GlobalDots

6 Capabilities of a Complete SOC Solution

Contents

EXECUTIVE SUMMARY

Bad actors succeed when organizations are not prepared or if they treat their cybersecurity with an “it won’t happen to me” mentality. These two are exactly what hackers look for when either trying to extort a business or when targeting one for any other purpose. In today’s ever-growing RaaS (ransomware as a business) frenzy coupled with organizational and personal data exfiltration to gain a competitive advantage, no business can continue its day to day without securing and protecting its assets and IP.

Integrating a complete and powerful SOC solution into your business will help alleviate the risks and workload involved in monitoring and protecting your network. When evaluating SOC options, whether in-house or outsourced, it is important to understand that a SOC’s capabilities will determine the success of your cybersecurity protection.

The 6 Critical Capabilities That Every SOC Should Include

This e-book will detail the six capabilities that contribute to a complete SOC solution: strategic monitoring, incident response, digital forensic investigation, threat intelligence, threat hunting, and SIEM optimization.

A chain is only as strong as its weakest link, and the same can be said about cybersecurity methodologies; all six SOC capabilities are critical for ensuring powerful cyber resilience. Not only should a SOC provide these capabilities, but they should also complement each other, strengthening the chain instead of individual pieces.

Strategic monitoring coupled with SIEM optimization reduces wasteful hours of analyzing false positives and alert fatigue, sharpening security operations and maintaining relevancy in a fast-paced environment.

Managed detection and response services like forensic investigation and incident response lead the way in providing a full, clear picture of any security event that demands attention and remediation.

Threat intelligence and automated threat hunting are critical today as passive cyber security no longer provides quality protection; proactive detection is needed to find threats before they happen. When these capabilities work together, your SOC will make cybercrime seem like cyber criminals are just not good at what they do.

Read about the six capabilities that make up a comprehensive SOC solution to learn how to optimize your cyber defense and make sure you are protected from every potential attack approach.

GlobalDots

Strategic Monitoring

Strategic Monitoring

Strategic monitoring in cybersecurity is the act of collecting data and information, like logs, from all the sources in your organization, such as systems, networks, and processes, and then analyzing it to identify the signs of a compromise. It's achieved through a combination of technology and cyber professionals who know how to provide protection for numerous attack vector types

.

Naturally, it makes more sense to focus on your company's security strategies rather than remediation, considering the amount of time that remediation can consume. Continuous 24/7 cybersecurity monitoring by a SOC can drastically enhance your security alerts.

Strategic monitoring can detect signs of compromise in real-time, resulting in early identification of potential breaches. The "strategic" element comes into play by creating correlations between the countless events, providing you with a more focused view of the alerts that could cause actual harm to your business.

- These signs of compromise can include:
- Abnormal user-account access such as failed login attempts
- Changes to file configuration such as deletion, alteration, or replacement of critical files
- Misuse of privileged account
- Unauthorized port access
- Abnormal changes during the updates of scheduled patches

Keeping up with Compliance

Your SOC should be able to help you meet regulatory requirements that require continuous monitoring (such as **PCI-DSS 10.5.5,11.5**) of your cybersecurity controls and networks. Non-compliant organizations have to face legal penalties and reputational damage.

What are the Challenges to Strategic Monitoring?

Cybersecurity monitoring has become a daunting task due to ever-growing and changing cyber threats and attacks, such as increased network traffic, malware volume and sophistication, ransomware, Trojan horse, bots, worms, and a lot more. These sophisticated attacks are able to circumvent your traditional cybersecurity controls. To deal with these recurring cyber threats, integrating a strategic monitoring process and technology into your SOC is crucial. Moreover, the massive use of SaaS, PaaS, and IaaS also creates a big challenge for network organizations.

Why is Strategic Monitoring in SOC so Critical?

In the digital world, there can be infinite cyber threats targeting your organization. For example, your employees may use Bring-Your-Own-Devices (BYOD) and/or Internet of Things (IoT) that can introduce severe threats to any corporate network, further leading to a data breach. Even outsourcing can invite unwanted cyber-attacks. Mishandling of big data or disparate logs can also cause an intrusion.

Strategic monitoring plays a pivotal role in the SOC's ability to keep you safe. Your SOC's strategic monitoring abilities should include:

- Real-time detection of cyber threats
- Instructions on how to deal with each specific threat
- Meets compliance standards to avoid legal issues
- Provides proactive security such as threat hunting
- Allows integration with security operations and network
- Help you know your adversaries with threat intelligence

Network Security Monitoring for Businesses

Network security monitoring is also a big challenge for businesses. It involves network blind spots, communication issues between network operations teams and cybersecurity, and problems with data that is not collected on time. Your strategic monitoring tool should provide you with real-time network monitoring capabilities whereby network intrusions will be monitored in a timely manner.

Your network security monitoring incorporates various technologies that help to detect and respond to irregular network behaviors. To this end, your cybersecurity monitoring tool will utilize valuable data, including endpoint forensic data, firewall logs, and log data from servers and endpoints. It also encompasses network telemetry data and full-packet capture. Various other sources are listed below:

- VPN logs
- Active directory logs
- DHCP logs
- DNS query logs
- Log files and data that is provided by antimalware sandboxes
- Proxy logs
- IPS/IDS alerts

Strategic Monitoring for SMBs

In most cases, small businesses do not have the knowledge and the right tools to deal with a sudden cyber-attack. Your SOC's strategic monitoring capability should help you monitor your system effectively to ensure that your business is protected against various cyber threats.

Successful Strategic Monitoring

Successful strategic monitoring determines the status of systems, processes, and activities to meet specified information needs, in addition to the network data and information that have been collected through the course of the monitoring (discussed in the previous section). Below is the list of these systems, processes, and activities:

- System monitoring
- Configuration management
- Vulnerability management
- Incident management
- Business continuity management
- Third-party risk management
- Environment and physical security management
- Implementation of Information Security Management System (ISMS) processes
- Cybersecurity awareness and training
- Audits
- Risk treatment process
- Risk management process

OUR RECOMMENDATION

A SOC's ability to monitor a network is what enables businesses to thwart notorious data breaches by detecting threats at the early stages. It is imperative that your SOC should provide contextual visibility within and across all the systems to accurately discover the earliest signs of suspicious activity in real-time to ultimately avoid having to deal with additional security issues.

GlobalDots

Incident Response

Incident Response

Incident response is an irreplaceable piece of your SOC. An ideal incident response team will analyze of all all the pieces of information that entered your system in the case of an incident. They will then either respond accordingly or give professional recommendations on how to respond to the specific incident you are dealing with at the given moment, depending ifon whether your SOC is in-house or outsourced.

What is Incident Response in Cybersecurity?

Incident response is the set of policies and procedures that are utilized to address and manage the aftermath of a cyber-attack or data breach, also known as a security, computer, or IT incident. With a SOC incident response plan, companies can limit damage, reduce costs and recovery time so that the business can get back up and running.

Knowing Potential Attack Vectors

An attack vector is a path or method whereby threat actors infiltrate corporate systems and networks. Hackers use attack vectors to exploit system vulnerabilities and human errors. Your concrete SOC incident response plan will better defend against these attack vectors. The following sections provide an insight into potential attack vectors that incident response embedded in a SOC will effectively counter.

Theft or Loss of Computing Devices

This threat vector incorporates a theft or loss of equipment used by the company, such as a smartphone or laptop. This may lead to malware and phishing attacks. A reliable cyber incident response plan for phishing attacks can prevent financial and reputational loss.

Email Attack

In an email attack, cyber attackers send a suspicious email to employees and management. The email contains a misleading message and/or malicious attachment that can inject malware into corporate systems and networks. Email attacks can also be a subset of phishing attacks.

The phishing attack incident response plan requires Computer Security Incident Response Team (CSIRT) to immediately separate valuable reports from the noise that turn user-reported emails into actionable intelligence.

Web Attack

A web attack is executed from a web-based application or website. Having a flexible SOC that can integrate with any standard-based proxy appliance or web gateway can offer high-performance web security

Distributed Denial of Service Attack

Since DDoS attacks prevent continuous delivery of critical services by opening the floodgates of unwanted traffic, a DDoS incident response strategy is vital to ensure business continuity and reliable, consistent services.

Advanced Persistent Threats (APT)

An advanced persistent threat describes an attack campaign in which an intruder creates an illicit, long-term presence on a network in order to mine sensitive data.

Incident Response Methodology

Many incident response vendors offer incident response and security operations. An effective incident response methodology, also known as incident response lifecycle, involves multiple stages and each step is carried out in a sequence.

Preparation

Preparation comes into play to develop an incident response mechanism within the enterprise and to install a minimum security-baseline in the corporate network and IT infrastructure. The security product and services are reviewed prior to installation. Social engineering activities are performed on systems, networks, and applications running on them. This should be a part of the incident response strategy.

Detection

With proper profiling and understanding of your systems, you give your organization a better chance of identifying problems.

When activity seems amiss, your SOC should detect any security incidents. Your SIEM or other security tools should issue an alert to relevant security personnel.

Containment, Eradication, and Recovery

Incident containment involves the decision-making process whereby appropriate resources are utilized to contain the incident.

Once contained, the eradication phase comes into place to eliminate the cause of the incident. Eradication efforts may involve deleting the malicious code snippet or software, disabling firewall ports, closing certain accounts, and so forth.

Lastly, recovery is one of the most important goals of this methodology as it allows a business to be up and running again. Recovery actions incorporate system restore, backup, and system hardening to prevent future security incidents.

Containment, eradication, and recovery should be an essential ingredient of any incident response framework. In addition, timing is everything. The faster that an organization is able to move through the incident response plan steps, the faster the organization will successfully be back in business.

OUR RECOMMENDATION

Create and regularly practice an incident response plan within your organization. You can maintain business continuity while making changes to your network's configurations based on threats, by enabling business leaders to monitor their IT environment in real-time for computer incidents and help them to prepare, detect, contain, eradicate, and recover from intrusions and cyber-attacks with as minimum time as possible.

GlobalDots

Forensic Investigation

Digital Forensic Investigation

Forensic investigations is an important component for any business that takes its cyber defense seriously. Your SOC is responsible for preforming forensic investigation during and after an attack to help understand what happened, where it happened, to what systems and machines, and any digital footprint left by intruders.

Phases of Digital Forensics

These phases illustrate a complete path that digital forensic investigators must finish by using their cyber digital forensic tools. Here are the phases of a digital forensic investigation:

Gathering Evidence

An effective digital forensics tool and team can collect data from multiple devices, computers, laptops, mobile devices, USB drives, servers, hard drives, digital cameras, and so forth. The data can be evidence and, thus, it must not be damaged or modified during acquisition. Your SOC's forensic investigation capability should enable data collection from numerous sources accurately without damaging original evidence.

Tracking and Investigating Email Crimes

Since emails are a widely used way of electronic communication, scammers employ various techniques, such as phishing, to compromise both private and corporate emails.

Proper digital forensics helps you investigate email crimes by tracking, analyzing, and investigating cyber trails and digital evidence through fast and accurate analysis to detect and prevent various email crimes such as:

Email Hijacking

Phishing Attacks

Email Spoofing

Email Spamming

Mail Bombing or
Mail Storm Identity

Fraud/Chain Letters

Performing Malware Forensics

No organization can be free of cybersecurity threats and attacks unless it is thoroughly protected against the menace of malicious code or scripts, known as malware. Digital forensic investigations are incomplete without investigating malware.

A forensic solution should aid in detecting malicious scripts or code manipulation and how the malware behaves on the infected system. It should discover indicators of compromise (IoC) and help locate malicious artifacts throughout the network. Doing so can help you and your team analyze the scope, severity, and repercussions of the security incident and sometimes even identify the perpetrators.

Conducting Data Exfiltration Forensics

Any digital forensic tool is incomplete if it cannot investigate the illegal transmission of critical data and information from your corporate network to clandestine hackers. Your team must be equipped with an appropriate digital forensic tool to detect and investigate data exfiltration. Conducting a full-scale investigation when necessary is critical for a SOC to be able to provide the network its securing.

GlobalDots

Threat Intelligence

Cyber Threat Intelligence

What is Threat Intelligence in Cybersecurity?

Threat intelligence, also known as Cyber Threat Intelligence (CTI), is data from a rich array of sources. The data is put through an analytical and logical process to evaluate it in context so that it can easily be used and understood by cyber threat intelligence analysts. The data may include indicators, mechanisms, implications, and action-oriented advice concerning existing and emerging cybersecurity threats and attacks.

The Importance of Threat Intelligence

Threat intelligence assists enterprises in making faster, more informed, and sound IT security decisions. These decisions allow stakeholders to change their behavior from a reactive to a proactive approach. Cyber threat intelligence can:

- Prevent cyber threats and attacks
- Provide direction on preventive and remedial measures
- Share tactics with the IT community to create collective knowledge

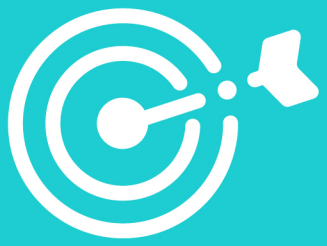
3 Types of Threat Intelligence

The following sections delve into the subcategories of cyber threat intelligence.

01

Strategic

Strategic threat intelligence is all about a company's threat landscape. The executive management prepares business strategy based on report findings. It involves threats and vulnerabilities to your organization and prevention measures to thwart future loss.



02

Tactical

Tactical threat intelligence provides an on-the-ground view that describes granular, atomic indicators related to known attacks. This technique involves machine-to-machine detection of threats. Using this feature, you identify artifacts in your corporate network.

03

Operational

With operational threat intelligence, you will be aware of the context for security events and incidents. Moreover, for the threat intelligence analyst or incident responder, operational threat intelligence allows them to expose potential risks, pursue previously undiscovered suspicious activities, and perform faster investigations.

How Does a Threat Intelligence Program Work?

There are six phases of creating and maintaining a threat intelligence program as part of a SOC.

1 Direction

- In this phase, you will set goals for your company's threat intelligence program. To this end, you need to understand:
- The business processes and digital assets that need to be protected.
- The potential impact of loss in the event of a security incident on those assets and if the business processes are interrupted.
- Prioritize the assets and business processes that need to be protected first.

2 Collection

The collection phase is used to meet the critical requirements of a threat intelligence program. Your efficient threat intelligence platform helps you to collect:

- Logs and metadata from security devices and internal network
- Threat Intelligence Feeds (TIF)
- Data from forums and websites
- Data from the dark web
- Data from open-source blogs and news

3 Processing

Plenty of raw data is gathered during the collection phase in a threat intelligence tool. The processing phase also assists in processing all raw data. An effective threat intelligence platform involves various other supporting tools to enhance features, especially Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) tools. The SIEM involves security alerts, data aggregation, advanced analytics, forensics efforts, dashboard, and threat intelligence feeds. The SOAR helps in automating manual, repetitive, and mundane tasks.

4 Analysis

The analysis phase helps in human-based decision-making. The processed information is analyzed and interpreted to provide sound judgments, such as looking for further investigation or implementing remedial measures.

5 Dissemination

In this phase, the output of the finished threat intelligence is disseminated to all stakeholders.

6 Feedback

One must understand the requirements and priorities of security operations teams for whom the threat intelligence is being performed. To this end, their regular feedback is critical to ensure an understanding of the requirements of each team. If the requirements or priorities change, make adjustments accordingly.

Strengthen Your Incident Response Quality Threat Intelligence

Effective threat intelligence can significantly minimize pressure on incident responders or Computer Security Incident Response Team (CSIRT). Having reliable threat intelligence software can:

- Automatically identify and eliminate false positives or pesky alerts,
- Enrich security alerts with real-time context,
- Gather and compare information from external and internal data sources to discover threat,

Cyber Threat Intelligence in a Security Operations Center (SOC)

Security teams in Security Operation Centers (SOC) are pressured due to too many false positive alerts and the long time required to triage these alerts. Due to the alert fatigue, threat analysts have to do additional work, and that time can be spent on other essential tasks.

The good news is that cyber threat intelligence platforms are offering reliable tools to provide an antidote to these problems. Using such a platform, users can:

- Correlate and enrich alerts
- Improve a response time
- Accelerate triage and simplify incident analysis and containment

Integration of Threat Intelligence Within a SOC

Your SOC should allow integration with threat intelligence whereby it can integrate other threat intelligence tools and feeds to itself.

GlobalDots

Threat Hunting

Threat Hunting

You can assume that persistent and focused adversaries are already present in your corporate systems and networks. Rather than waiting and allowing them to do harm, be proactive and detect them with a SOC's threat hunting capability to prevent data breaches that may lead to financial, reputational, and compliance issues.

Cyber threat hunting is a proactive and iterative search through endpoints, networks, and datasets to detect suspicious, malicious, and risky activities that have evaded detection by existing cybersecurity controls.

Avoid Challenges with Proactive Threat Hunting

Traditional cybersecurity controls such as antivirus programs and firewalls are based on reactive approaches that respond to security incidents that have occurred to your organization. Insider threats and Advanced Persist Threats (APT) are challenging to deal with in this way.

A cyber threat hunting solution should be an integral part of your SOC that enables your team to constantly look for cyber threats and prevent them from penetrating corporate networks before they become risks to your business. Threat hunting acts before the security incidents, unlike the reactive approaches that execute after the IT incident.

The Significance of Effective Threat Hunting

With an efficient threat hunting program, you should be able to place a dedicated, appropriate focus on the efforts to purposely identify and curb cyber adversaries that may already be larking in your IT environment.

SOCs threat hunters don't wait to respond to Indicators of Compromise (IoC) or security alerts. Instead, they actively search for cyber threats to prevent them from happening.

Automated Threat Hunting

Your SOCs threat hunting should automatically absorbs all IoCs from network devices or/and systems. All collected IoCs cannot be malicious. The SOC then investigates and extracts actual IoCs from the rest. If malicious IoCs are detected, they will be marked on the blacklist for future reference.

Determine Your Threat Hunting Success Metrics

It is vital to know whether your threat hunting tool is effectively hunting cybersecurity threats. To this end, you need to know some metrics. Below is the list of these metrics that help you understand your threat hunting success:

- Number of infected hosts by severity
- Number of security incidents by severity
- Logging gaps that have been discovered and corrected
- Number of detection gaps that have filled
- Identified vulnerabilities
- False-positive rates of transitioned hunts
- Number of hunts that have transitioned to new analytics
- Insecure practices that have been discovered and corrected

Threat Hunting Steps

To fully understand the significance of threat hunting, you'll need to know the steps involved in the actual process.

01

Step 1: Create Hypothesis

The hypothesis is a logical path of detection or an educated guess based on the ideas of what potential threats may be lurking in your IT environment and how you could identify them. The hypothesis also incorporates the Tactics, Techniques, and Procedures (TTP) that adversaries utilize to penetrate your network.

02

Step 2: Using Tools to Investigate Hypothesis

Your team may use various tools and techniques to investigate the developed hypothesis. Instead of buying multiple tools, your SOC should have a single platform that can help investigate your hypothesis effectively. Your SOC's threat hunting capabilities should allow you to proactively search for cyber threats that are lurking undetected across all types of networks.

03

Step 4: Automated Analytics

Threat hunters must not waste their time doing the same threat hunting campaign again and again. Once the threat has been identified and the problem addressed, automation must be created to save valuable time and resources the next time there is a similar event.

04

Step 3: Identification of TTPs And Patterns

In this step, you should search for and uncover adversaries' TTP and new malicious patterns of behavior.

How Should Your SOC Utilize Threat Hunting?

Your SOC shouldn't allow cyber-attacks to complete their lifecycle and pose damage to the organization's IT assets. It should quickly take in threat information during the kill chain. After that, analysis begins, and once the data is processed, your SOC should send you instructions that clearly explain how to handle the threat quickly.

THREAT HUNTING RECOMMENDATIONS

Threat hunting should include identifying and correlating patterns by including numerous data sources to fully uncover adversary activities. As time passes, businesses can grow their hunting maturity capabilities. It is important to understand that threat hunting enables businesses to stay a step ahead when it comes to bad actors. As you identify and block cyber-attacks, hackers will continue to find new ways to infiltrate and cause damage. Being proactive can keep you focused on what matters and maintain business productivity.

GlobalDots

SIEM Optimization

SIEM Optimization

When it comes to ensuring the confidentiality, integrity, and availability of an organization's critical data and information such as personally identifiable information (PII), banking data, company secrets, and more, your SOC is the main line of defense. For this reason, optimization of your SIEM is an essential part of remaining ahead of any oncoming or new threats.

Optimize SIEM Technology To Avoid Redundancy

SIEM (security information and event management) is a technology that aggregates and analyzes data from various sources across your IT infrastructure.

SIEM technology is a critical part of any robust cybersecurity operation, but to remain relevant, it requires proper implementation and continuous maintenance to maximize effectiveness. At the same time, most SMBs have limited cybersecurity budgets and don't have enough in-house security professionals. Nevertheless, implementing a SOC equipped with a regularly maintained SIEM can save you countless hours and maintain business focus.

SIEM Optimization and Tuning

The SIEM has two primary functions that are relevant for your SOC: reporting and forensic information about security incidents, and generating alerts based on correlations and algorithms that were written to detect various set rules, which would indicate a security event.

SIEM tuning is the process of filtering all the data that is being received to identify cybersecurity risks, system failures or anomalies, compliance, and more. This should be done as part of the initial setup process for your SIEM. Tuning a SIEM to your organization is very specific, because each organization's needs, activities, behaviors, and assets are different. In this way you will get the best value from your SIEM. It's very important not to overlook asset categorization and network hierarchy configurations, which are commonly forgotten. Essentially what you're doing by configuring your SIEM is setting up a process to avoid rules that constantly trigger false positives.

With a SIEM as part of your SOC, it's crucial that it is properly tuned to your specific business's needs, otherwise the SIEM will not detect security incidents that can put your business at risk. Additionally, tuning is not a one-time process done during initial set-up. To maximize your investment, and best protect your business and assets, your SIEM should be regularly optimized and tuned to stay up to date with the latest IOCs, TTPs, and threat intelligence.

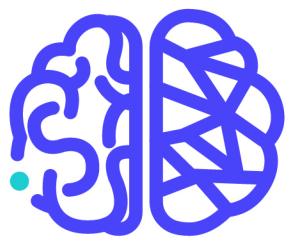
Avoiding Redundancy

Companies, both large and small, invest a lot of time and resources to detect, collect, normalize, log, load, and index big data for multiple security purposes; this process tends to create redundancy.

A good SOC backed by AI can help you avoid redundancy by providing you with easy-to-understand data concerning potential threats. An AI should be able to gather the data needed to ensure your success with threat hunting and early threat detection. The information provided by the AI can save you time because you don't have to analyze large amounts of data to address the potential threat.

Optimization with Artificial Intelligence (AI)

By using AI capability, your SOC can manage billions of datasets from both structured and unstructured sources. In addition, it can find connections between cybersecurity threats such as malicious IP addresses and other suspicious files, which will automatically cause a red flag alert.



AI should be able to generate behavioral analysis to accurately detect threats. Signature-based techniques are less effective against rapidly growing cybersecurity threats, especially boot-record and ransomware attacks. AI effectively identifies risky behavior that might lead to phishing attacks or lure your corporate employees into downloading a malicious attachment.

Harden Your Cybersecurity Posture with Cyber Professionals

When it comes to maintaining and optimizing your SIEM, it's important to have cybersecurity experts on hand. If you lack the expertise in-house that is required to constantly maintain and optimize your SIEM, it's recommended to seek outside help to manage it. After a few months without maintenance, the SIEM technology can already start to be outdated, since it hasn't been updated with new rules and correlations based on the ever-changing cyber threats.

CONCLUSION

The cybersecurity arena is only growing more complex overtime and as technologies advance. Global regulatory standards set a bar for organizations in order to help protect businesses from underperforming and mistreating their cyber posture. Implementing the right SOC that will maintain proper protection and response against cyberattacks, especially before they occur, is critical. That is why understanding how a SOC works and what capabilities it should have can drastically help you in selecting the right one for your business.

Each of these six capabilities are essential in protecting your organization from threats, each complimenting the other to detect, track, analyze, and develop proactive tactics. Gaining powerful threat intelligence from a wide variety of sources provides a deep understanding of threat behaviors and TTPs, fueling SIEM optimization and creating new rules for potential threat mitigation. Strategic monitoring enables rapid incident response while holding all the information necessary to quickly contain, eradicate and recover from oncoming threats. Ultimately, a proactive approach to cyber security is the way to gain the upper hand with an added layer of protection. Threat hunting tracks down evasive threats and hunts down suspicious activity which are then turned into new rules to optimize your SIEM technology.

When the capabilities are combined into a single centralized location, like CYREBRO's cloud-based interactive SOC Platform, cybersecurity becomes simplified and manageable. CYREBRO's SOC Platform combines all these capabilities, providing organizations with a complete SOC solution, without the need to build a SOC SIEM solution in-house. It provides a single platform that gives your business the power of enterprise-grade cyber security without the necessary investment.

As the threat landscape grows, becoming more sophisticated and complex, using a simple combination of antivirus and firewall as your defense is not nearly enough. A capable, managed SOC to watch over and monitor your business, while knowing how to quickly react and respond, can save you unnecessary financial and reputable damages.

About GlobalDots

GlobalDots is a 20-year global leader in cloud innovation, connecting over 1,000 global businesses with the latest cloud and web technologies, such as Security, Web Performance, DevOps & Cloud Management, Corporate IT, and advanced AI/ML models. Led by a team of seasoned engineers and architects, GlobalDots offers easy end-to-end innovation adoption, from consulting to ongoing professional services, proactively introducing newer and better solutions to support businesses in maintaining a scalable, up-to-date technology posture in a quickly-changing world. With our implementation expertise and high-end professional services, we empower clients to streamline business processes and scale globally at ease.

BOSCH · SentinelOne · Payoneer · Playtika · Lufthansa · WIX · nuvei · AppsFlyer · monday.com · FIAT · SimilarWeb

Web Performance

Web Security

Cloud Security

DevOps & Cloud Management

Hosting, networking & hardware

GlobalDots
Cloud Innovation Hunters

Contact Us

Follow Us