Microsoft Security

Extending SIEM: How to get the most from your security stack

Contents

For more than a decade, SecOps teams have relied on security information and event management (SIEM) systems to monitor and analyze security alerts across their digital infrastructure.

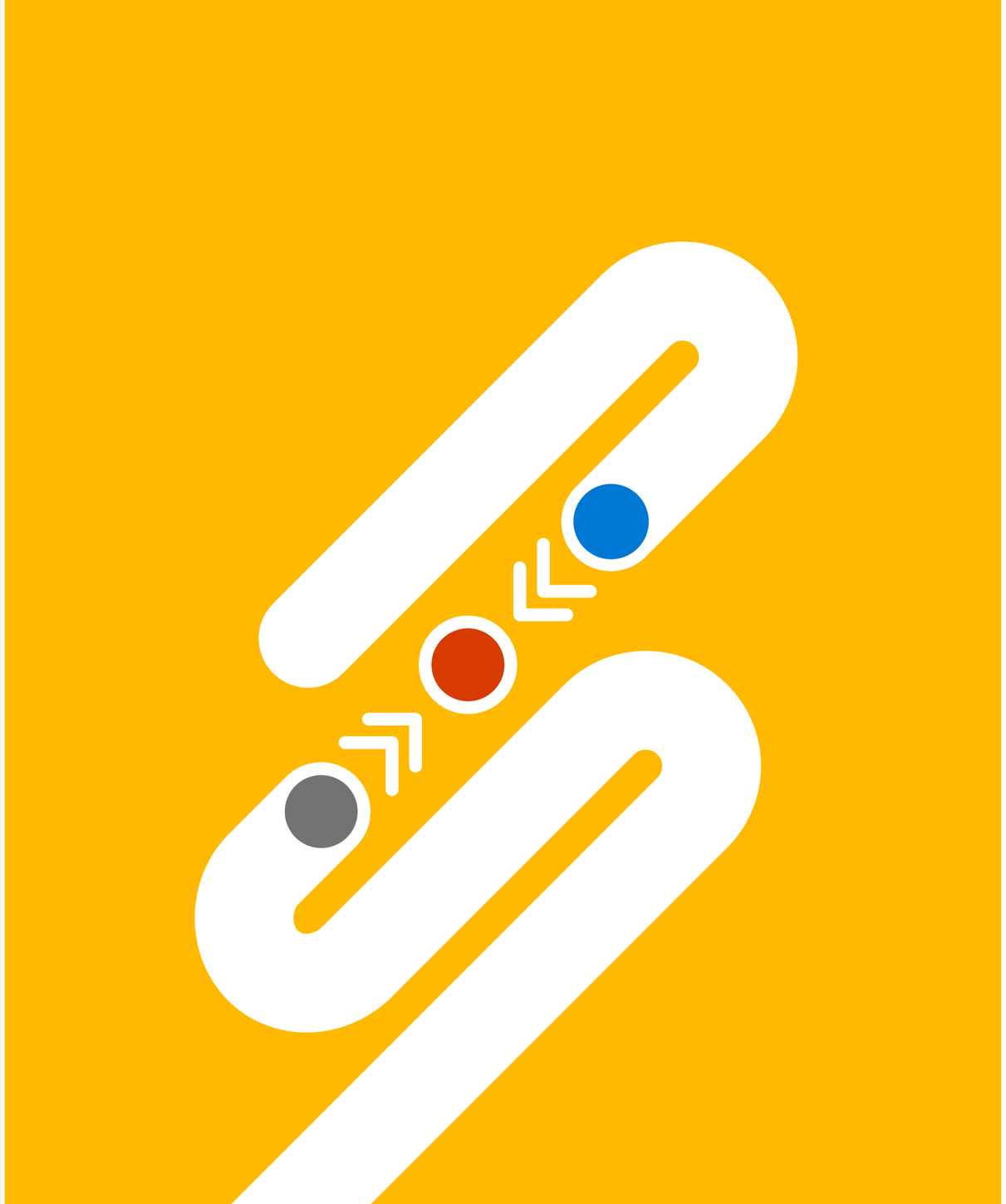
As the volume and sophistication of cyberattacks have grown, security teams added a myriad of tools to their SIEM systems in an attempt to increase visibility into vulnerabilities and active threats.

Through it all, SIEM systems have remained a powerful tool in the SecOps toolbox. Organizations continue to invest heavily in SIEM, averaging $580,000 per year for staffing, infrastructure, licensing, and ongoing software costs, according to IDG research. The majority of those organizations use an on-premises SIEM platform, but one-third have deployed a cloud-based solution to take advantage of some of the cloud's cost and performance efficiencies.

As organizations move more of their IT stack to the cloud, cloud-based security tools such as SIEM are following. A variety of cloud-based services supplement SIEM solutions with various security management functions. While these services are critical in helping SecOps teams identify issues, close vulnerabilities, and respond to active threats, they have created additional layers of complexity and unfiltered noise that may actually increase risk instead of reducing it.

SecOps teams need a better option to identify, protect, and defend against an ever-changing attack surface. Extended detection and response (XDR) platforms are emerging as a way to strengthen a cloud-native SIEM for greater threat protection, smarter telemetry, advanced automation, and increased efficiency.

In this e-book, we examine the challenges of using point solutions with SIEM and explain how integrating SIEM with XDR can make SecOps more manageable while increasing protections across the enterprise.



SIEM is essential–and it can be even better

SIEM offers security teams critical visibility, but SecOps teams know more is needed for truly effective risk mitigation. As enterprise perimeters expanded beyond the corporate walls, SecOps teams added a variety of third-party tools and services to get more out of their SIEM solution, and maximize protection across cloud and on-premises environments.

Common cloud-based services used to augment SIEM configurations include:

Cloud Access Security Broker (CASB)

A CASB serves as a "blanket" on top of a cloud-native SIEM. It collects log information from multiple sources and exposes anomalous events and threats, which makes the SIEM cloud-aware and gives it the information needed for remediation.

Cloud Security Posture Management (CSPM)

CSPM automates the identification and remediation of risks across cloud infrastructures and also applies best practices for cloud security in multi-cloud environments. CPSM continuously monitors risk in the cloud and predicts where it may appear next. It can be integrated with the SIEM to streamline visibility and capture insights and context about misconfigurations and policy violations.

Cloud Workload Protection Platform (CWPP)

CWPPs are security offerings that target the unique protection requirements of workloads in modern hybrid, multi-cloud environments. CWPPs give IT and security teams the ability to discover and protect workloads that have been deployed in on-premises and public cloud environments. CWPPs allow SecOps teams to understand vulnerabilities with insights from research, and help secure workloads across virtual machines, containers, databases, storage, app services, and more. They are often used in tandem with CSPM tools.

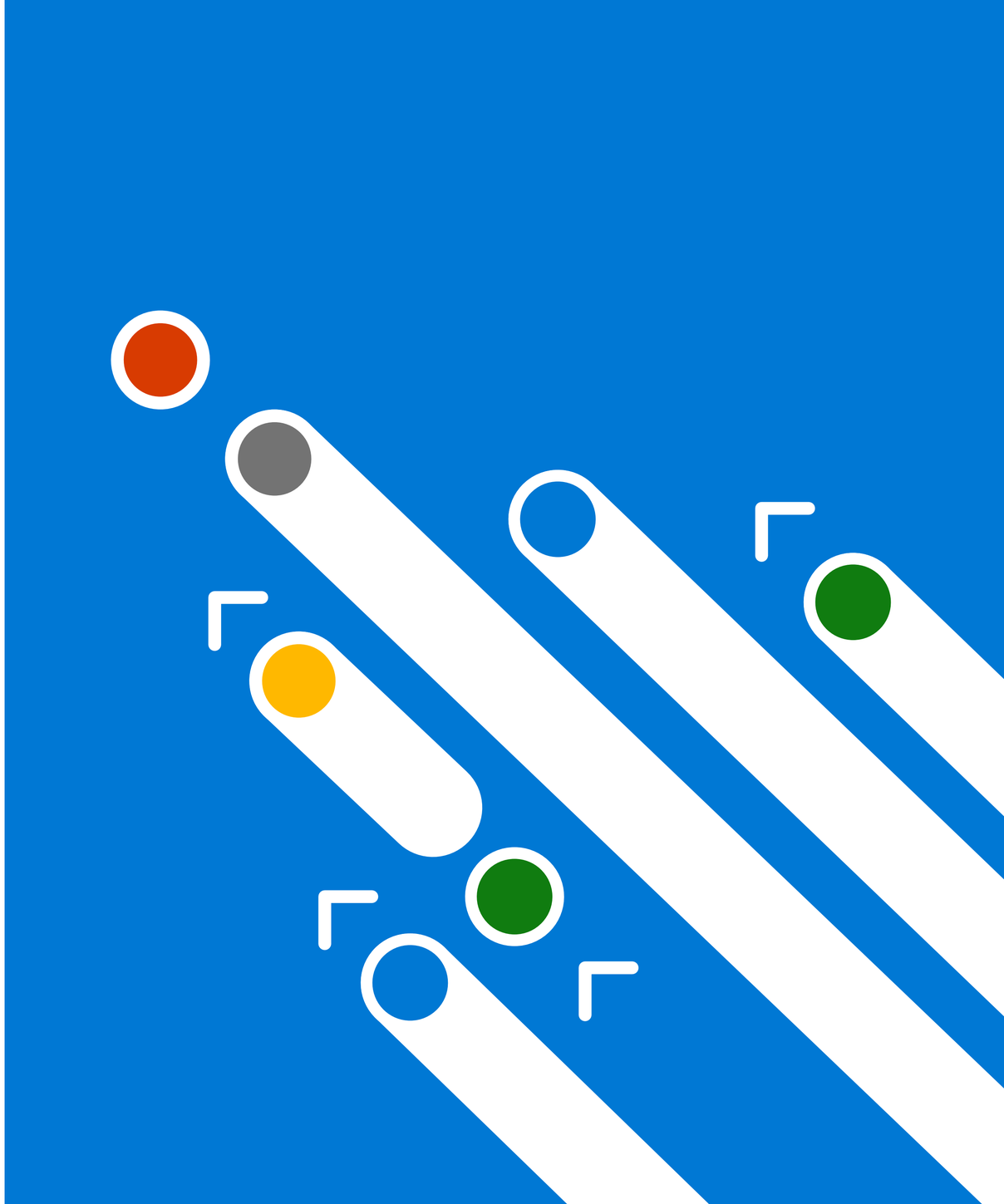
Endpoint Detection and Response (EDR)

EDR determines if malware has been installed on an endpoint device and finds ways to respond. Once installed, EDR solutions collect data from many different sources and stores it in a central database.

While all of these tools offer important features that can help a SIEM system improve protection, integrating and managing them presents its own set of challenges.

Too many solutions add complexity and challenges

A patchwork of security tools and strategies make it difficult to meet the demands of today's distributed enterprise. One-off security solutions can be time-consuming to deploy and inevitably contribute to a daunting mix of consoles and reports that are tough to monitor and manage.



Reducing complexity in security infrastructure was a top-five priority for security leaders surveyed in Foundry's 2021 Security Priorities study. One in five organizations said this complexity makes it difficult to retrieve timely, actionable intelligence from security systems.

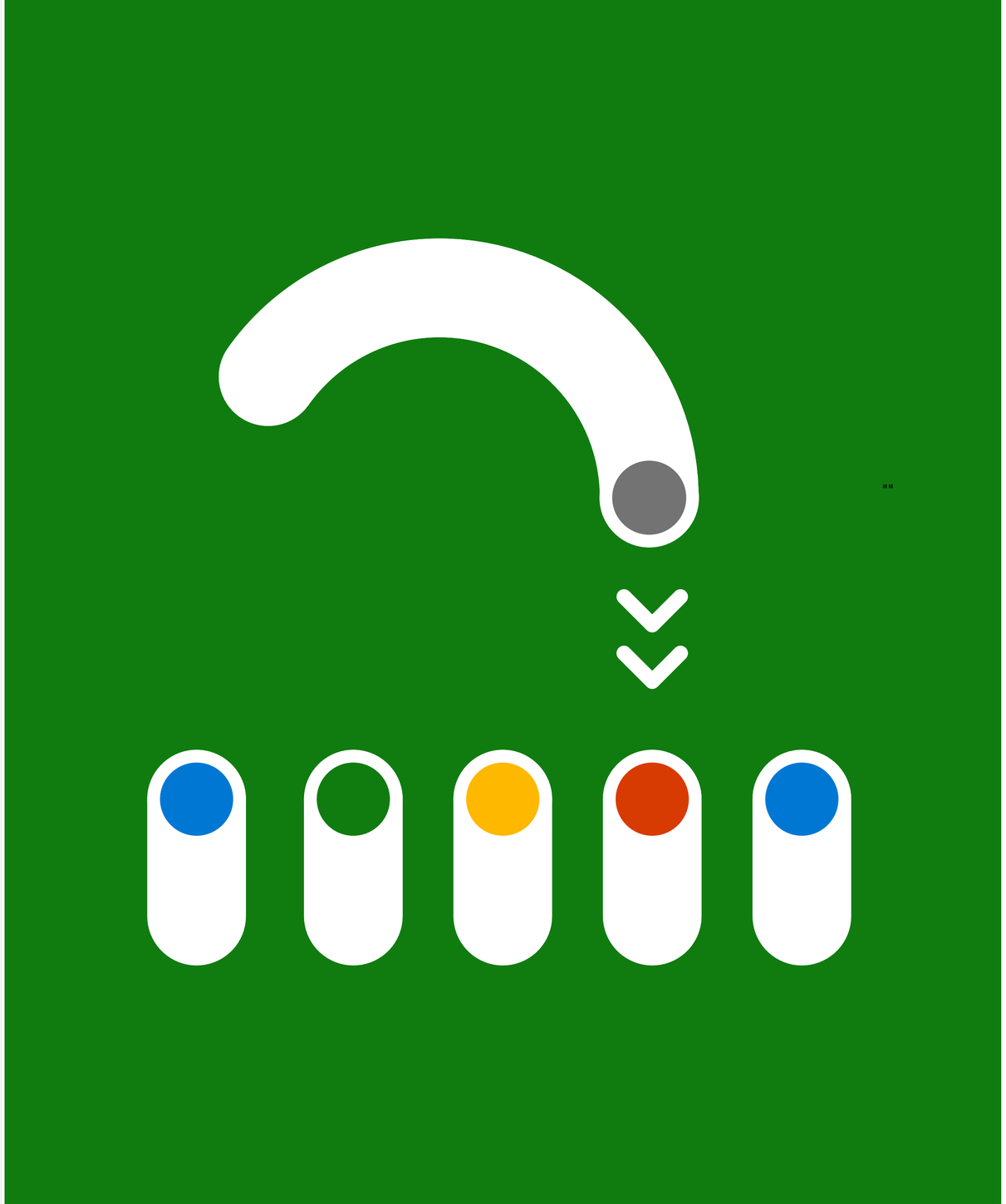
Defenders need solutions that work seamlessly with SIEM to deliver integrated protection and coordinated detection and response. All components of the security stack must work in concert to find and remove sophisticated adversaries wherever they lurk.

Given the enormous amount of security signal generated by the digital ecosystem, modern solutions also need built-in artificial intelligence (AI) and automation to process routine tasks and filter high-value alerts out from all of that noise. SIEM needs to evolve beyond visibility and log data to offer SecOps teams a more proactive approach to identifying and mitigating threats, while also automating many tasks and offering the simplified, seamless level of management CISOs require to reduce risk.

Moving to a cloud-based SIEM is an important step in that direction. A Forrester Consulting Total Economic Impact™ (TEI) study found that organizations deploying the Microsoft Sentinel cloud-native SIEM solution saw significant cost savings and an increase in security operations efficiency. Among the benefits:

- Microsoft Sentinel reduced the number of false positives and the effort required by analysts to investigate alerts, leading to $2.2 million in efficiency gains.
- Microsoft Sentinel was less expensive than a legacy SIEM solution, saving $4.9 million on licensing, storage, and infrastructure costs.

Microsoft Sentinel reduced management effort by 56%, saving $1.2 million.



Get more from your SIEM with XDR

A cloud-native SIEM solution provides valuable insights, giving SecOps teams a comprehensive command-and-control experience across the entire enterprise. It can collect and analyze data across the entire organization to detect, investigate, and respond to incidents that cross silos, and can enhance SecOps efficiency with customizable analytics and built-in automation.

Instead of layering on multiple point solutions that add counterproductive complexity, CISOs should consider integrating XDR as a more effective complement to SIEM, helping to gather and process telemetry from across the IT stack in a single dashboard. XDR provides depth of knowledge into specific threats, while SIEM provides broad visibility for mananging security operations from a bird's-eye view.

XDR takes security management beyond endpoints to help SecOps teams investigate attacks by examining specific resources across platforms and clouds. XDR applies threat intelligence to aggregated data to more effectively identify trends, allowing SecOps teams to more quickly spot vulnerabilities, detect attacks, and respond using auto-remediation. The technology can help reduce the number of alerts that the security team must investigate by using correlation and behavioral analysis on consolidated threat data to eliminate false positives and low-fidelity alerts.

Microsoft's XDR solution includes Microsoft 365 Defender and Microsoft Defender for Cloud, which automatically collects, correlates, and analyzes security signals and threat alert data involving endpoints, users, applications, the internet of things, and cloud workloads. It uses AI and automation capabilities to stop attacks faster and remediate affected assets.

A Forrester Consulting TEI study found that organizations using Microsoft 365 Defender reduced the likelihood of a security breach by 60% and decreased the time required for investigation and remediation of security incidents by 89%.

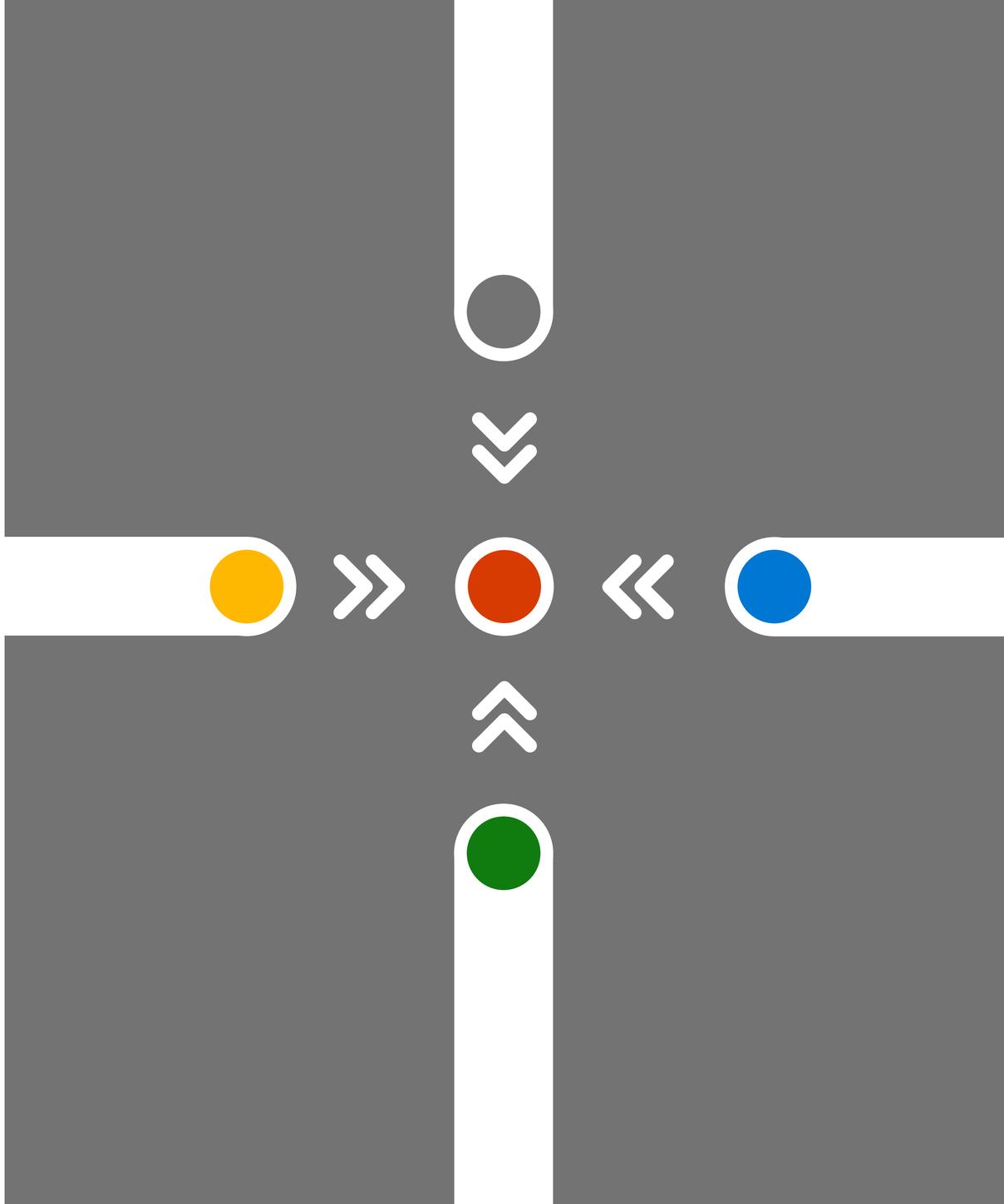
Because of its depth of functionality and automation capabilities, XDR also can help CISOs address the pressing challenges of the cybersecurity talent gap. An (ISC)² Cybersecurity Workforce Study puts the global cybersecurity talent shortage at more than 4 million people. With skilled security professionals in high demand, SecOps teams are often overwhelmed with alerts and a backlog of incidents that need to be investigated and potentially remediated.

The Forrester Consulting TEI study found that Microsoft 365 Defender's ability to highlight cross-platform incidents contributed to increased efficiency for security teams, adding an estimated $6.7 million to an organization's bottom line. Improved incident response time saved another $3 million.

Microsoft 365 Defender reduced the likelihood of a security breach by 60 percent

Integration and synchronization provide broader threat context

Integrating SIEM and XDR will allow systems to share even more incidents, schema, and alerts, giving SecOps teams a unified view and the ability to seamlessly drill down into individual incidents for more context. Together, Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender offer broad and deep visibility across organizations while improving SecOps efficiency and response times.



Connectors allow organizations to stream data from the Microsoft XDR solution into Microsoft Sentinel so SecOps teams can view, analyze, and respond to Defender alerts, and the incidents they generate, in a broader organizational context.

For example, a team using Kusto Query Language (KQL) to explore log analytics in Microsoft Sentinel can use that same query in Microsoft 365 Defender to look at performance-related data or follow up on an alert. Information between the two systems is synchronized bidirectionally, so security analysts can easily move from one tool to the other to identify, remediate, and close an incident. When an incident containing a security alert is closed in one system, the corresponding alert in the connected system will be closed automatically.

By feeding XDR data into SIEM, organizations can derive more value from both technologies. An integrated SIEM and XDR environment provides a single dashboard for viewing and managing threats across multicloud, on-premises, and hybrid environments. It allows for billions of pieces of signal data from XDR and other sources to be reduced to thousands of alerts and tens of incidents, thereby minimizing alert fatigue and false positives for SecOps teams.

Integration enhances the ability of SecOps teams to perform centralized, context-based threat detection, analysis, and response. SIEM platforms offer log management and retention capabilities for XDR data, so it is available for threat investigation and forensic analysis. This can enable better insight into past security incidents so measures can be taken to prevent the same events from happening again.

Integrated threat protection, detection, and response with Microsoft SIEM and XDR

Attacks are escalating in frequency and sophistication. Legacy tools are no longer enough to keep up with the evolving threat landscape, and CISOs need better visibility across their digital environments.

Microsoft's vision for SIEM and XDR is to deliver a single, integrated solution to help SecOps teams stop attacks and keep their organization safe. Microsoft SIEM and XDR solutions extend beyond native and hybrid models to provide the depth of automated correlation from XDR, integrated with the breadth of a cloud-native SIEM.

Learn more about how integrated threat protection can help stop breaches across your entire organization.

Microsoft Security

©2022 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.