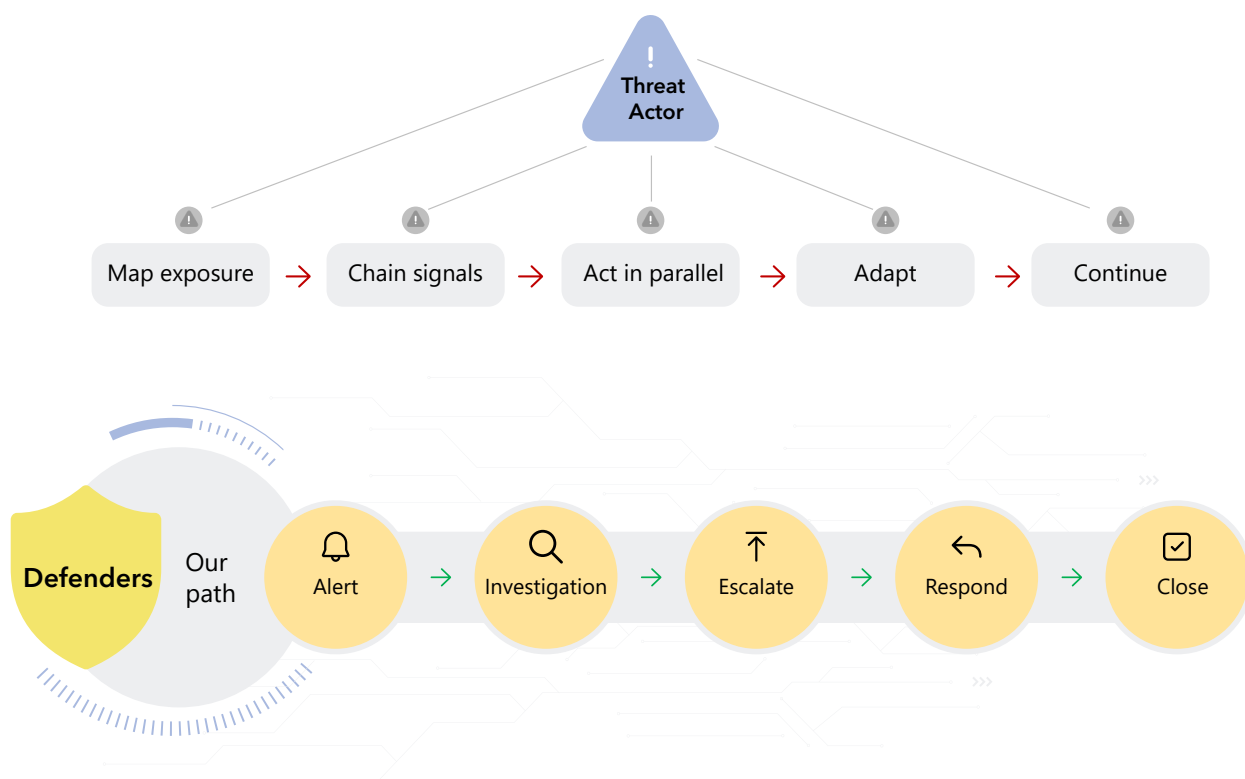
Lock down every managed endpoint and they may compromise a trusted vendor. Strengthen identity controls, and they may pivot through an application, a cloud workload, or an AI system. And agents have only made this easier.



Defenders are task-driven. Attackers are outcome-driven.

This creates a fundamental mismatch. Security teams improve protection one task at a time, while attackers continuously evaluate the environment for whatever path remains available.

As attack surfaces become more connected and AI enables adversaries to operate at unprecedented speed and scale, simply completing more tasks becomes an increasingly poor proxy for protection.



The question is no longer, can security teams keep up with the work?
It's , how do we change?

Designing for a new unit of work

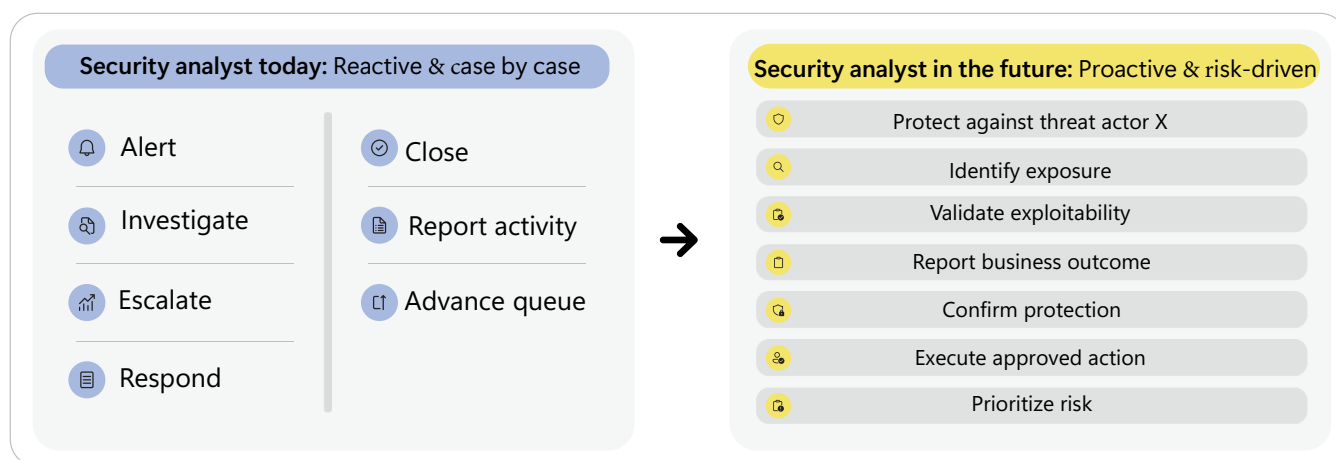
Even for security teams more outcome-focused than average, significant portions of the day are spent on work that supports protection but doesn't directly improve it.

Consider an active incident. Once triage confirms a threat, analysts begin gathering context: correlating related alerts, querying data lakes, analyzing behavior, validating attack paths, comparing observed TTPs against threat intelligence, coordinating with other teams, and documenting findings. All of that work is important. None of it contains the threat.

The defender's attention gets pulled into the mechanics of understanding the problem rather than improving the outcome. An agentic system changes that equation.

While agents gather evidence, analyze relationships, investigate attack paths, validate controls, and coordinate actions, defenders remain focused on what actually matters: Is the threat contained? Is the attack path eliminated? Is the business protected?

More importantly, defenders are no longer limited to a single objective at a time. While agents work through the investigation and coordination required to secure one outcome, security teams can focus their attention on the next. This is the shift.



The question is no longer, how many alerts did we process?
The question becomes, how much risk did we remove?

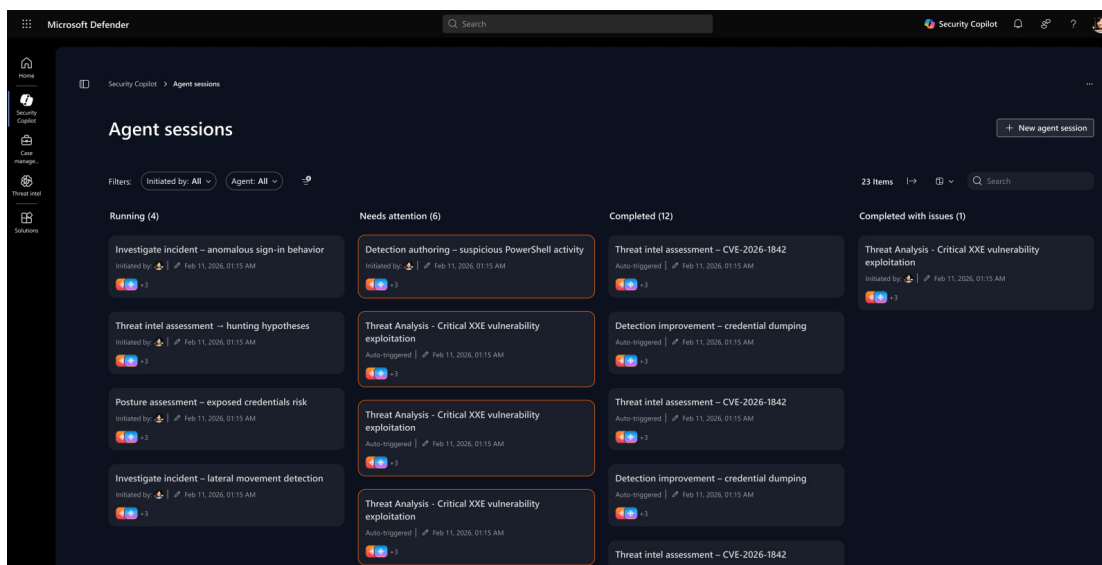
From security operations to a security system

While agents investigate, validate, correlate, and coordinate, defenders can remain focused on protection itself.

Instead of becoming absorbed in the mechanics of a single incident, security teams can think across multiple objectives at once. While one set of agents works to contain a threat, another can evaluate exposure to a newly disclosed vulnerability. While remediation is underway for one business service, another can be validating protections around a critical AI application.

For the first time, human attention is no longer the limiting factor.

Security leaders gain the ability to pursue multiple protection objectives in parallel. Analysts spend less time managing investigations and more time making decisions. Teams shift from reacting to individual events to continuously improving the overall security posture.



The result is not simply faster security operations. It is a fundamentally different capacity for defense.



Every role in the SOC is significantly changed

With agents taking on much of the execution work, security leaders gain the freedom to rethink how teams are structured and where expertise is applied.

For years, SOC's scaled by adding layers: analysts to triage alerts, specialists to investigate incidents, and senior experts to handle escalations.

As agents absorb more of that work, the bottleneck shifts from execution to decision-making.

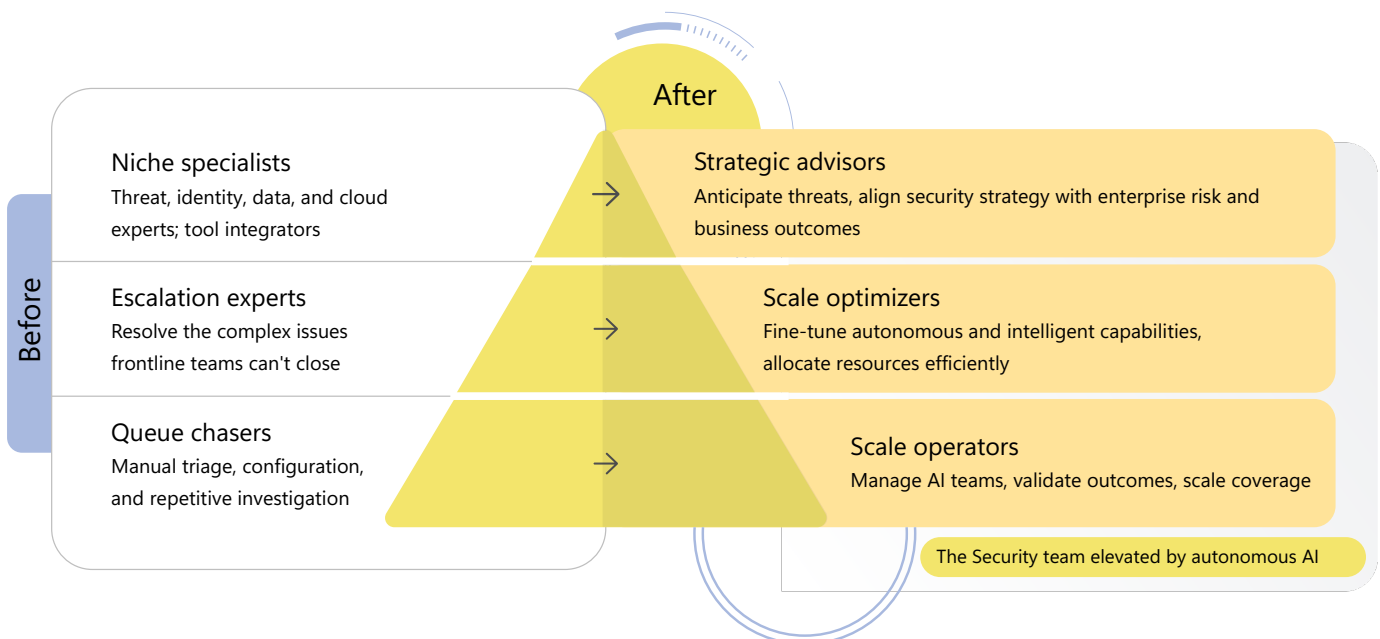
Less effort is spent moving information between specialists and queues. More expertise is concentrated on deciding what matters most, validating outcomes, and improving protection.

Human expertise moves higher in the stack

Teams can become flatter. Less effort is spent moving information between specialists and queues. More expertise is concentrated on deciding what matters most, validating outcomes, and improving protection.

The identity expert becomes less focused on identity incidents and more focused on identity risk. The vulnerability manager becomes less focused on remediation projects and more focused on exposure reduction. The incident responder becomes less focused on collecting evidence and more focused on containment strategy.

Human expertise doesn't disappear. It moves higher in the stack—from processing work to directing outcomes. The organizations that benefit most from AI won't simply execute security work faster. They'll redesign their teams around what humans do best: judgment, prioritization, governance, and strategy.



Accelerate your SOC transformation with [Microsoft Defender Experts](#). Get expert-led services to help you modernize security operations, defend against threats, build cyber resilience, and more.

The role capability shift

As human attention becomes less constrained by investigation and coordination work, organizations gain the freedom to rethink how expertise is distributed across the team.

In the past, as workloads increased, new tiers, queues, and escalation paths emerged to absorb volume and route work to the right experts.

In an agentic system, headcount is no longer driven primarily by alert volume. The design question becomes: What capabilities do I need around the agents?



SOC Analyst → Agent Orchestrator

Validates findings, approves system actions, resolves ambiguity, and handles low-confidence or high-impact decisions.



Detection Engineer → Frontier Security Engineer

Defines guardrails, codifies expertise, pressure-tests defenses, and turns proven security practices into repeatable system behavior.



Threat Hunter Adversary → Exposure Lead

Directs continuous attacker-informed exploration, validates attack paths, and focuses the organization on the exposures most likely to matter.



SOC Leadership → Risk System Orchestrator

Owens protection outcomes at the system level, measuring resilience, risk reduction, and the effectiveness of human and agent collaboration.

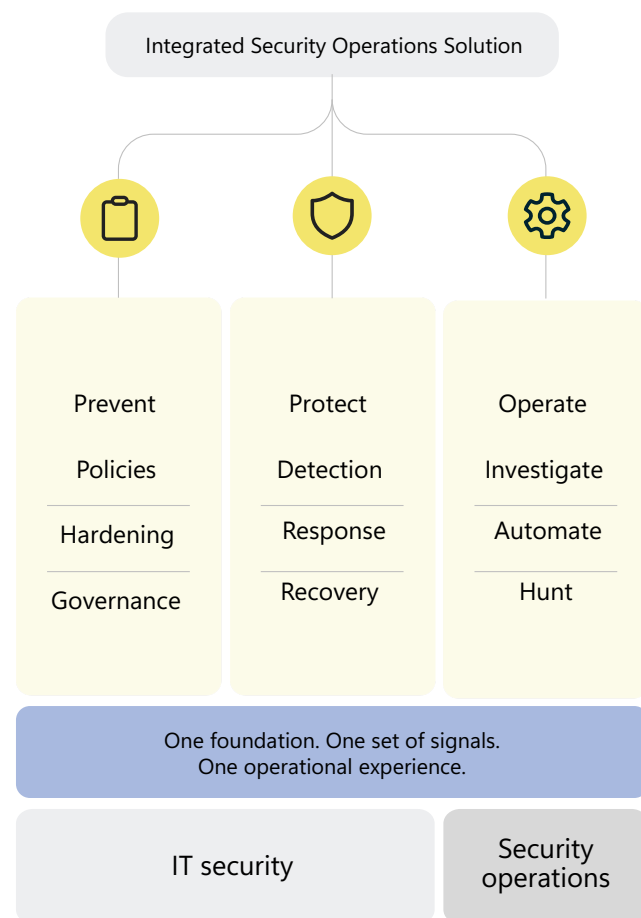
The next-generation SOC prioritizes expertise over escalation, strategic decision-making over coordination, and measurable outcomes over activity.

The Integrated SOC: The foundation for an era of continuous learning defense

The future of security operations will not be defined by a single technology or product milestone. It will be defined by a new capacity to defend as one intelligent, adaptive system. The integrated security operations center—ISOC—is the foundation for that future: an operating model in which people, AI agents, intelligence, and controls continuously sense change, reason across the environment, and translate intent into coordinated protection at the speed of the threat.

In the ISOC, defense becomes a living system rather than a sequence of handoffs. Specialized capabilities can continuously anticipate paths to compromise, connect signals that would otherwise remain fragmented, and coordinate governed action across domains. Each cycle of discovery, decision, and response strengthens the next—allowing the SOC to evolve from reacting to events to shaping a more resilient security posture before threats become business impact.

Security operations needs a common foundation



Microsoft Defender unifies prevention, detection, investigation, response, and threat intelligence into a single security operations experience.

Start with the foundation

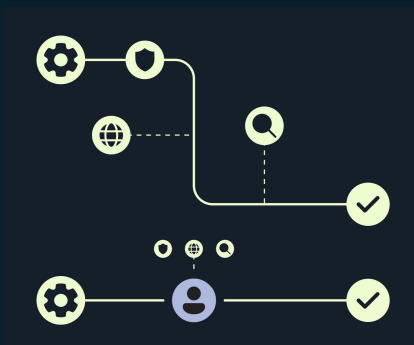


You can't coordinate people, agents, intelligence, and controls if they live in disconnected systems.

The first step is creating a shared foundation for security data, context, and action. Security teams need a platform that can unify identities, endpoints, cloud resources, applications, data, intelligence, and AI into a common understanding of the environment.

Before you can orchestrate work, you need a system that sees the whole picture.

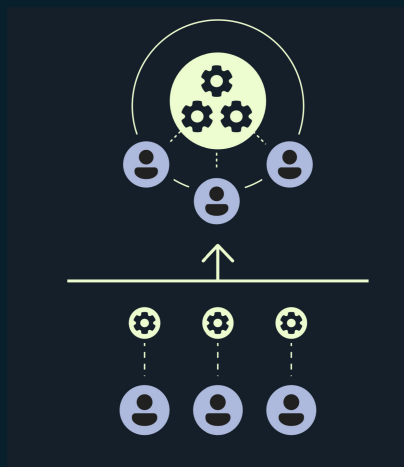
Introduce agents into the workflow



Most organizations won't jump directly to autonomous systems. They'll start by offloading well-defined activities: investigating incidents, validating exposures, analyzing attack paths, prioritizing remediation, and gathering evidence.

The goal isn't immediate autonomy. It's creating capacity. As agents prove they can consistently execute work, they free human experts to focus on decisions, priorities, and outcomes.

Scale from agents to systems



The real transformation happens when agents stop working independently and begin working together.

An incident investigation agent informs an exposure agent. An exposure agent coordinates with a remediation agent. A threat intelligence agent provides context across both.

Instead of augmenting individual tasks, organizations begin building systems capable of pursuing protection objectives. This is where leading organizations are headed—combining human expertise, specialized agents, and shared context into continuously improving security systems.

Building security systems for the AI era

Organizations that succeed in the age of AI will move beyond task execution and build systems that continuously reduce risk. Instead of measuring progress by alerts closed, investigations completed, or vulnerabilities remediated, they will focus on broader protection outcomes: reducing exposure, disrupting attack paths, strengthening resilience across the organization.

Human expertise will become more strategic as agents extend defenders' capacity, allowing security teams to focus on judgment, priorities, governance, and the decisions that shape protection at scale. The teams that begin building those systems today will be better positioned to defend at AI speed tomorrow.

Microsoft brings together security signals, threat intelligence, AI, and protection capabilities across identities, endpoints, cloud resources, applications, data, and AI systems. That connected foundation makes it possible to move beyond isolated tasks and toward coordinated defense.

Integrate now or pay later

-  Explore Microsoft's integrated security operations solution
-  Strengthen defenses and build cyber resilience with expert-led services