Enterprise Strategy Group™ by TechTarget

Accelerating SOC Maturity

A Roadmap to Modernizing Security Operations

Dave Gruber | Principal Analyst

ENTERPRISE STRATEGY GROUP

JANUARY 2025

This Enterprise Strategy Group eBook was commissioned by Microsoft and is distributed under license from TechTarget, Inc.

Contents

"89% of organizations now rank the risk of a successful ransomware attack **as a top five threat to their viability**."

Dave Gruber | Principal Analyst
ENTERPRISE STRATEGY GROUP

BACK TO CONTENTS

Introduction

As organizations of all sizes and complexities race to bolster their cybersecurity programs, the growing threat of successful cyberattacks demands swift and strategic action. Security and IT leaders are tasked with securing every facet of their operating infrastructure, ensuring alignment with key business objectives. Yet, this challenge often feels like hitting a moving target as both the attack surface being defended and the threat landscape evolve, becoming larger, more diverse, and increasingly complex.

Despite differences in organization size, complexity, and security program maturity, the threats and adversarial tactics faced by security teams are strikingly similar. For example, 89% of organizations now rank the risk of a successful ransomware attack as a top five threat to their viability, underscoring the urgency to advance their security programs.[1]

> "Selecting the right SIEM solution is no longer just about **managing logs**."

Amid these challenges, security information and event management (SIEM) solutions have emerged as a cornerstone technology for security operations. Recent innovations have transformed SIEM platforms into critical enablers for accelerating security program development and achieving greater maturity. Selecting the right SIEM solution is no longer just about managing logs; it's about empowering your security team to drive meaningful outcomes across the entire threat lifecycle.

This report delves into the security maturity journey, exploring how organizations can leverage SIEM solutions to align with their evolving needs, enhance their defenses, and achieve operational excellence in the face of a constantly shifting threat landscape.

[1]. Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023.

BACK TO CONTENTS

Architecting a Scalable Security Program Strategy

Architecting a Scalable Security Program Strategy

As security leaders embrace the mandate to strengthen security posture, most must do so within strict operating constraints and challenges, including limited funds, skill shortages, and IT operating infrastructure vulnerabilities, which are often outside of their control. Most will already have some number of security controls in place, in addition to varying levels of security operations (SecOps) processes and supporting staff and technology. The challenge is, therefore, how to best leverage existing investments and processes while moving ahead to a more robust and comprehensive security posture.

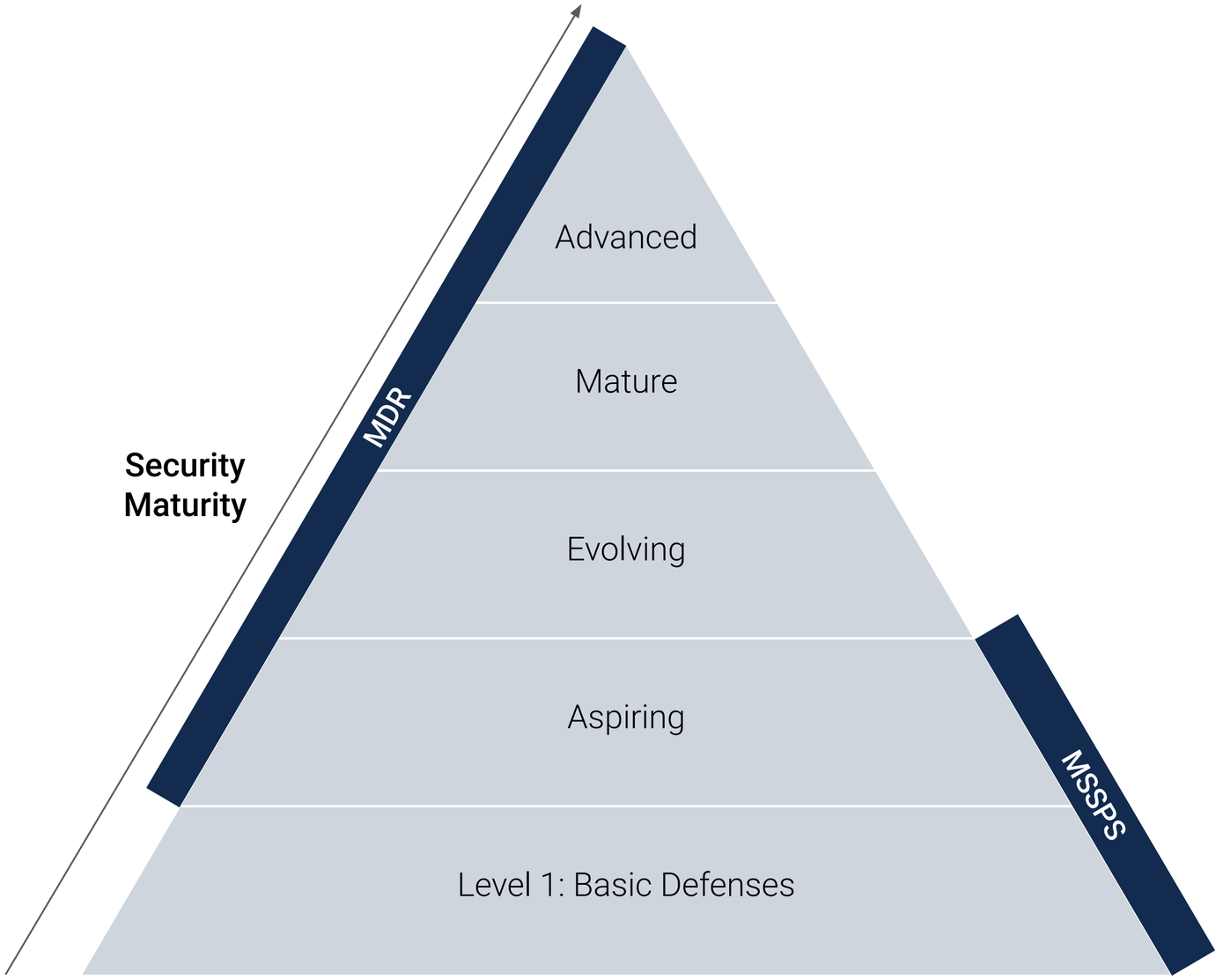
The Security Maturity Journey

Security maturity refers to an organization's level of preparedness and capability to protect its information assets and effectively respond to security threats, essentially indicating how well developed and well implemented their security practices are. These practices range from basic compliance to a proactive and continuously improving security posture across the organization.

For many, their security program journey follows a rather predictable path that can be described in terms of overall security maturity levels. As such, a higher security maturity level signifies a better ability to mitigate risks and defend against cyberattacks, leading to reduced cyber-risks, improved compliance with regulations, enhanced business resilience, and better decision-making regarding security investments.

While many security and capability maturity models exist and can be used to benchmark and analyze an organization's progress, there are five levels of security in most models.

The Journey to Security Maturity



BACK TO CONTENTS

The Critical Role of Security Operations

SecOps: A Core Pillar of Program Maturity

Within the many strategies involved in modern security programs, the SecOps function is a core pillar.

Enterprise Strategy Group's security operations and analytics platform (reference) architecture (SOAPA) describes the common operating components powering a mature SecOps function.

SOAPA: Security Operations and Analytics Platform Architecture

Cloud-based services and delivery:

- SaaS Applications
- Platform and Infrastructure
- Managed as a service (MSP)
- Analytics, shared threat intel...

Security operations platform layer
(automation and orchestration)

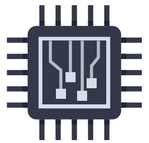
Security Controls:

- Remediation
- Policy updates
- Risk mitigation...

XDR, SIEM, network forensics, EDR, TIP, IRP, UEBA...

Analytics layer

Software services and integration layer



- Data transformation
- Publish/subscribe
- API set
- Message bus...

- On premises
- Cloud-based
- Hybrid

Common distributed data services

- Data pipelining
- De-duplication
- Compression/encryption...

Security Telemetry
(Logs, flows, network and host sensors, threat intelligence, IAM, cloud services, vulnerability,...)

BACK TO CONTENTS

SOAPA Foundational Building Blocks

Foundational to the SOAPA model are three core pillars:

The Data Layer

The common distributed data services layer handles all aspects of security data pipelining, gathering telemetry, intelligence, and hygiene data across the estate. To provide needed visibility, this core function must be both performant and dynamic, capable of supporting continuous change and scale across the IT operating environment. Common tools used to support this layer include SIEM, custom data lakes, data pipeline management tools, and more.

The Analytics Layer

The analytics layer must be capable of correlating, analyzing, and detecting all aspects of threat and risk. This critical layer must continuously analyze massive quantities of inbound signals, together with threat intelligence and dynamic risk data. The model is not prescriptive on where and how this process takes place but rather embraces the use of both centralized and distributed analytics processes. Like the data layer, this core function must be both performant and dynamic, capable of supporting continuous change and scale across the IT operating environment. Common tools used in this layer are the many detection and response tools (XDR, EDR, NDR, CDR, etc.), SIEM, user entity and behavior analytics (UEBA), threat intelligence platforms (TIPs), and more.

The Platform Layer

The platform layer provides the connection between human and machine. Automation and orchestration capabilities, now fueled by AI and generative AI (GenAI), support the triage, prioritization, investigation, and response processes needed to mitigate cyber-risk. Common tools used to support this layer often include SIEM (inclusive of SOAR), IT service management platforms, automation workflow tools, integrated security operations platforms, and more.

Note that SIEM has evolved to provide capabilities across all three SOAPA pillars, making SIEM solutions an important, often-used foundational technology in support of the SecOps security maturity journey.

BACK TO CONTENTS

A Deeper Look at Leveraging SIEM to Accelerate Security Maturity

Accelerating Outcomes With SIEM

SIEM solutions have evolved to support many functions within the SecOps function. As such, SIEM solutions have become commonly utilized within the SecOps function at many levels. With such importance to this critical collection of capabilities, investments in SIEM solutions often occur early in the security maturity journey. However, use cases and SIEM advantages often vary as maturity increases.

Depending on the security maturity level of an organization, SIEM solutions can be applied in different ways. Despite a past reputation of complexity and excessive cost, modern SIEM solutions are significantly more approachable, affordable, and scalable. SIEM solutions are, therefore, applicable to a wider audience, especially at maturity levels 2, 3, and 4. This section will review how and where SIEM solutions can help security teams operating at levels 2, 3, and 4 overcome specific challenges and where SIEM solutions can help support improved SecOps outcomes.

Level 1: Basic Defenses

Often unstructured and relatively unorganized, an organization at Level 1 might just be starting out with its information security processes and defining what those look like.

Most Level 1 organizations depend on third-party managed service providers (MSPs) to address their IT and security needs. For this reason, few hire dedicated security personnel, with most depending on their IT leaders to manage the funding and relationship with a service provider for all security infrastructure and operations.[2] MSPs and managed security service providers (MSSPs) will often utilize customized SIEM tools in support of basic security operations functions.

As a result, Level 1 organizations should see efficiency improvements, such as a reduction in security data management costs and improved analyst coverage and throughput, plus efficacy improvements, such as improved mean time to detect and a reduction in mean time to respond (MTTR).

“Despite a past reputation of complexity and excessive cost, modern SIEM solutions are **significantly more approachable, affordable, and scalable.”**

Leveraging Microsoft Sentinel at Level 1

For organizations that are not using an MSP and are already leveraging Microsoft environments, such as Azure Active Directory, Microsoft 365, or Defender, can quickly connect these services to Microsoft Sentinel, enabling centralized visibility and basic threat detection without requiring advanced security expertise. With Microsoft Sentinel’s scalable pay-as-you-go model, Level 1 organizations gain foundational SIEM capabilities while reducing operational overhead, ensuring their security programs align with limited budgets and resources.

[2]Source: Enterprise Strategy Group Research Report, Midmarket and Small Enterprise Cybersecurity Program Development: A Work in Progress, November 2024.

BACK TO CONTENTS

Level 2: Aspiring

Environment: Moving to more formalized security processes, at Level 2, actions and responses can be repeated by different members of specific teams. At this level, there will likely be some disconnect between departments where individual security processes are performed or documented differently.

Most organizations at this level are beginning to formalize and document security policies and processes and have committed funds to begin the architecture of a more modern security program. With only one dedicated security expert typically employed, most Level 2 organizations still primarily operate in a reactive fashion, responding to cyber-related issues as they occur. Most also lack visibility into portions of their operating environment and, therefore, struggle to understand risk and keep up with attacks.

Challenges: When alerts are triggered within individual controls, only those that cause tangible disruption are typically investigated and mitigated, leaving other alerts unaddressed. With only limited, fragmented tools in place, many complain about too many alerts and too much security data to manage effectively. With limited, if any, integration or aggregation of security data in place, and a dependence on manual processes to investigate and mitigate, investigations are complex and time-consuming. Consequently, security personnel in organizations at this level often struggle to keep up with the volume and complexity of threats, resulting in alert fatigue, frustration, burnout, and high turnover of security personnel.

SIEM Advantages: Modern SIEM solutions can enable Level 2 organizations to transition from reactive to more proactive security operations. Out-of-the-box (OOTB) connectors ease the effort needed to aggregate, correlate, and analyze security data across the many commonly deployed security controls, providing new levels of visibility, threat detection, and analysis.

This new level of foundational threat detection should enable security personnel to see and respond to more threats, with less effort spent investigating using the many disparate security tools and data sets deployed.

As a result, Level 2 organizations should see efficiency improvements, such as increased staff productivity, improved response orchestration, and a reduction in on-premises infrastructure, plus efficacy improvements, including expanded visibility and coverage as well as a reduction in MTTR.

Leveraging Microsoft Sentinel at Level 2

Microsoft Sentinel offers centralized visibility by seamlessly aggregating and correlating security signals across disparate tools and environments. Its OOTB connectors and built-in automation significantly reduce deployment complexity and time, enabling teams to gain actionable insights without requiring deep engineering expertise.

Microsoft Sentinel's intelligent threat detection capabilities, powered by machine learning (ML) and advanced analytics, help reduce noise and prioritize critical alerts, addressing alert fatigue and ensuring security personnel focus on the most pressing threats. Additionally, its scalable cloud-native architecture supports growing security needs without the overhead of traditional SIEMs, positioning SecOps teams to maximize efficiency and resource use.

BACK TO CONTENTS

Leveraging Microsoft Sentinel at Level 3

Microsoft Sentinel's cloud-native architecture efficiently handles growing data volumes while providing tools to reduce the costs and complexity of data pipeline management. In addition, Microsoft Sentinel provides tools for SOC optimization, enabling SecOps teams to improve both cost efficiency and security coverage through dynamic, data-driven recommendations.

By unifying SIEM and XDR capabilities, Microsoft Sentinel delivers integrated threat detection, investigation, and response, eliminating silos across on-premises and cloud environments. Its built-in automation capabilities and AI/ML-driven analytics empower security teams to prioritize threats effectively, reducing noise and accelerating decision-making.

Furthermore, Microsoft Sentinel incorporates high-value threat intelligence to enhance detection accuracy and refine response actions. As organizations invest further in automation, Microsoft Copilot's AI-driven capabilities enhance operational efficiency, enabling faster triage, investigation, and response. This combination positions Microsoft Sentinel as a scalable, comprehensive solution for Level 3 organizations striving to automate workflows, improve visibility, and manage growing security complexities.

Level 3: Evolving

Environment: Processes and procedures at Level 3 are standardized across the entire organization. Guidance on security procedures and policies is provided and embraced organization-wide, and the culture of proactive responses to security is supported and communicated by leadership.

Level 3 organizations exhibit a high commitment to improving their security program, often employing a formal security leader and one or more dedicated security personnel. Visibility across the attack surface is a core objective, leading many to focus on solutions capable of aggregating, correlating, and analyzing security data throughout the operating environment, both on premises and in the cloud. Level 3 organizations often want to automate security workflows and are looking to leverage AI/ML capabilities to improve threat detection. The use of more threat intelligence is often desired at this level, as security teams understand how threat intel can help them refine security coverage.

In support of these objectives, (extended) threat detection and response tools (XDR, EDR, NDR, etc.) are commonly deployed here and are often used in conjunction with SIEM solutions. The focus is on improving the overall security operations function, including detection, investigation, and response processes.

Challenges: At this level, scalability becomes a key challenge. With alerts and supporting security signals streaming in from every aspect of the operating environment, growing volumes of security data increase noise levels and make prioritization more complex. With more data and data sources, the need for more seamless data integration is often desired to minimize data pipeline engineering and data pipeline maintenance costs. And while early investment in automation is happening, many face scalability issues, moving beyond basic process automation and further limiting overall program scalability.

SIEM Advantages: As organizations advance their security maturity, modern SIEM solutions provide a modern solution to overcome scalability and data integration challenges at Level 3. As the cost of data pipeline management grows, unification of the SIEM and XDR pipeline can accelerate detection and response and reduce pipeline management. Integrated threat intelligence can further improve threat detection and investigation, which can result in more effective response actions.

As a result, Level 3 organizations should see efficiency improvements, such as a reduction in data pipeline management costs and a further reduction in data storage costs, plus efficacy improvements, such as more contextual threat understanding, more comprehensive response actions, and further MTTR improvement.

BACK TO CONTENTS

Level 4: Mature

Environment: All aspects of the security program at Level 4 are formally managed, measured, and monitored. Security controls across the entire attack surface are optimized, monitored, measured, and reviewed at regular intervals. Often, analytical tools in place by Level 4 are capable of reporting quantitative statistics related to security controls and events.

Organizations operating at Level 4 have well-established, repeatable processes, utilizing highly integrated processes, tools, and data, often within a single security operations platform. These organizations are significantly investing in proactive security strategies, prioritizing threat hunting and risk and attack surface reduction, and operationalizing threat intelligence to inform security architecture and strategy.

A majority of mature security teams have adequate personnel and security skills on board but are typically also leveraging multiple MDR and incident response (IR) service providers to supplement many aspects of the security program.[3] Comprehensive IR plans and a disciplined preparedness process further strengthen cyber resilience.

With a focus on continuous improvement, mature teams are ripe to capitalize on the use of AI and GenAI for predictive analytics and autonomous threat mitigation, as demonstrated by 95% of respondents to a recent survey predicting that GenAI will be used for SecOps use cases over the next 12 to 18 months.[4]

Challenges: Despite the relatively mature security tools stack, many different tools, vendors, and data repositories are often still in use, adding complexity and operational management costs. As such, 69% of organizations are actively consolidating or integrating SecOps tools.[5] Despite mature technologies in use, these organizations continue to face scalability challenges, supporting infrastructure complexity across cloud, multi-cloud, and hybrid environments. And despite being relatively well funded, the high costs and complexity of operations at this level make security leaders pay close attention to the ROI of ongoing security program investments, always looking for opportunities to optimize.

SIEM Advantages: At Level 4 maturity, modern SIEM solutions enable organizations to optimize their security operations through advanced automation, AI-driven insights, and seamless integrations. These tools can help Level 4 organizations further optimize their ability to proactively manage risk by leveraging advanced analytics and AI. Integrated security platforms, inclusive of SIEM, can increase visibility and control while reducing complexity. Sentinel's cloud-native architecture can reduce complexity, especially in more diverse, distributed environments.

As a result, Level 4 organizations should see efficiency improvements, such as a further reduction in tools management and administration, more automated investigation and response activities, improved analyst throughput, and fewer escalations, plus efficacy improvements, such as more risk-driven response plans, improved security hygiene, and further MTTR improvements.

[3]Source: Enterprise Strategy Group Research Report, The Triad of Security Operations Infrastructure: XDR, SIEM, and MDR, June 2024.
[4]Ibid.
[5]Ibid.

Leveraging Microsoft Sentinel at Level 4

Microsoft Sentinel includes built-in capabilities for security orchestration, automation, and response (SOAR), UEBA, and threat intelligence. Further, Microsoft Sentinel's native integration with XDR capabilities and posture management solutions enable organizations to achieve unified visibility and control across multi-cloud, hybrid, and on-premises environments.

Microsoft Sentinel's cloud-native architectu re simplifies management of complex, distributed environments, enabling organizations to consolidate security tools and streamline operations. Its advanced analytics and threat intelligence capabilities improve proactive threat hunting and autonomous risk mitigation, reducing the time and effort needed for detection and response.

By integrating SIEM with existing SecOps tools, Microsoft Sentinel enhances visibility and control across multi-cloud, hybrid, and on-premises infrastructures while delivering measurable ROI through reduced operational costs and complexity. Additionally, Microsoft Sentinel's predictive AI and GenAI capabilities position it as a tool for organizations aiming to capitalize on autonomous threat detection, remediation, and continuous improvement at scale.

By reducing operational complexity and leveraging predictive AI and GenAI capabilities, Microsoft Sentinel positions itself as a comprehensive, innovative solution for mature security operations, capable of delivering measurable ROI and continuous program optimization at scale.

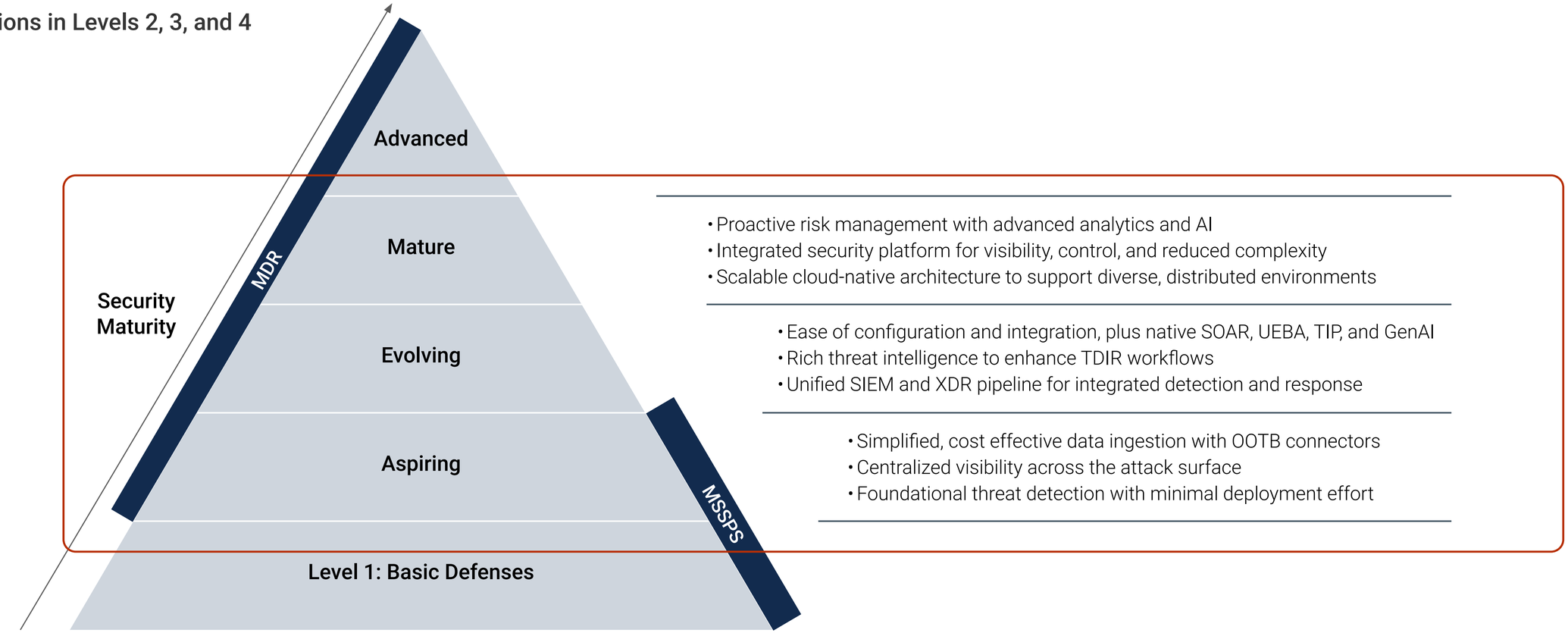
BACK TO CONTENTS

Level 5: Advanced

At this level, information security strategies and processes are continuously analyzed and improved, with a focus on the identification of opportunities to further strengthen program efficacy and efficiency. Optimization is a key focus.

Most mature of all security teams, Level 5 organizations operate in a well-funded, highly customized and optimized manner. Security leaders play a strategic role in helping the broader organization achieve its core operating objectives. Security is a frequent topic in the C-suite, and the CISO is highly accountable in supporting strategic operating investments across every function. In this highly architected environment, the security stack can be very customized, with security architects and engineers focused on tailoring every aspect of the operation to meet the specific needs of each function. The use of multiple SIEMs and multiple data lakes is common, as is a custom data pipeline capable of infusing the SecOps function with the precise data needed to provide the highest levels of security for the organization.

SIEM Applications in Levels 2, 3, and 4



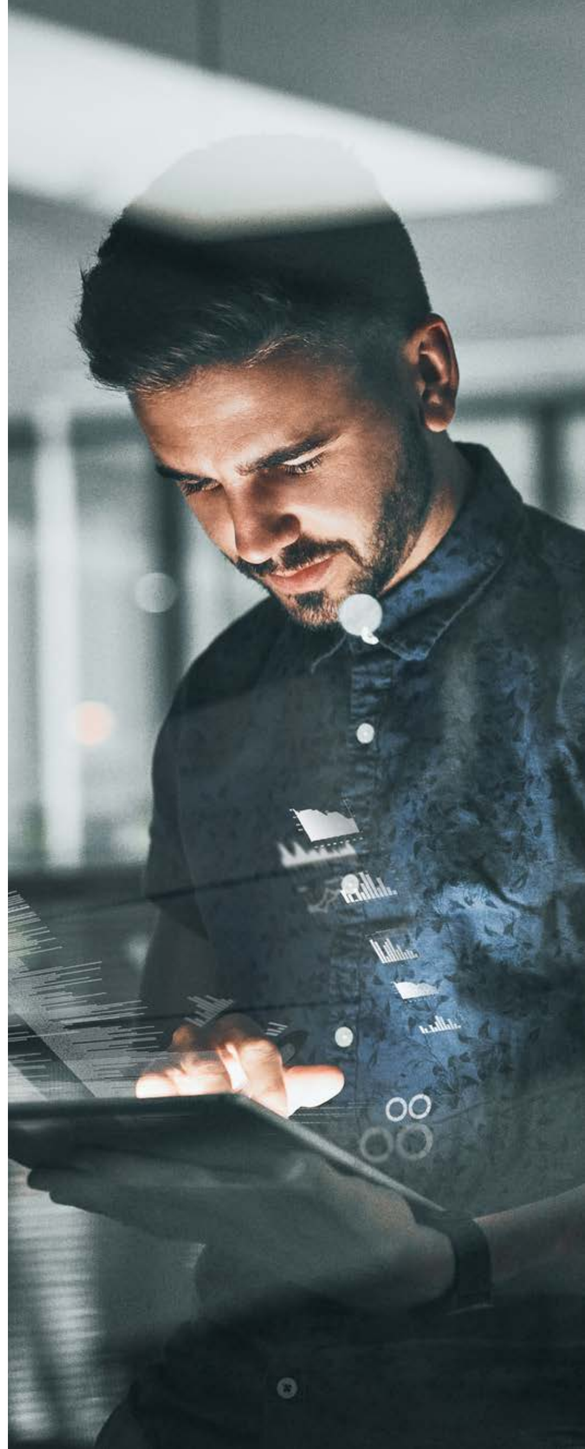
BACK TO CONTENTS

Accelerating Outcomes With SIEM

Security program development and maturity require a seamless combination of people, process, and technologies, supported by cross-functional leadership to ensure alignment with organizational objectives. As security leaders advance their programs, understanding security maturity levels helps define where they are today and what is achievable throughout their maturity journey. Central to the security maturity journey, a well-performing SecOps function is critical for achieving resilience and delivering measurable security outcomes. Further, to combat the growing complexity of today's threat landscape, organizations require scalable, integrated, and automated SecOps capabilities.

The good news is that security solution providers such as Microsoft are rapidly innovating in this area, delivering highly integrated, automated, and scalable tooling and infrastructure to power the SecOps function. Supporting all levels of security maturity, Microsoft Sentinel provides a modern SIEM solution that can help organizations enhance their SecOps performance, drive continuous program improvement, and scale security operations in line with evolving threats. Its cloud-native architecture creates an opportunity to unify security operations, seamlessly integrate existing tools, and achieve new levels of visibility, automation, and scalability.

Enterprise Strategy Group recommends that organizations explore modern SIEM solutions such as Microsoft Sentinel to help accelerate security program development and reduce complexity.



ABOUT MICROSOFT

Secure Your Multi-cloud, Multi-platform Environment With an AI-powered SIEM

Microsoft Sentinel is helping organizations transform security operations with an innovative, cloud-native SIEM that includes built-in SOAR, UEBA, advanced threat intelligence, and GenAI capabilities. Offering comprehensive detection, investigation, and response capabilities across multi-cloud and multi-platform environments, Microsoft Sentinel empowers analysts to confidently protect their organizations from today's and tomorrow's threats with unparalleled visibility, cloud flexibility, and comprehensive coverage.

LEARN MORE

Microsoft

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.