infopulse
Part of TietoEVRY Group

EBOOK

SOC Adoption: Three Scenarios to a Better Security Posture

Table of Contents

Over the past year, businesses across the globe leaped several years ahead in terms of digitization. The massive pivot to remote work and rapid adoption of emerging technologies placed a greater strain on security teams.

> **59% of respondents said their organization had faced a material or significant cybersecurity incident in the past 12 months.**
>
> *EY Global Information Security Survey 2020*

Many leaders found themselves underprepared to confront the reverse side of digitization — an expanded portfolio of digital assets and endpoints, requiring robust protection and 24/7 monitoring. Cloud-born and cloud-based IT infrastructure requires reinforcement. Legacy and on-premises systems command regular security patches and maintenance as well. Newly set and expanded data repositories need to be secured in line with the industry compliance standards. At the same time, security teams (and oftentimes individual IT personnel) are already overwhelmed with the remote workforce support.

To bridge the widening gap between IT security capabilities and present-day operational demands, an increasing number of leaders are considering Security Operations Center (SOC) adoption. In this eBook, we offer an in-depth view of SOC operations adoption, setup, and management.

What is SOC?

SOC SERVICE PROVIDERS ALSO PERFORM REGULAR ASSESSMENTS OF THE COMPANY’S OVERALL SECURITY POSTURE

Security Operations Center (SOC) is a dedicated business unit, operating under a set of defined procedures and employing technology to continuously monitor, analyze, respond, and prevent cybersecurity incidents.

Acting as a hub, SOC teams take full control over the pre-established safe operating procedures (SOPs) to attain as much as possible of the corporate’s technical environment and infrastructure, as well as ensuring compliance with the regulatory standards. SOC teams are responsible for monitoring the company’s infrastructure (on-premises and in the cloud), networks, connected devices, and data exchanges between them.

Apart from assuming the “watch guard” role, SOC service providers also perform regular assessments of the company’s overall security posture and suggest further improvements in response to emerging threats.

Enterprise SOC responsibilities include:

- Proactive security monitoring
- Development and execution of an incident management plan
- Threat response and remediation
- Log management
- Alert prioritization, management, and response
- Root cause analysis
- Vulnerability assessment and management
- Infrastructure and network hardening

In essence, SOC teams establish the protocol for preventive security maintenance and act accordingly. Proactive detection and cybersecurity incident response mechanisms should already be in place prior to the establishment of the SOC cybersecurity unit.

How Does the SOC Work?

The SOC stands at the frontline of enterprise security, scanning the corporate requirements for threats, vulnerabilities, breaches, and non-compliance round the clock. SOC primarily performs supervisory and investigative functions. The unit acts as a secondary structure to baseline IT security and cybersecurity teams and processes.

IT SECURITY

People, processes, and technology, aimed at protecting corporate IT assets against internal incidents such as accidental data breaches, insider attacks, misconfigurations, and non-compliance.

CYBERSECURITY

People, processes, and technology, aimed at protecting organizations against targeted attacks (hacking) and external security threats (malware, DDoS attacks, etc.).

The SOC acts as a controlling unit, ensuring that all IT security and cybersecurity policies are in place, properly executed, and regularly updated in response to emerging threats. In addition to controlling, a well-established SOC also performs the following four cornerstone functions:

1

MONITORING

SOC teams analyze the entire IT environment and ensure high endpoint protection against insider and external threats. Using an array of tools for asset discovery, scheduled infrastructure scanning, and real-time monitoring, SOC teams ensure early detection of potential threats and other suspicious activities.

2

THREAT HUNTING & PREVENTION

With a fit-for-purpose toolkit and round-the-clock availability, a SOC team can achieve proactive detection of emerging threats and schedule focused follow-up actions — security patching, policy adjustments, customized risk treatment plans, or new security systems implementation.

3

THREAT INVESTIGATION & INTELLIGENCE

All the threat intent, collected by the SOC teams, is further analyzed and translated into new security insights for the company. Using the gathered information on the nature, origin, and potential impact of the threat, SOC analysts can develop new recommendations for systems hardening, vulnerability mitigation, and updates to the Security Awareness program.

4

RESPONSE

Armed with sufficient data and a robust toolkit, a SOC team can rapidly respond to the most elaborate attacks, isolate threats, and mitigate the impact on business operations and sensitive data.

62%

Of security incidents occur due to negligence[1]

$11.45 million

The average total cost of insider threats[2]

$368 million

The average total cost of a data breach[3]

280 days

The average time to identify and contain a breach[4]

[1] Observe IT: 2020 Cost of Insider Threats Global Report

[2] Ibid.

[3] IBM: Cost of a Data Breach Report 2020

[4] Ibid.

Types of SOC Operations by Maturity Levels

	Level 1	Level 2	Level 3	Level 4	Level 5
Capabilities Present	Baseline security monitoring and response Ad hoc log data collection and management Entry-level endpoint detection response	Security event centralization Reactive threat intelligence workflows Basic security analytics Automated alert prioritization Manual vulnerability assessments	Documented monitoring process Analytics-based threat intelligence Incident management and response plans Proactive threat detection Proactive threat identification Automated workflows for threat investigation	Consolidated log data and security event centralization Server, endpoint, and network forensics Mature threat detection and response processes ML/DL-based threat response tools KPI/SLA-based performance	24/7 security monitoring, prevention, and detection systems Proactive capabilities to identify and mitigate vulnerabilities Mature SIEM architecture, SIEM log sources, SIEM correlation rules Cross-functional integration Real-time threat intelligence Workflow and response automation Proactive and iterative threat hunting capabilities Strong SOC program governance

BEFORE SOC IMPLEMENTATION, YOU SHOULD START WITH AN AUDIT OF THE EXISTING SECURITY PROCESSES

SOC adoption outcomes and success rates strongly correlate with the company's overall maturity levels in terms of security and ITIL Service Management. Given the complex nature of implementing SOC, we always recommend that our clients start with a preliminary audit of the existing security processes, technical capabilities, and security needs.

Based on the above, organizations vary between Level 1 and Level 5 in terms of security maturity — and readiness for different types of SOC adoption scenarios respectively.

Level 1

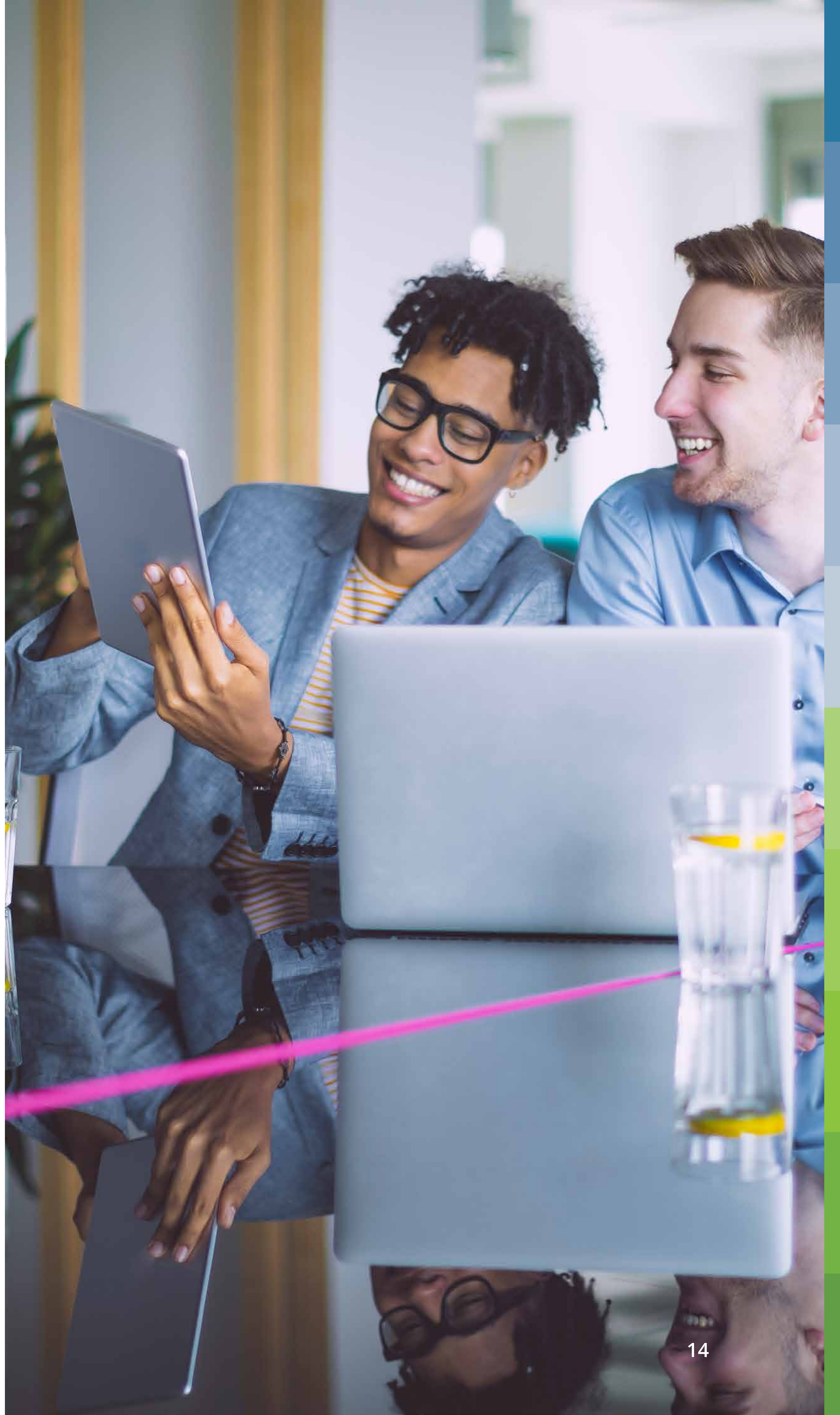
At ground level, companies already have the following security controls in place:

- Baseline security monitoring and response, aligned with compliance requirements
- Ad hoc log data collection and management
- Entry-level endpoint detection response
- No formal incident response and management plans.

Such companies have the minimum security requirements covered. However, they are not in a good shape to effectively respond to targeted attacks and remain vulnerable to insider breaches. In most cases, low maturity stems from the lack of security specialists and domain expertise for establishing effective threat detection, prioritization, and management.

RECOMMENDED SOC ADOPTION SCENARIO:

- Security Assessment
- Assets identification, risk level estimation, defining use cases and response scenarios
- Shared or Dedicated SOC as a Service
- Documenting and systematization of internal processes



Level 2

At this stage, businesses rely on manual and proactive threat response, yet standardization is lacking. This often results in sporadic security coverage and prolonged response to security incidents.

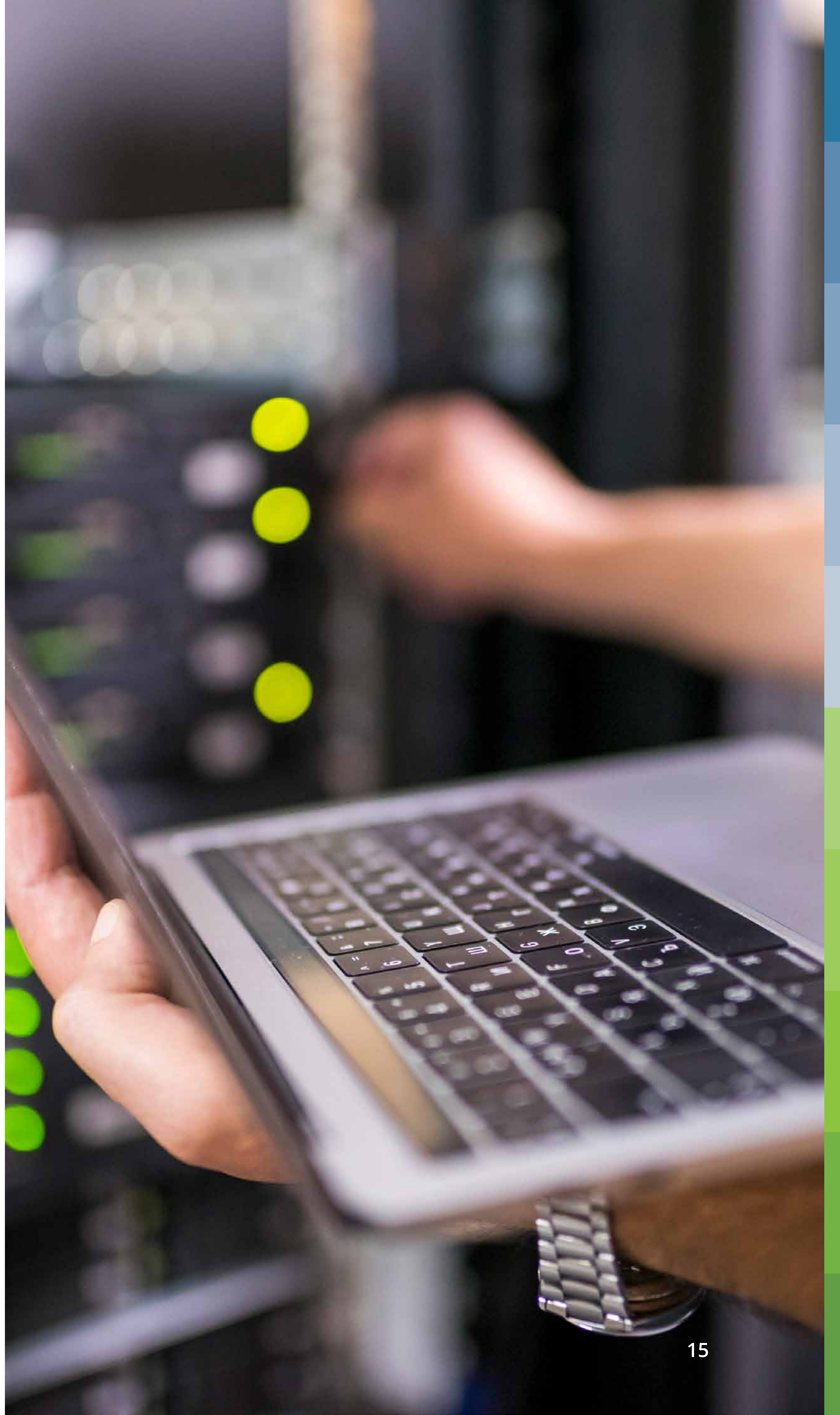
At Level 2 companies already have:

- Established security event centralization capabilities
- Reactive threat intelligence workflows
- Entry-level analytics capabilities
- Automated alert prioritization
- Manual vulnerability assessment.

The above results in a higher degree of security. However, the company has capabilities to detect major threats, rather than identify early signs of breach or exposure. Security teams still have blind spots, especially when it comes to sophisticated attacks. Visibility into both internal and external threats is moderate.

RECOMMENDED SOC ADOPTION SCENARIO:

- IT Security Assessment, including the existing Infrastructure Event Management
- Cybersecurity Consulting
- Cost-efficient approach to data collection and processing
- Risk assessment
- Business-critical assets monitoring
- Documenting basic processes, procedures, and responsibilities
- Shared or Dedicated SOC as a Service



Level 3

Level 3 organizations rely on documented, consistent security best practices and also leverage security tools to streamline repetitive chores.

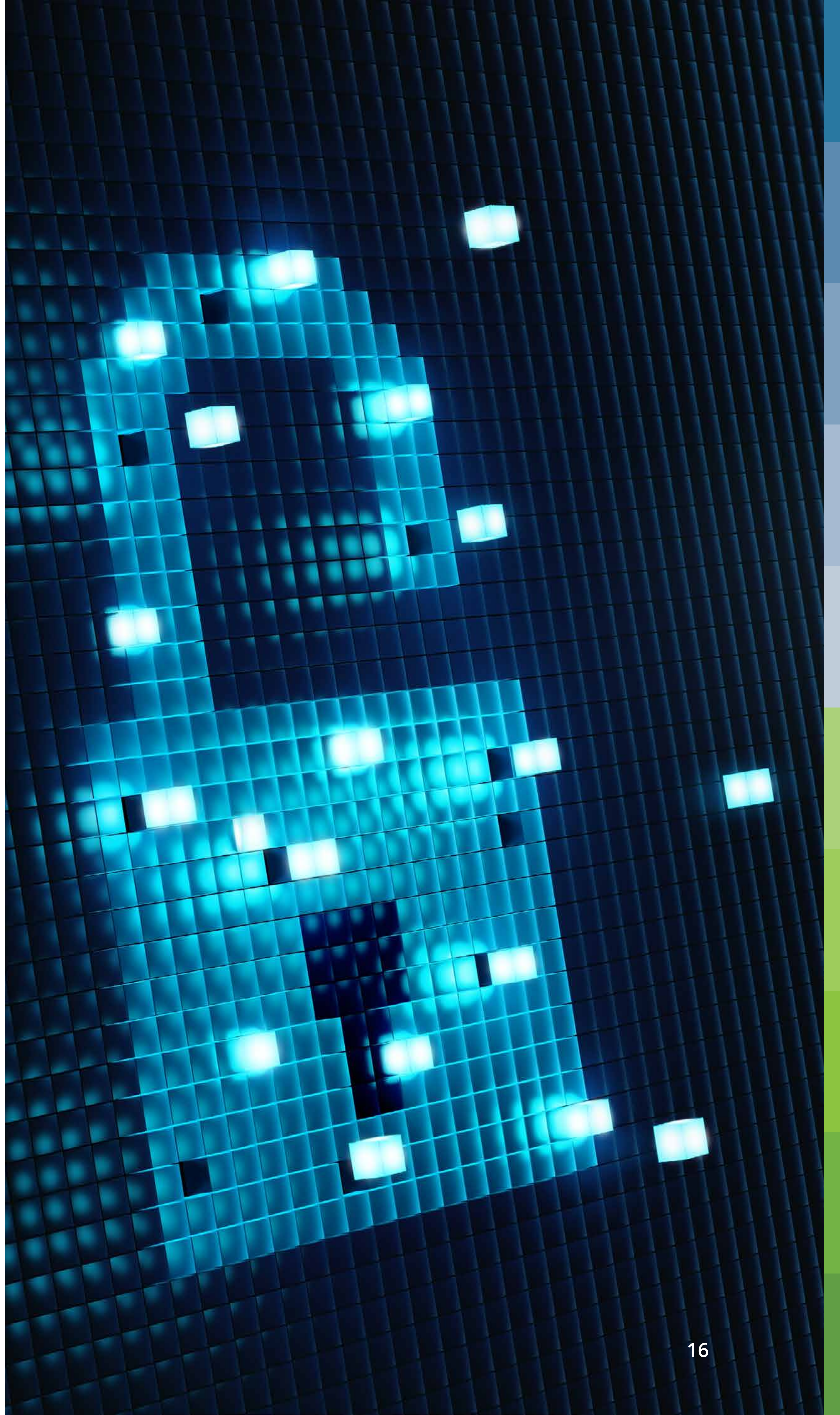
The range of capabilities includes:

- Formalized monitoring process
- Analytics-based threat intelligence
- Established incident management and response plans
- A wider range of threat detection capabilities
- Proactive threat identification
- Automated workflows for threat investigation.

SOC solutions and teams can be effectively established at this point to drive further operational improvements in terms of visibility, hardening, and proactive monitoring. Level 3 organizations are in a good position to detect incidents early but they may require a longer time to respond due to somewhat lacking cross-functional coordination abilities.

RECOMMENDED SOC ADOPTION SCENARIO:

- Security Assessment
- Define and measure KPIs for formalized monitoring process
- Utilize commercial threat feeds
- Cost-efficient approach to data collection and processing
- SOC as a Service or SOC delegation



Level 4

Level 4 organizations can decisively respond to an array of security incidents thanks to a well-documented response process, backed by automated threat detection, investigation, and analytics tools.

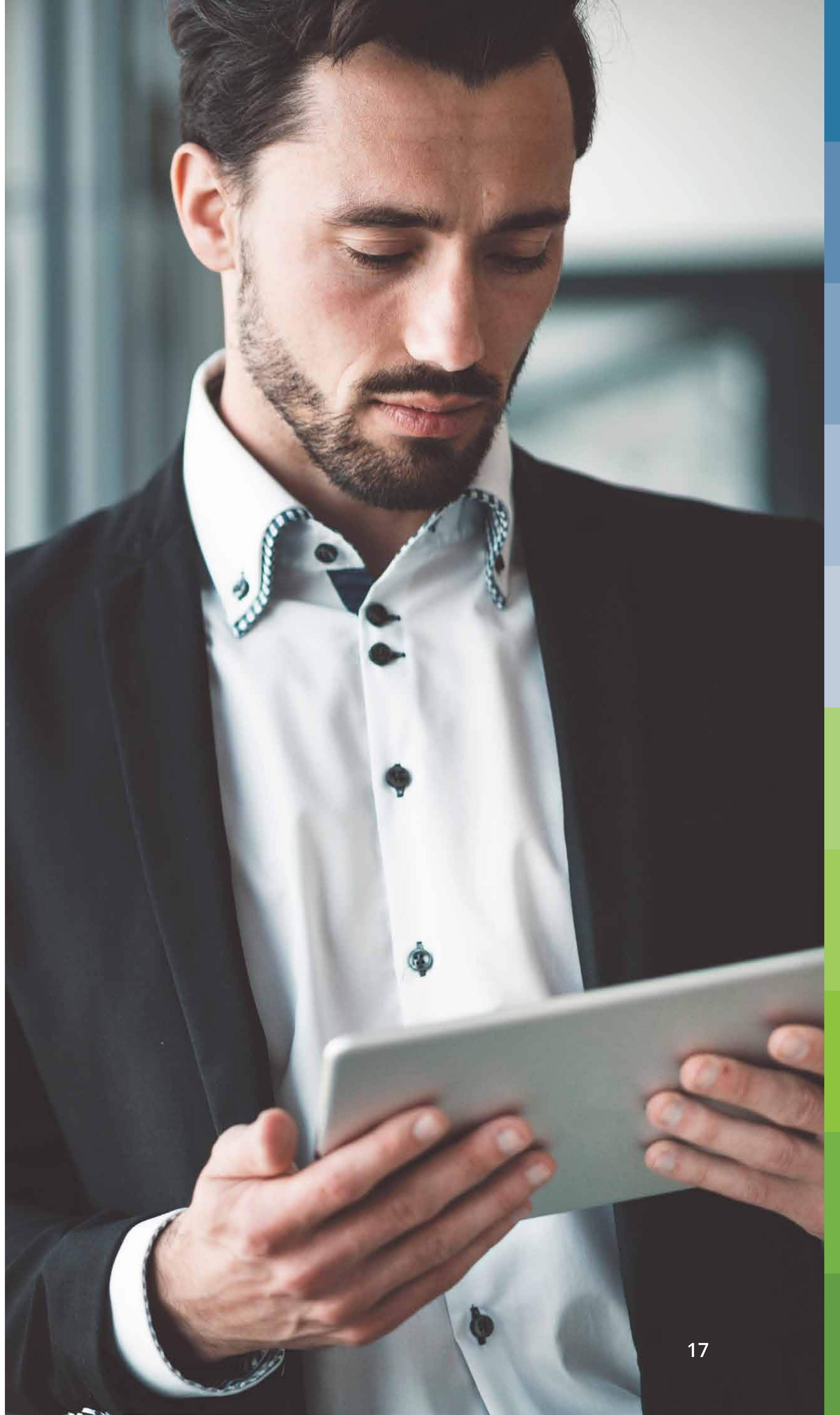
The following security facets are in place:

- Consolidated log data and security event centralization
- Server, endpoint, and network forensics
- Mature threat detection and response processes
- Machine learning solutions for anomaly detection
- KPI/SLA-based performance capabilities.

Level 4 organizations can rapidly handle emerging threats at the onset stage and effectively collaborate across the board to drive company-wide security improvements. Such businesses are also likely to have 24/7 physical SOC teams or rely on a SOC as a service provider.

RECOMMENDED SOC ADOPTION SCENARIO:

- Security Assessment
- Threat response automation
- Cost-efficient approach to data collection and processing
- Utilizing monitoring data for insightful decision-making
- SOC as a Service or SOC delegation



Level 5

Security is a company-wide endeavor, actively supported by all stakeholders. Level 5 organizations assume a proactive stance on threat management and security. They have:

- Corporate-wide agenda for ensuring certain levels of security and driving continuous improvement
- 24/7 security monitoring, prevention, and detection systems in place
- Proactive capabilities to identify and mitigate vulnerabilities
- Mature SIEM architecture and supporting SOC technologies for maximizing their staff's efficiency.

Typically, Level 5 organizations operate in regulated industries — finance, telecom, and healthcare, among others — and their aspirations to security excellence are also driven by regulatory and compliance requirements.

They are also a prime target for cybercriminals but have the resilience to withstand targeted attacks and stay one step ahead of emerging threats.

RECOMMENDED SOC ADOPTION SCENARIO:

- Cybersecurity consulting
- CIRT (Cyber Incidents Response Team) cooperation with government entities and other enterprises
- Proactive detection of zero-days threats
- SOC delegation or SOC maintenance

Three Ways to Introduce SOC to Your Organization

Traditionally, SOC implementation was an option reserved for transnational enterprises with significant budgets for setting up in-house operations. In recent years, however, alternative SOC adoption scenarios have emerged, offering a better price-to-value ratio and lesser degree of operational challenges in implementation.

In this chapter, we discuss **three routes to SOC adoption:**

- In-house SOC setup and maintenance
- SOC maintenance outsourcing
- Managed SOC

SOC OPERATIONS ESTABLISHMENT AND MAINTENANCE

As the name implies, this SOC adoption model assumes proactive SOC adoption guidance. **An experienced security provider will conduct an assessment of your current processes, infrastructure, and compliance requirements** to come up with necessary security improvements, operational changes, and security investments.

Such "build" scenarios assume assistance with the following:

- Formalize the list of key SOC service functions that will guide the daily processes and procedures for the staff.
- Determine all the required processes and services required to support the corporate security operations (varies depending on the company size, industry, and customer base).
- Establish the optimal SIEM architecture, identify the necessary toolkit, and create a prioritized list of security technology investments.
- Develop a SOC staffing schedule, formalize the required roles and responsibilities each role entails. Create a tiered SOC structure and assign responsible people for managing different event types.
- Create a set of internal regulations, such as playbooks, policies, procedures, escalations, and management plans to standardize SOC operations and ensure response and coverage.
- Suggest workflow automation scenarios and investments in best-in-class predictive security analytics solutions or anomaly detection algorithms.
- Guide through the adoption process and facilitate alignment of the newly established SOC team with the company-wide ITIL service management standards.

A SECURITY SERVICE PROVIDER ALSO ENABLES SOC MAINTENANCE SERVICES AND MAY ALSO ASSIST WITH HIRING FOR SUCH KEY ROLES AS SECURITY ANALYST (L1, L2), ETC.

BUSINESS CASE

A transnational telecom company already has an established network operations center (NOC), responsible for monitoring and responding to threats originating from network devices. Internal business user security is handled by the IT department. However, both units are understaffed, have limited visibility into each other's operations, and, respectively, underperform when it comes to analyzing external or insider threats, as well as ensuring 24/7 threat protection.

HOW SOC CAN HELP

In such a case, establishing a SOC team could help **consolidate the existing security efforts**, **achieve better visibility** into the entire infrastructure, and **enhance threat investigation**, mitigation, and prevention capabilities. With core SOC functions performed by an external service provider, internal teams can better focus on ensuring baseline user security, timely implementation of new security policies and high standards of IT services delivery to corporate users.

Benefits

- Expert SOC guidance, minimizing the chances of sub-par security decisions
- Acute advice and consultancy on existing practices and necessary improvements
- Possibility to augment your security teams with provider-supplied security talent
- Sustainable, low-risk, and faster establishment of SOC operations
- High operational performance, backed by established metrics and SLAs
- Maintaining a separate SOC in-house also ensures higher data security and compliance

Challenges

- **High maturity required:** Organizations with low cybersecurity maturity (under Level 4), insufficient security staff, and a low level of operational experience will struggle to operate a new SOC unit post-establishment. Companies that cannot distinguish between reactive vs proactive approaches to security are unlikely to benefit from this option.
- **Strong ITIL security management process:** Businesses that already have a strong IT servicing backbone and a bench of security talent (or ability to hire it) are stronger candidates for ad hoc SOC implementation. By combining the external know-how in managing SOC with internal security knowledge, your company can rapidly transition to the next level of security operations.
- **SOC establishment costs.** Maintaining a 24/7 in-house SOC team is a budget-demanding initiative. Apart from base salaries, you should factor in the recruiting costs, bonus payments for holiday hours, staff retention, and training. Enterprises with an average cybersecurity budget of $31 million, spend a third of it on SOC[5]. It follows that in-house SOC units may be cost-inhibitive for everyone, but nationwide or global organizations.

[5] Security Boulevard: Businesses Now Spend a Third of Their Cybersecurity Budget on SOC

CASE STUDY

How Infopulse Laid the Ground for SOC Implementation

ONE OF THE BIGGEST TELCOS IN UKRAINE

ONE OF THE BIGGEST TELCOS IN UKRAINE

A nationwide telecommunication service provider planned to build a SOC with a SIEM system in its core. The customer decided to test Azure Sentinel and learn its capabilities. An essential requirement was to provide efficient control over expenses.

Infopulse conducted an assessment of the existing IT infrastructure and licenses and balanced connections focused on both costs and SOC capabilities by defining unbillable (Microsoft) & billable (3rd party) systems & solutions. The implementation included five test cases:

1. **DETECTION OF UNAUTHORIZED FILES COPYING FROM SHAREPOINT.**
2. **DETECTION OF NON-TYPICAL USERS' AUTHORIZATION IN CLOUD SERVICES** (for Azure AD users).
3. **DETECTION OF NON-TYPICAL USERS' AUTHORIZATION BY USING BLOCKED USER ACCOUNTS** (for Azure AD users).
4. **PHISHING EMAILS DETECTION CONFIGURATION AND TESTING** (e.g., users forward suspicious emails for subsequent self-analysis).
5. **CONFIGURING AND TESTING A CASE THAT USES DATA RECEIVED FROM ONE EXTERNAL SOURCE** (e.g., Check Point FW).

BUSINESS VALUE

A pilot project demonstrated the advantages of Azure Sentinel as a cloud-native SaaS solution and integrated SIEM/SOAR with automation:

- Tested and proved Azure Sentinel capabilities in terms of seamless integration with the Microsoft cloud ecosystem.
- Optimized solution costs by analyzing and assessing the viability of implementing connections with the third-party systems.
- Provided a report with recommendations on further implementation steps.

The client is now planning to utilize Azure Sentinel as part of their Security Operations Center.

Contact our experts to learn how we can optimize your security expenses ›

SOC SERVICES OUTSOURCING

In the UK, over 48% of businesses[6] experience a shortage in basic cybersecurity skills. Cyber security personnel does not have sufficient capabilities to perform tasks put forward in the Cyber Essentials scheme, and do not receive support from an external cybersecurity partner.

Globally, the matters are equally complex. While 51% of executives[7] plan to add more full-time cybersecurity personnel to their teams, most struggle to find suitable candidates. In particular, roles related to cloud security and security analysis are in the shortest supply.

27%

Of UK businesses have a gap in incident response capabilities (and do not outsource this task)[8]

30%

Of UK businesses have a gap in areas such as penetration testing, forensic analysis, and security architecture

50%

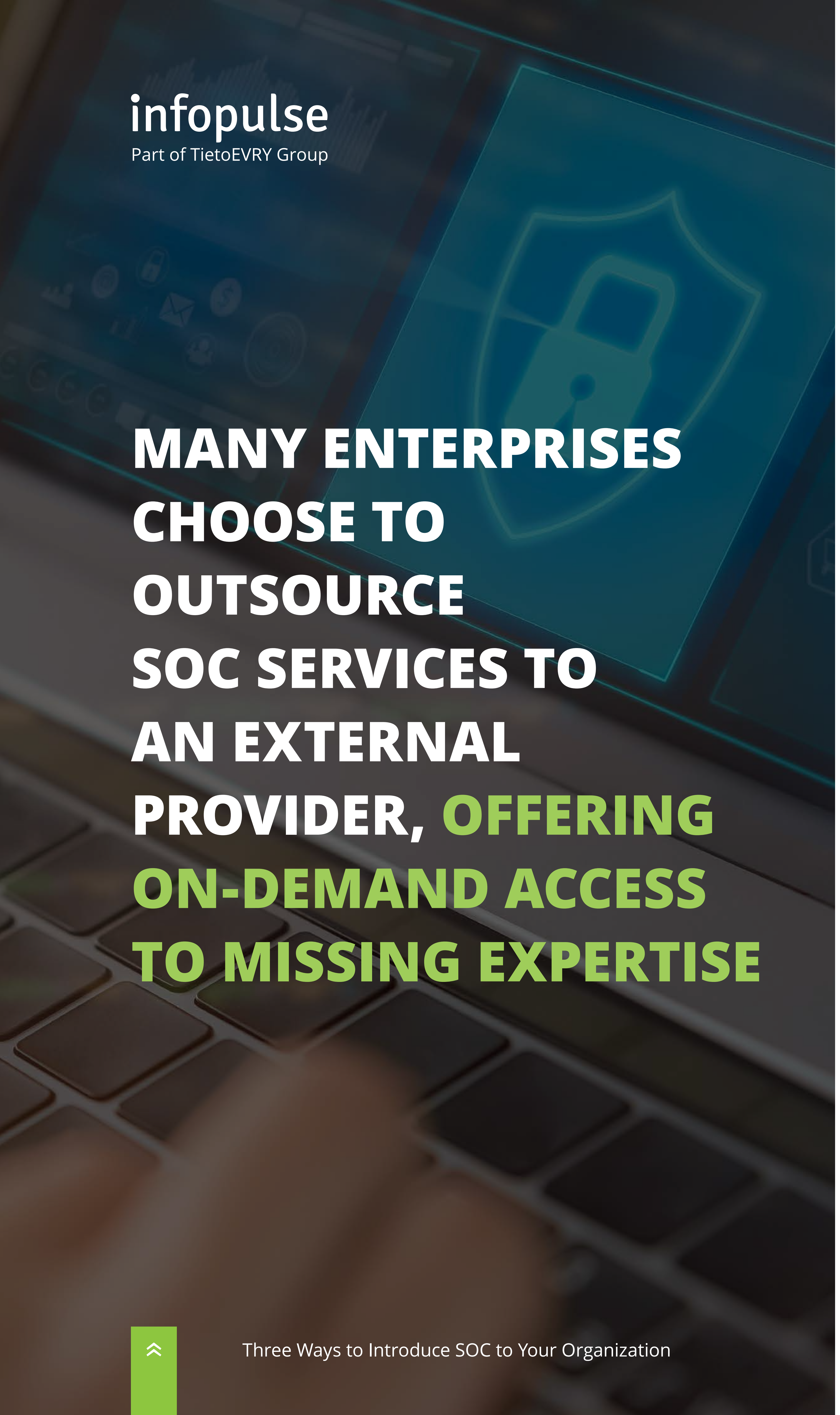
Fewer than needed cybersecurity experts are available for hire in the US[9]

$3.5 million

Cybersecurity jobs are projected to remain unfilled by the end of 2021[10]

51% OF EXECUTIVES PLAN TO ADD MORE FULL-TIME CYBERSECURITY PERSONNEL TO THEIR TEAMS

[6] Gov.UK: Cyber security skills in the UK labour market 2020
[7] ESG & ISSA Research Report: The Life and Times of Cybersecurity Professionals 2020
[8] Gov.UK: Cyber security skills in the UK labour market 2020
[9] Security Magazine: New research shows US cybersecurity talent shortage
[10] PwC: Global Digital Trust Insights Survey 2021



MANY ENTERPRISES CHOOSE TO OUTSOURCE SOC SERVICES TO AN EXTERNAL PROVIDER, OFFERING ON-DEMAND ACCESS TO MISSING EXPERTISE

Due to constricted access to talent, many enterprises choose to outsource SOC services to an external provider, offering on-demand access to missing expertise and a cost-effective way to provide 24/7 L2/L3 support.

A qualified security service provider can assist with securing cloud infrastructure, SIEM/SOAR deployment, and execution of the specified number of use cases, in-line with the SLAs.

SOC services delegation makes sense when you already have baseline security policies and practices, but lack the people to ensure timely support, 24/7 monitoring and proactive threat detection. Oftentimes, cloud migrations act as a prerequisite for SOC establishment. With an expanded defense surface, in-house teams may not have the capacity and expertise to tackle cloud security alongside on-premises infrastructure.

BUSINESS CASE

A retail business expanded its cross-border operations and launched a new e-commerce website, hosted in the cloud. The company already has sufficient L1 support staff to cover the basic events and respond to customer queries 8x7. An in-house security team is responsible for maintaining on-premises datacenter and ensuring IT security among business users.

However, the business lacks people and expertise to ensure optimal cloud security round-the-clock. After cross-border expansion, their operations have also become more vulnerable to external threats (hacking) and they wish to establish a more proactive security response plan. They also rely on a custom-built payment processor, which needs to be additionally secured.

HOW SOC CAN HELP

In such a scenario, the service provider can outsource L2 and L3 support services to an external provider to **achieve better security coverage**. Furthermore, a SOC provider can help the retail business **secure their custom payment** system, **establish protection** against most essential attack vectors, and **monitor against the common threats** using the installed SIEM/SOAR solutions.

Most Commonly Delegated SOC Use Cases

- L2/L3 24x7 On-call support
- Threat response automation
- NIDS deployment
- Vulnerability scanning
- SIEM/SOAR deployment
- Threat detection and intelligence
- 24x7 security monitoring
- Network traffic monitoring

- Threat response and containment
- Anomaly detection
  (user access and authentication, exploit, network baselines)
- Unauthorized access monitoring
  (users, devices, networks)
- Log management

Benefits

- Comprehensive cost-effective security coverage
- Access to missing expertise and skill sets
- Reduced security risks and threat exposure due to professional management
- SLA-backed SOC team performance
- Ability to progressively implement new security facets and best practices
- Scalability — expand your technical footprint without worrying about maintenance

Challenges

- **Right-sizing the scope of the services.** SOC is a complex unit. Not every industry or business type needs to maintain a team of highly qualified security analysts on a 24x7 call. Before selecting a service provider, consider whether your organization really needs SOC or perhaps, can do equally well with a lower-level cybersecurity solution. For example, most cloud operations can be effectively secured with native SaaS tools, such as Azure Sentinel, Azure Traffic Monitoring, and Azure Security Center, if you are using Microsoft Azure.
- **Service provider selection.** Different service providers assume a different degree of responsibility when it comes to SOC services delegation. As you compare value propositions, pay attention to the scope, boundaries, and SLAs every contender proposes. The best way to reduce the risks of selecting a sub-optimal arrangement is by seeking out a mature service provider, offering a scoped, itemized, deliverables-based service model.

SOC AS A SERVICE

SOC as a service is a new paradigm of SOC services delegation, offering a “wholesome” approach to SOC adoption — from baseline security setup to ongoing maintenance and continuous improvements.

At Infopulse, we structure managed SOC services into tiered service packages, varying in terms of:

- Number of supported users and locations
- Logs in package included
- L1/L2/L3 support availability
- Response automation
- Customer SOC use cases development and support
- Detalization and types of reporting

SOC as a service is an excellent solution for both mature and entry-level companies, seeking structural and technological improvements to their security. In each case, we begin an engagement with a comprehensive IT security assessment, aimed at determining the optimal level of security coverage your company needs and the missing security facets due for implementation.

With a SOC as a Service adoption model, you receive a customized services package, security architecture, and toolkit configuration, plus an on-call team to fully cover all your security needs and meet the set SLAs.

SOC as a service is an excellent solution for both mature and entry-level companies, seeking structural and technological improvements to their security

During **the onboarding stage (varying between two and twenty weeks)** you will work closely with our consultants who will:

- Report on the current state of security, identified vulnerabilities and shortcomings
- Suggest the optimal security architecture, licenses, and strategies for cost optimization
- Implement and customize the necessary security toolkit and establish supporting processes
- Implement support for custom use cases — service arrangements, covering specific business needs, company equipment (e.g., IoT systems), or in-house developed business systems
- Take over all the established SOC responsibilities, based on the package tier
- Conduct training workshops for in-house staff
- Regularly report on new findings and suggestions on further areas for improvement

At Infopulse, Managed SOC combines ad hoc security consultancy and adoption guidance — offered as a stand-alone solution by other providers — and SOC services delegation with a higher level of predictability, efficacy, and expertise.

With managed SOC, you do not need to seek out individual experts to augment your security operations or compete with other employers for in-demand security talent. Similarly, you also optimize SOC operating costs by eliminating employee training, upskilling, and retention costs.

75%

SOC specialists report burnout from increased workloads[11]

60%

Find a career in cybersecurity to be taxing in terms of work/life balance[12]

65%

Cybersecurity specialists think their employer doesn't provide sufficient training[13]

[11] Devo:2020 Devo SOC Performance Report
[12] ESG & ISSA Research Report: The Life and Times of Cybersecurity Professionals 2020
[13] Ibid.

Apart from ensuring sufficient staffing, we also help you select, configure, deploy, and customize security tools that suit your business needs. Security technology has made significant progress over the past five years, especially in terms of analytics, automation, and predictive capabilities. However, investment in state-of-the-art tools does not automatically translate into measurable improvements in a corporate security posture.

82%

Cybersecurity leaders are spending 20+% of their IT budgets on advanced technology investments

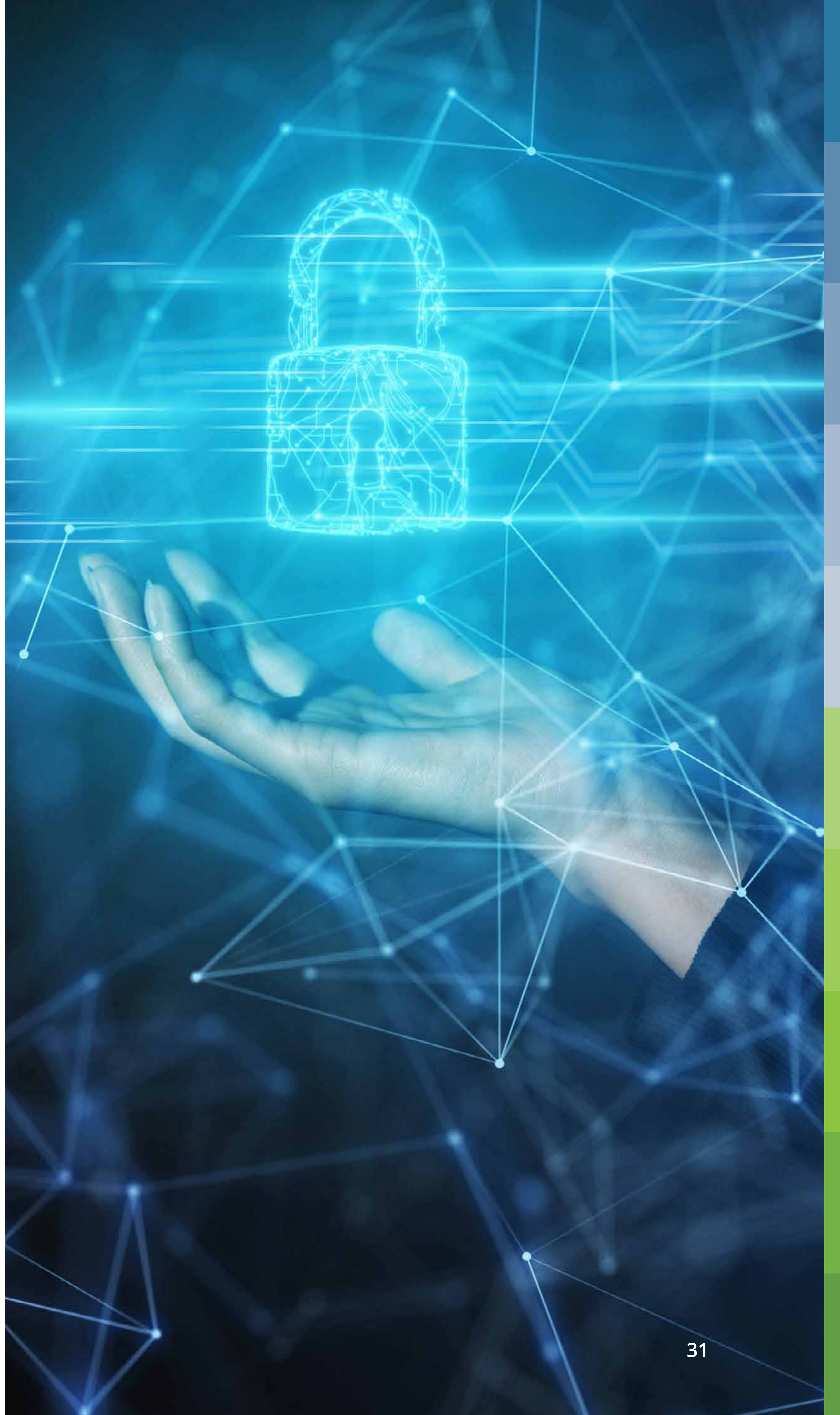
58% vs **24%**

Companies with mature cybersecurity programs have a higher percentage of contained breaches that have no impact on operations

69%

Of companies struggle to stay ahead of attackers and the cost of doing so is unsustainable[14]

[14] Accenture: State of Cybersecurity Report 2020



Based on the assessment data, we help your company align new technology investments with current and future security needs. This way you receive the best coverage and capabilities, fine-tuned to your infrastructure, without overspending.

We help select, deploy, and configure:

- SIEM tools (including subscription to commercial-level threat intelligence)
- SOAR
- Ticketing systems
- Event management systems
- Security incidents response platform
- Automated threat detection and response tools
- Advanced security analytics (including predictive solutions)

Nearly every industry significantly vaulted ahead in terms of digitization over the past year. The cyber threat landscape, too, became more hazardous and elaborate. With SOC as a service, you can develop a staunch security perimeter, furnished with the best-in-class commercial tools and set a dedicated “watchdog” to guard it without establishing a dedicated security department in-house.

Benefits

- Suited for companies at any level of security maturity
- Security levels and protection, customized to your industry
- Lower TCO of SOC with predictable monthly costs
- Access to in-demand cybersecurity talent and domain expertise
- Customizable levels of support and security coverage
- High service levels, pegged to metrics and SLAs
- Technology investment consultancy and assistance with meeting compliance requirements
- Support of custom SOC use cases for out-of-the-box security scenarios
- Continuous security improvements and advisory

Challenges

- **IT infrastructure visibility required.** Prior to setting up a SOC, it is essential to conduct an infrastructure audit to achieve an end-to-end view of its components. Security experts underline the importance of providing them with a comprehensive assets inventory and data classification to enable efficient SOC performance.
- **Establishing effective communication.** Having delegated SOC to a chosen security provider, one should provide a single point of contact in their organization to enable effective cooperation. Appointing such a role, the company can significantly reduce time and resources required to process certain operations and, thus, increase the overall performance of the SOC team.

AGRICULTURAL GIANT

CASE STUDY

Leveraging the Capabilities of Cybersecurity Automation with Azure Sentinel

AGRICULTURAL GIANT

Infopulse helped our client, a European leader in agriculture, enhance their cybersecurity system by reconfiguring the current Azure Sentinel setup with maximum efficiency and introducing automation. After assessing the existing IT perimeter, our experts developed the solution's high-level architecture and solution implementation strategy. Azure Sentinel capabilities were validated by four SIEM/SOAR test cases:

1

DETECTING POTENTIAL THREATS WHILE USING MICROSOFT TEAMS.

Configured a set of analytical rules and data parsing via Logic Apps and Office 365 Management Activity API.

2

IDENTIFYING CORPORATE DATA LEAKAGE VIA EMAILS.

Set up an automated rule to detect users forwarding multiple emails to the same external SMTP address.

3

REJECTING POTENTIALLY HARMFUL FILES WHEN UPLOADED TO CORPORATE CLOUD STORAGE.

Tested incident alerts on uploading potentially harmful executable files to common folders in SharePoint and OneDrive.

4

IDENTIFYING POTENTIAL COMPROMISED ACCOUNTS.

Identifying cases with successful sign-ins from IPs that tried to exploit blocked or disabled user accounts.

BUSINESS VALUE

Test scenarios demonstrated the advantages and capabilities of Azure Sentinel as a cloud-native (SaaS) security automation system and enabled our customer with:

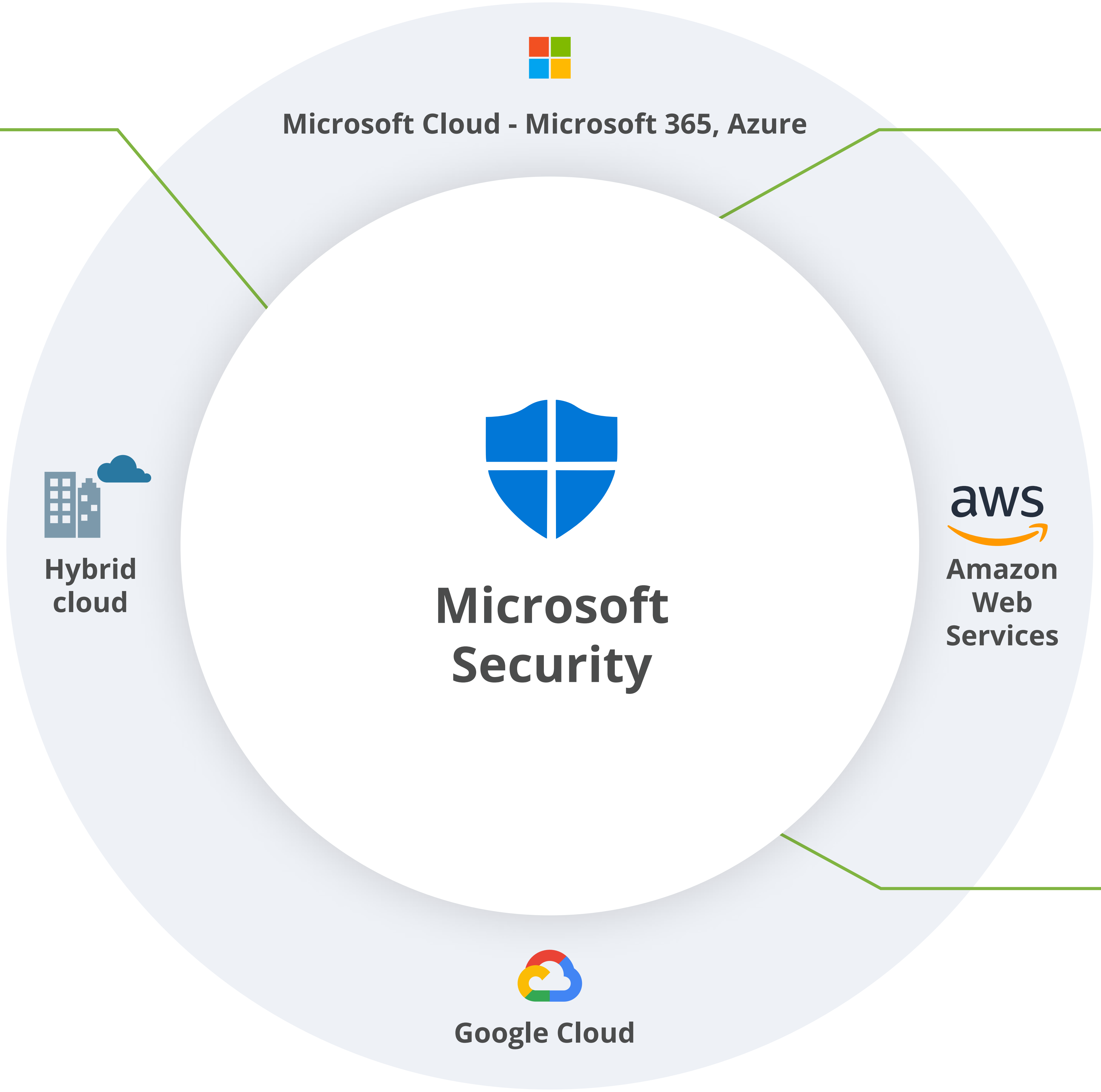
- Automated cybersecurity rules for the selected test cases that allow minimizing the human factor.
- Successful integration of Azure Sentinel with Exchange, SharePoint, Teams, and Microsoft Threat Protection.
- Automated report generation via Azure Sentinel and Power BI.
- The roadmap for the further implementation of Azure Sentinel with extended integration into the company's IT infrastructure.
- Estimated license cost reduction for Azure Sentinel as a single SIEM & SOAR system.

Contact our security team to learn how Azure Sentinel can tackle your security challenges

Powering Your SOC with Microsoft Security Tools

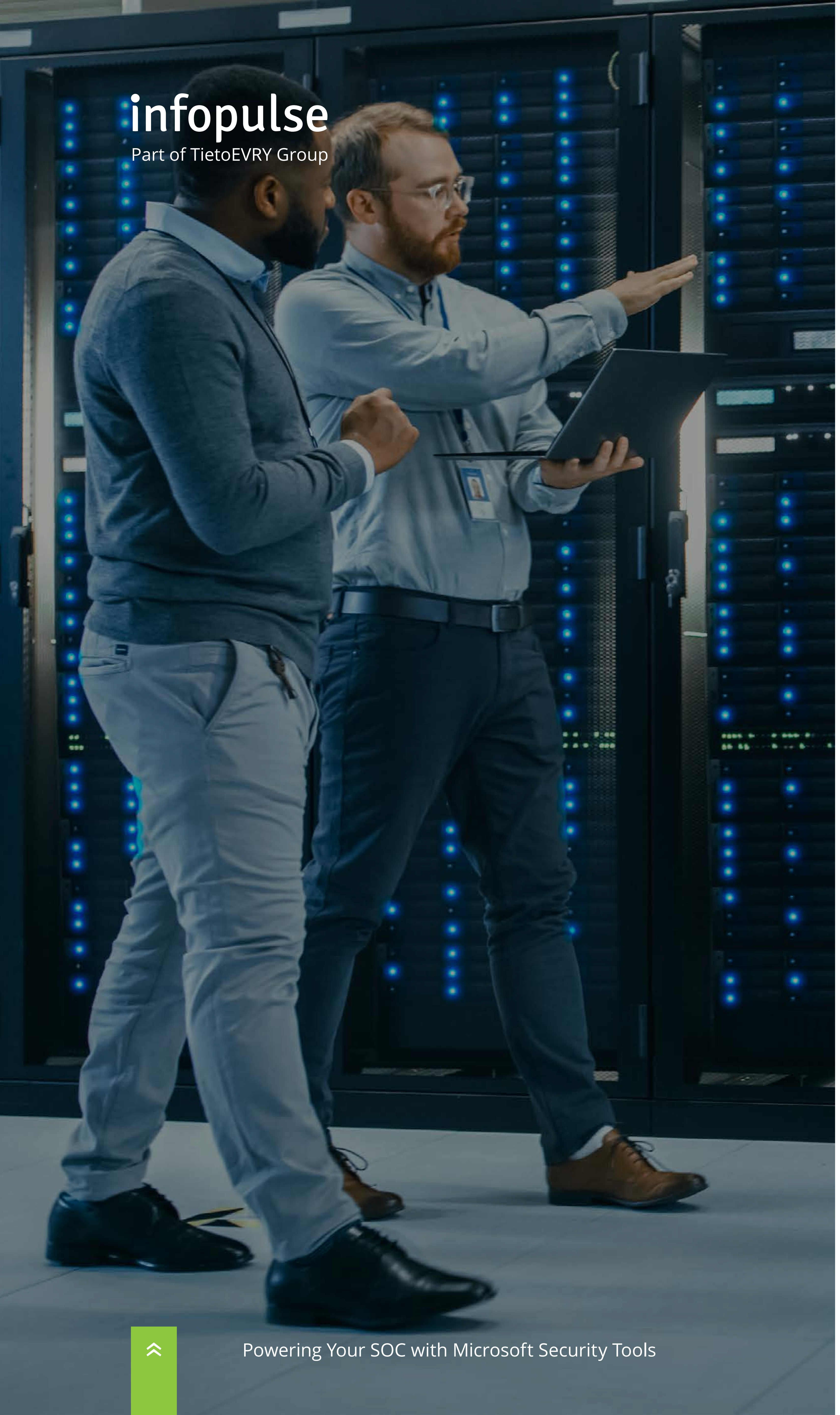
INTEGRATE UP TO 40 CATEGORIES

Endpoint detection and response
Endpoint protection platform
Forensic tools
Intrusion prevention system
Threat vulnerability management
Anti-phishing
User and entity behavior analytics
Threat intelligence feeds
App and browser isolation
Attachment sandboxing
Application control
End-user training
Network firewall (URL detonation)
Host firewall
Secure email gateway
Security assessment
SIEM
SOAR
Cloud access security broker
Cloud workload protection platform
Cloud security posture management
Incident response services
DDOS protection
IoT protection



Data discovery
Data classification
Data loss prevention
Insider risk management
Database security
Information and messaging encryption
Device encryption
Encrypted cloud storage
Secrets management

Identity governance
Active directory
Mobile application management
Mobile device management



Microsoft offers a comprehensive range of native security solutions, capable of covering all Microsoft assets, as well as third-party infrastructure (including multi-cloud and hybrid environments). Comprehensive, versatile, automation-driven, the ecosystem of Microsoft Security solutions amplifies SOC analysts' abilities to detect, triangulate, investigate, and act upon a broad array of security events.

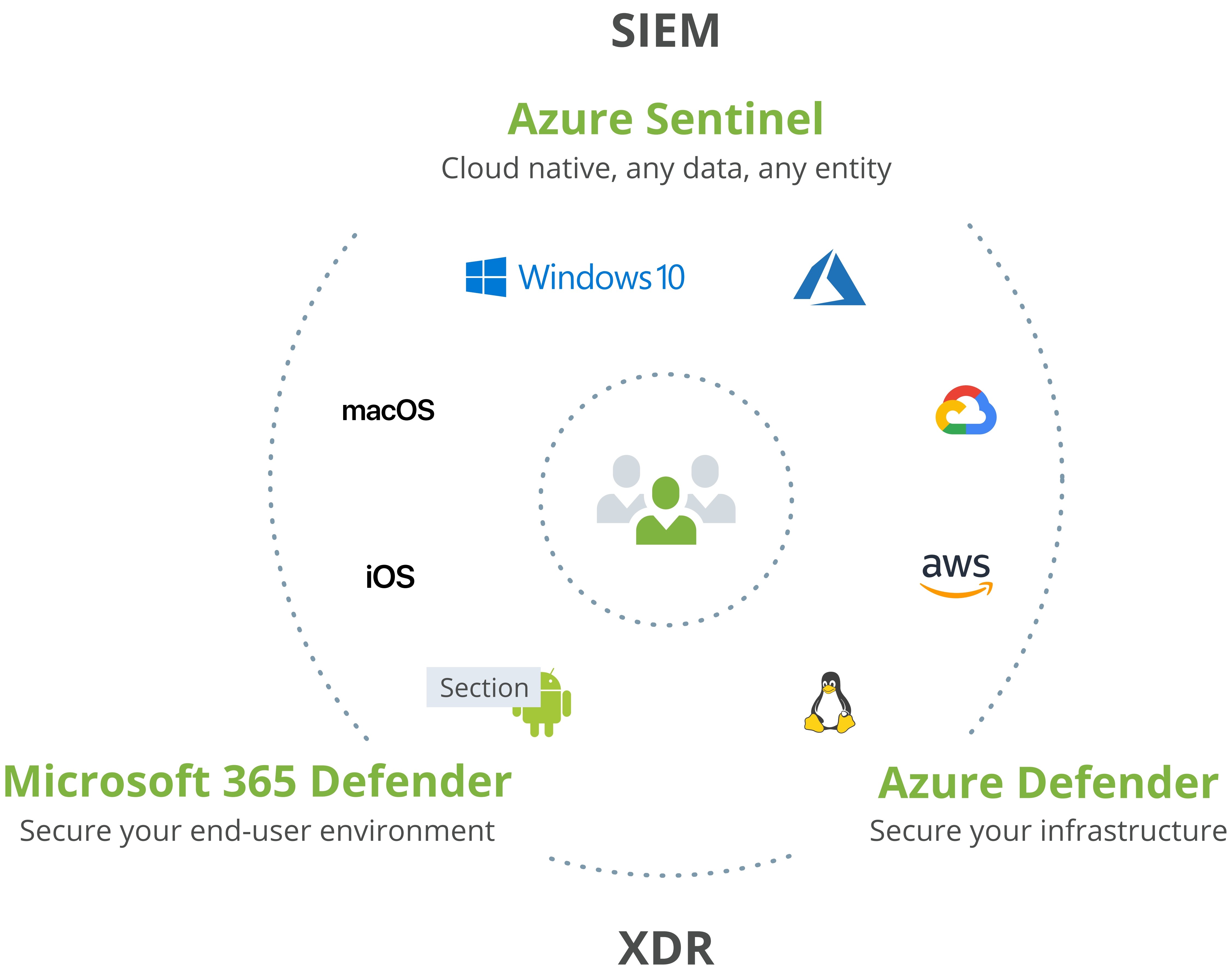
KEY BENEFITS

- End-to-end protection
- Integrated compliance
- Automated event management
- Efficient investigation workflows
- AI-driven threat analysis
- Built-in connectors for non-Microsoft solutions

SECURITY TASKS COVERED

- Identity and access management
- Automated SIEM and SOAR
- Extended detection and response (XDR) solutions
- Zero Trust model implementation
- Cloud security and workload protection

Microsoft SOC Solutions for SOAR, SIEM, and XDR


SIEM
Azure Sentinel
Cloud native, any data, any entity
Windows 10
macOS
iOS
aws
Section
Microsoft 365 Defender
Secure your end-user environment
Azure Defender
Secure your infrastructure
XDR

Azure Sentinel

Cloud-native SIEM + SOAR solution, scalable across the entire technical estate. Aggregates log data from Microsoft products, as well as third-party solutions, connected via APIs.

Microsoft Azure Sentinel facilitates security data collection across the organization. It can be connected with non-Microsoft services such as threat intelligence providers, DNS machines, DLP solutions, or other cloud services, via APIs or agents to aggregate real-time log data for analysis. Equipped with state-of-the-art machine learning capabilities, Sentinel runs a continuous analysis of incoming data and notifies SOC teams about legitimate threats. Built-in user analytics automatically notifies your teams about any deviations and provides timely insights for threat detection and prevention. As Sentinel is built on Azure cloud, it's more scalable and cost-effective than legacy SIEM and SOAR systems.

BENEFITS FOR SOC TEAMS:

Up to **79%**

Reduction in the number of false positives thanks to Azure Sentinel's AI-driven correlation engine and behavior-based analytics

Up to **80%**

Reduction in labor efforts, associated with advanced investigations

Over **$2.2M**

Estimated efficiency gains[15]

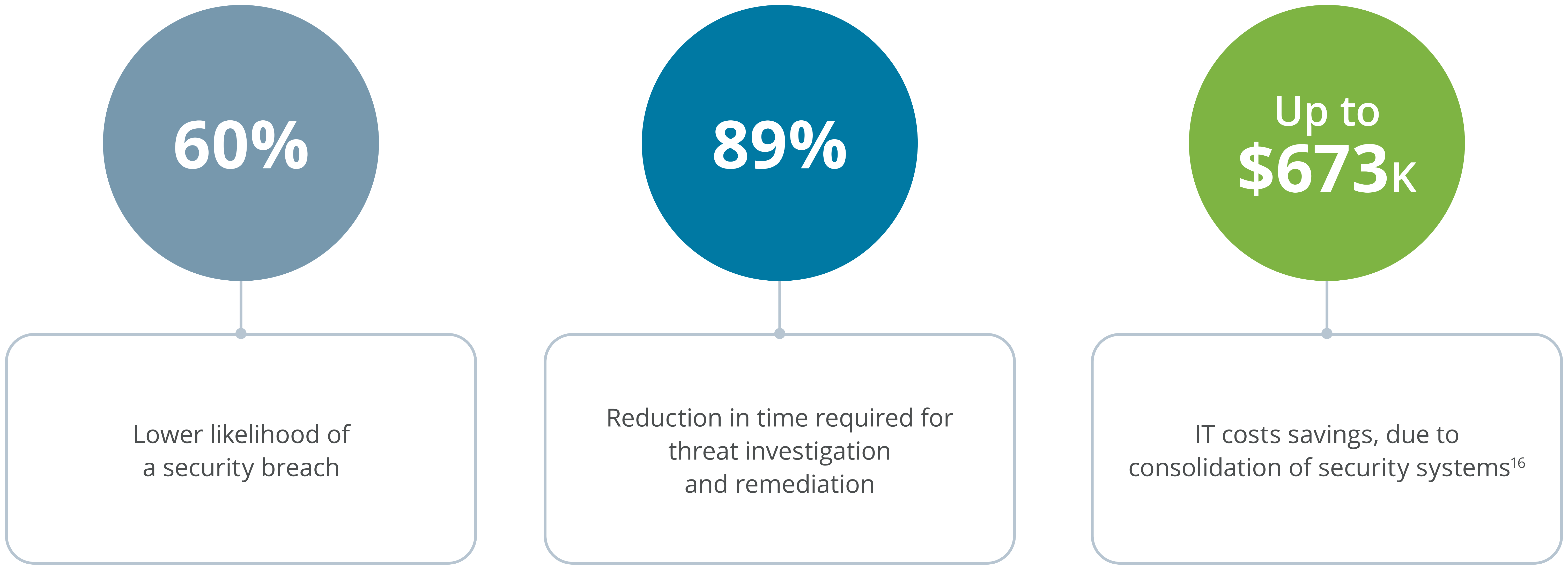
[15] The Total Economic Impact™ of Microsoft Azure Sentinel by Forrester Consulting, 2020

Microsoft 365 Defender

Fully integrated detection and response (XDR) solution for Microsoft 365 and compatible platforms (Android, iOS, Linux, MacOS, Windows).

Microsoft 365 Defender provides a robust suite of automation capabilities for threat detection, investigation, remediation, and prevention for connected products. The tool operates across five perimeters — identity protection, endpoint security, application security, email, and document security. All functionality is accessible from a single dashboard and augmented by convenient analytics dashboards. Effectively, this transforms siloed alerts, into contextualized incidents, featuring insights on how the breach occurred and progressed across the environment. SOC teams can leverage Microsoft 365 Defender to proactively investigate threats and implement better security control across the board. Additionally, users can configure custom AI-powered security workflows for auto-healing affected assets.

BENEFITS FOR SOC TEAMS:



60%

Lower likelihood of a security breach

89%

Reduction in time required for threat investigation and remediation

Up to $673K

IT costs savings, due to consolidation of security systems[16]

[16] The Total Economic Impact™ Of Microsoft Office 365 Threat Intelligence by Forrester Consulting, 2018

Azure Defender

Cloud-native XDR solution for Windows and Linux servers, containers, and serverless workloads on Azure and in hybrid environments.

Azure Defender is cloud XDR solution, covering the entire corporate ecosystem of connected cloud assets and workloads, as well as IoT and edge devices. The solution also features automated threat detection capabilities, powered by Microsoft intelligent security graph, preventive protection tools, and post-breach remediation. Azure Defender helps locate emerging threats and vulnerabilities within applications, running on your virtual machines (including containers), as well as within on-premises and multi-cloud databases. Built-in behaviorial analytics and advanced monitoring capabilities also assist with threat hunring and post-breach event analysis. Learn how the attack progressed across your ecosystem and implement better controls to stafe off critical threats.

BENEFITS FOR SOC TEAMS:

50%

Reduction in mean time to threat remedication

86%

Reduction in threats, requiring rededicaion efforts

86%

Reduction rate in the number of false positives[17]

[17] The Total Economic Impact™ Of Microsoft Azure Security Center by Forrester Consulting, 2021

How to Build a Business Case for SOC Adoption: Checklist

□ **ASSESS THE CURRENT CYBERSECURITY MATURITY LEVELS: USE THE FRAMEWORK PROVIDED IN THIS BOOK.**

- □ **Ensure that your organization already has the following processes in place:**
  - □ Critical IT infrastructure protection
  - □ Baseline event monitoring and logging
  - □ Reactive cybersecurity response plan
  - □ Threat detection, prevention, and monitoring capabilities

□ **CREATE A LIST OF REQUIREMENTS FOR SOC OPERATIONS:**

- □ **Security threat monitoring:**
  - □ Do you have standard security workflows?
  - □ Which tools (cloud-based and/or on-premises) do you use?
  - □ Does your organization require 24/7 security monitoring?
  - □ What are your current blind sposts in terms of monitoring?
- □ **Security incident management:**
  - □ Which regulatory, compliance, or business requirements have to be met?
  - □ Are there any customer SLA targets? If none, which ones should be set?
  - □ Which metrics do you use to monitor the security team’s performance?
- □ **SOC staffing:**
  - □ Which security roles are you looking to fill in?
  - □ Does every role come with a clear description of responsibilities?
  - □ Do you have a sample staffing schedule?
  - □ Does your in-house team need extra security training?
- □ **Process development and optimization**
  - □ Do you have documented operational processes and SOPs?
  - □ Which processes require improvement/automation?
  - □ Does your company require new operational playbooks?
- □ **Emerging threat strategy**
  - □ How well can your organization respond to novel threats?
  - □ How will you ensure that your cybersecurity practices are up to date?
  - □ Are you considering new technology investments to improve your approaches to proactive security?

Conclusions

The cybersecurity landscape has shifted dramatically over the past years. Yet, many organizations have only recently come to the need for proactive security that extends beyond the basic alert systems and rapid security team mobilization in case of an incident. SOC enables proactive security, but its efficacy falls short without proper reactive measures in place (cybersecurity). However, tackling both issues at once is operationally taxing for most businesses to handle on their own. That’s why alternative SOC adoption scenarios have come to the fore.

By opting for a hybrid SOC model — where some of your security operations are delegated to a managed service provider, advanced SIEM solutions and Endpoint Detection and Response (EDR) systems — businesses at different stages of maturity (and with different security budgets) can gain the security coverage they need to operate in a safe and compliant manner.

Take advantage of the cutting-edge approach to enterprise security, facilitated by Infopulse experts having a broad experience in the domain.

Infopulse Managed Security Operation Center: Services Included

CLOUD-BASED MANAGED SIEM

- Straightforward SIEM deployment and integration
- Extended integrated SOAR capabilities
- Limitless scalability
- 200+ built-in analytical rules
- Commercial threat intelligence sources
- Machine learning models and data visualization

HETEROGENEOUS LOG SOURCES

- Cloud-based, hybrid, or on-premises log sources supported
- Native Microsoft logs support
- Non-billable Azure activities, Office 365, and Microsoft 365 security solutions logs
- 100+ predefined data connectors
- Networks, services, servers, business systems logs collection, aggregation, and correlation

RESPONSE AUTOMATION

- Automated incident response on common events
- Programmable Azure Logic Apps customization
- Integration with a vast number of devices, infrastructure components, or business systems

SERVICE CUSTOMIZATION

- Service modification via custom connectors development and log support
- Bespoke use case development
- Customizable reporting
- Various means of communication

EXPERIENCED SOC L1/L2/L3 TEAM

- Up to 24x7 availability
- SLA-based service
- Extended security domains competence profiles
- Event monitoring, incident investigation, reporting, and handling guidance

COST IMPROVEMENTS AND OPTIMIZATION

- Assessment of the existing infrastructure as part of the on-boarding process
- Optimizing costs by collecting the required data only
- Providing technology and solution suggestions for service consumption optimization

ABOUT INFOPULSE

Infopulse, part of the leading Nordic digital services company TietoEVRY, is an international vendor of services in the areas of Software R&D, Application Management, Cloud & IT Operations, and Cybersecurity to SMEs and Fortune 100 companies across the globe. Founded in 1991, the company has a team of over 2,000 professionals and is represented in 7 countries across Europe and North and Latin America. Infopulse is a Global Outsourcing 100® company recognized by IAOP®.

CONTACT US

☎

UA: +380 (44) 585-25-00
US: +1 (888) 339-75-56
FR: +33 (172) 77-04-80
BG: +359 (876) 92-30-90

DE: +49 (3222) 109-52-35
UK: +44 (8455) 280-080
PL: +48 (663) 248-737
BR: +55 (21) 99298-3389

✉ info@infopulse.com

FOLLOW US

www.infopulse.com