



Mastering the Art of SOC Analysis

12 Top Tips and Skills for Aspiring Security Operations Center Analysts





Table of Contents

Introduction	3
Learn Network Architecture	4
Learn Network Analysis	5
Learn Log Analysis	6
Learn Endpoint Analysis	8
Know Your Cloud	9
Know Your Active Directory	10
Detect & Hunt for Threats	12
Operate With A Tool-Agnostic Mentality	13
Practice Effective Communication	14
Develop Effective Questioning Skills	15
Reinforce Your Knowledge	16
Join The Cybersecurity Community	16
Conclusion	17
Tomorrow's Threats Require a New Enterprise Security Paradigm	18



A person wearing a blue shirt and a lanyard is shown from the side, typing on a laptop. The laptop screen displays a dashboard with various charts and data. The background is a blurred server room with rows of server racks and blue lighting.

Introduction

As cybersecurity threats increase in sophistication and frequency, the demand for skilled Security Operations Center (SOC) analysts continues to rise. In tandem with defensive strategies and advanced security software, SOC analysts fill a critical role in keeping enterprises safe from attacks. They are responsible for identifying and mitigating oncoming threats, protecting sensitive information, and ensuring the overall security of an organization's digital assets.

Demand for skilled SOC analysts is climbing, so aspiring defenders need to ensure they have the technical knowledge, analytical skills, and critical thinking abilities required for the job. This eBook covers the top twelve tips and skills that aspiring analysts will need to master as they begin their journey toward success in the SOC analysis field.

Learn Network Architecture

Understanding the fundamental networking concepts is essential for SOC analysts. Start with the Open Systems Interconnection (OSI) model and the TCP/IP protocols basics.

Networking is the backbone of any IT infrastructure. For an aspiring SOC analyst, learning networking basics means understanding how data flows across the network; a skill critical in identifying and responding to security incidents.

By building a foundational understanding of networking concepts such as IP addressing, subnets, domain name system (DNS), routing, and protocols like TCP/IP, ICMP, and UDP, a SOC analyst can identify anomalies, track down malicious activity, and create effective security policies.

Since most attackers are initiated from the network, having a good grasp of network security fundamentals, including [firewalls](#), intrusion detection and prevention systems (IDPS), and [network segmentation](#) provide SOC analysts with an edge in responding to security incidents. Understanding network fundamentals typically includes the below areas of interest:

- ✓ **Learn networking fundamentals** - Learn about network topologies, addressing, protocols, and networking devices. Resources such as the [CompTIA Network+](#) or [Cisco CCNA certifications](#) can provide a solid foundation in fundamental networking concepts.
- ✓ **Learn network security principles** - Focus on firewalls, intrusion detection and prevention systems (IDPS), and virtual private networks (VPNs).
- ✓ **Practice with hands-on labs** - Use virtual labs or physical equipment to gain hands-on experience in configuring and troubleshooting networks. Examples include:
 - [GNS3](#) - This free, open-source network simulation software allows users to design, configure, and test virtual networks.
 - [Packet Tracer](#) - This network simulation software developed by Cisco allows users to design, configure, and test network topologies.
 - [EVE-NG](#) - This network emulation software allows users to design, configure, and test virtual networks and complex network configurations.
 - [TryHackMe](#) - This platform provides guided, pre-configured labs accessible through a browser. The variety of high-quality courses and their low entry barrier allow learners to gain exposure to different tools and concepts.
- ✓ **Join networking and security communities** - Connect with professionals in the networking and security industry to learn from their experience, ask questions, and gain insights into the latest trends and technologies. Online communities such as Reddit's [/r/networking](#) or [/r/netsec](#), or professional associations such as ISACA, ISSA, or (ISC)², can be a great resource for connecting with others in the field.
- ✓ **Stay up to date with industry news** - Follow security and networking news sites such as [Dark Reading](#), [BleepingComputer](#), or [SecurityWeek](#) to stay informed on the latest security threats and trends.

Learn Network Analysis

Analyzing network traffic can help identify suspicious activities and potential threats. Learn to use network analysis tools like Wireshark, Network Miner, and Snort.

Network traffic analysis involves examining the packets of data transmitted between devices on a network to identify patterns, anomalies, and signs of malicious activity. SOC analysts can detect suspicious behaviors such as unauthorized access attempts, data exfiltration, malware infections, and command-and-control communication by analyzing network traffic.

They can also use network traffic analysis to trace the origin of an attack, determine the scope of compromise, and identify affected assets. Network traffic analysis skills are key for any aspiring SOC analyst looking to build proficiency in threat detection and incident response. To get started on learning how to analyze network traffic, consider the below steps:

- ✓ **Build up networking basics** - Before analyzing network traffic, it is essential to have a solid understanding of networking concepts such as TCP/IP, DNS, HTTP, and SSL. Learning to interpret a packet's structure and each header field's role can help identify and troubleshoot network issues.
- ✓ **Use network analysis tools** - Various network analysis tools can help analyze network traffic, such as [Wireshark](#), [tcpdump](#), and [tshark](#). These tools can be used to capture, decode, and analyze packets in real time or from saved capture files. Using Wireshark, for example, analysts can filter traffic by IP address, protocol, port, or keyword and analyze packet contents such as payload, headers, and timestamps.
- ✓ **Practice analyzing network traffic** - The best way to improve network traffic analysis skills is by practicing on real-world network traffic data. Sample capture files are obtainable from online resources such as the [Wireshark Sample Captures](#) page or by capturing traffic on a test network. Use the traffic to simulate an attack and create detection rules using a NIDS-like [snort](#).
- ✓ **Learn from online resources** - Various online resources provide tutorials, blogs, and videos on network traffic analysis, such as the Wireshark University, PacketTotal, and the SANS Institute. These resources can help budding analysts learn advanced techniques like protocol analysis, network forensics, and malware analysis.

Learn Log Analysis

SOC analysts deal with a large volume of logs from different sources. Understanding how to parse, search, and analyze logs is crucial. The aspiring analyst must be comfortable using log management tools such as Splunk, ELK, and Graylog.

To be effective in their role, SOC analysts need to show proficiency in log analysis. Logs are a critical information source containing a wealth of data about system and network activity, user behavior, and security events. By analyzing logs, SOC analysts can identify suspicious activity, track the [spread of malware](#), and detect potential security incidents.

Log analysis also plays a crucial role in [incident response](#). When a security incident occurs, SOC analysts must investigate it, determine its scope and impact, and identify the root cause. Data captured in logs can help SOC analysts reconstruct the incident timeline, identify the attacker's entry point, and determine the extent of the compromise.



Analyzing logs will also be required for any in-depth [forensic investigations](#). The analysis involves examining logs generated by various systems and applications to detect anomalies, suspicious activities, and signs of compromise. Experienced analysts can detect events such as failed login attempts, unusual network traffic, and system changes that may indicate a security incident. Below are some methods aspiring analysts can take to improve their log analysis skills:

- ✔ **Become familiar with log management tools** - Log management tools like Splunk, ELK, and Graylog can help analysts to parse, search, and analyze logs. These tools can collect logs from different sources, apply filters and transformations, and visualize log data. Use these tools to view the organization's security posture comprehensively.
- ✔ **Learn common log formats** - Logs come in a variety of formats. Learning common log formats like Syslog, Apache, and Windows Event Logs will serve to develop a stronger understanding of log data and how to make sense of it.
- ✔ **Study log analysis, parsing, and search techniques** - SOC analysts must have a wide arsenal of knowledge on log analysis techniques such as anomaly detection, correlation analysis, and threat hunting. Also, practice parsing and searching logs with different log [management tools](#) and techniques.
- ✔ **Use regular expressions (Regex)** - Regular expressions ([regex](#)) are a powerful tool for parsing and searching log data, allowing analysts to extract specific information from logs quickly.
- ✔ **Filter noise** - Logs may contain a lot of noise, such as debug messages, informational messages, or system messages. Filtering out noise helps analysts focus on the essential log data only.
- ✔ **Use visualization tools** - Visualization tools like graphs, charts, and dashboards are useful when trying to understand log data quickly. Utilize any visualization features within log management tools to create graphs or dashboards that show trends or anomalies in log data.
- ✔ **Stay updated on threat news** - Cybersecurity threats and attack techniques constantly evolve. Stay in the know with the latest cybersecurity news and trends. Follow [industry blogs](#), attend webinars, and participate in online communities to stay informed.

Learn Endpoint Analysis

Endpoints are a prime target for attackers, and SOC analysts need to understand how to secure them. Learn how to use endpoint security tools like Wazuh, OSSEC, and SentinelOne.

In today's digital landscape, [cybercriminals](#) are continually devising new ways to exploit vulnerabilities and launch attacks. Enforcing a traditional perimeter-based security model is no longer enough. Since security operations centers (SOCs) are at the forefront of identifying and mitigating these threats, SOC analysts need to be familiar with a variety of tools and techniques to protect their organization's network and sensitive data. Among these, one of the most critical tools that SOC analysts need to master is [endpoint security](#) tools.

[Endpoint security tools](#) protect against cyberattacks, focusing on securing endpoints like laptops, desktops, mobile devices, and servers. The endpoint is where an attack usually occurs, and it's also the entry point for malware and other cyber threats. Endpoint security tools help to identify, isolate, and remediate the threat before it can cause significant damage.

Endpoint security tools in the hands of a knowledgeable SOC analyst can do the following:

- ✓ **Protect vulnerable endpoints** - Attacks on endpoints can result in data breaches, system disruption, and other security incidents. Endpoint security tools help to protect against these attacks by providing real-time visibility and control over devices.
- ✓ **Perform advanced threat detection** - Endpoint security tools use [advanced threat detection](#) mechanisms like behavioral analysis, machine learning, and artificial intelligence to detect and respond to threats. These tools can identify and isolate suspicious activities, providing SOC analysts with the information they need to respond to incidents quickly.
- ✓ **Increase visibility** - Endpoint security tools provide SOC analysts with a complete view of endpoint devices, including their applications and processes. This visibility allows analysts to identify vulnerabilities and misconfigurations that cybercriminals could exploit.
- ✓ **Save time** - Endpoint security tools can [automate and orchestrate response actions](#), reducing the time it takes to detect and respond to incidents. This automation helps SOC analysts to focus on high-priority incidents, improving the overall efficiency and effectiveness of the SOC.

There are several endpoint security tools that SOC analysts need to master to protect their organization's network and sensitive data. The most important of these are:

- ✓ **Endpoint Detection and Response (EDR)** - **EDR solutions** provide real-time visibility into endpoint devices, enabling SOC analysts to quickly detect and respond to incidents. EDR solutions use advanced threat detection mechanisms like behavioral analysis and machine learning to identify and isolate suspicious activities.
- ✓ **Antivirus & Anti-Malware** - These can help to protect against known threats. These tools use **signature-based detection** to identify and block known malware and viruses.
- ✓ **Vulnerability Scanners** - These tools scan endpoint devices for **vulnerabilities** and provide SOC analysts with a list of vulnerabilities that need to be addressed.
- ✓ **Patch Management Tools** - These are vital to keeping endpoint devices up to date with the latest security patches and updates. These tools protect endpoint devices against known or so-called “N-day” vulnerabilities.

05

Know Your Cloud

Understanding how cloud computing works and its security risks are becoming increasingly important. Learn cloud concepts and best practices for Incident Response.

Businesses of all sizes rely heavily on technology to operate efficiently. Effective SOC analysts strive for a deep understanding of the latest technologies and tools used in cybersecurity. One area that is becoming increasingly important is cloud computing.

Cloud computing refers to the delivery of computing services over the internet. Instead of hosting software applications and data on local servers or personal devices, users can access these resources remotely over the internet. Cloud computing services can include infrastructure as a service (**IaaS**), platform as a service (**PaaS**), and software as a service (**SaaS**). Essential cloud concepts for SOC analysts include cloud service models, deployment models, security controls, compliance frameworks, and incident response.

There are many benefits to using cloud computing, such as cost savings, scalability, and flexibility. However, **potential risks** also need to be considered, such as data security and compliance. As a SOC analyst, it is important to understand cloud computing basics to monitor and respond to security incidents effectively.

Cloud computing has fundamentally changed how IT infrastructure is designed, implemented, and secured. With the adoption of cloud services, traditional security measures such as firewalls and intrusion detection systems are no longer sufficient to protect against **modern cyber threats**. SOC analysts must now be able to monitor and analyze data from cloud environments and traditional on-premises systems.

One challenge in cloud computing is the [shared responsibility model](#). Cloud providers are responsible for the security of the underlying infrastructure, while the customer is responsible for securing their own data and applications. This means that SOC analysts should understand the cloud provider's and the customer's [security controls](#) to detect and respond to security incidents effectively.

06

Know Your Active Directory

Active Directory (AD) is the backbone of most organizations' identity and access management systems. A good SOC analyst will thoroughly understand AD concepts like domains, users, groups, and permissions.

[Active Directory \(AD\)](#) is a centralized database that stores information about users, groups, computers, and other resources. It's the backbone of most organizations' identity and access management systems and is critical in securing access to sensitive data. Active Directory naturally presents an [attractive target](#) for attackers.

To effectively monitor and secure AD, SOC analysts must understand its key concepts, including domains, users, groups, and permissions. Domains are logical groupings of computers and other resources managed as a single unit. Users are individual accounts that are granted access to resources within the domain. Groups are collections of users or computers that are assigned common permissions, and permissions define what actions users can perform on specific resources.

SOC analysts must be able to effectively monitor and manage AD to identify and respond to security incidents. They should thoroughly understand [AD security best practices](#), such as implementing strong password policies, restricting administrative access, and regularly auditing AD activity.

They should also be familiar with [AD security tools](#), such as Microsoft's Active Directory Users and Computers (ADUC) console, which allows them to manage users, groups, and other AD objects. Another tool, Active Directory Domain Services (ADDS), is used to manage domain controllers and replication. SOC analysts use AD to perform the following functions:

- ✓ **Centralized Identity and Access Management** - Active Directory is Microsoft's centralized identity and access management tool, which enables system administrators to manage user accounts and access resources across an entire organization. This is critical for SOC analysts because they must quickly identify who has access to what resources to investigate security incidents properly.
- ✓ **Log Analysis** - AD logs can provide valuable insights into the behavior of users and systems within an organization. SOC analysts need to be able to analyze these logs to detect anomalies and identify potential security threats.
- ✓ **Group Policy** - Active Directory Group Policy allows system administrators to enforce security policies across an organization's IT infrastructure. This is crucial for SOC analysts because they must quickly identify any security policy violations that could lead to a [security incident](#).
- ✓ **Attack Surface Reduction** - Active Directory includes tools such as Group Policy and security baselines that can be used to reduce an organization's attack surface. SOC analysts must deeply understand these tools to analyze and mitigate security incidents effectively.

Active Directory Tools and Concepts to Master for SOC Analysis

- ✓ **Domain Controller** - The [domain controller](#) is the heart of AD and is responsible for authenticating users, storing user account information, and enforcing security policies. SOC analysts must understand how domain controllers work to investigate security incidents properly.
- ✓ **LDAP** - Lightweight Directory Access Protocol (LDAP) is used to access and manage directory services. SOC analysts need to be able to use LDAP to query AD and obtain valuable information for security analysis.
- ✓ **PowerShell** - [PowerShell](#) is a powerful command-line tool that can be used to manage AD. SOC analysts need to deeply understand PowerShell to automate tasks and perform advanced security analysis.
- ✓ **Security Baselines** - AD security baselines are recommended security settings that can be applied to an organization's IT infrastructure. SOC analysts must thoroughly understand these security baselines to configure and monitor an organization's security posture properly.

Detect & Hunt for Threats

Writing filters that are used to hunt or detect threats is a foundational part of most analysts' skills set.

Threats float in and out of visibility and may not leave a network, log or endpoint footprint. Additionally, there is a chance you're not collecting or monitoring one of the mentioned data sources. **Brute force attack** detections need to be made for each source; if it's targeting your SSO, it may not have a network or host footprint. The same can be said for other attacks.

Within SOCs, this creates an exponential amount of detections to be made. SOCs can often suffer from **alert fatigue**, trying to detect suspicious activity across multiple applications. This creates the need for high quality detections in order to detect and identify malicious activity without burying yourself in noise.

Creating high quality detections is a **skill**. Similarly to languages, these skills can be applied across platforms and technologies once learned. An example of a more **advanced detection** could be one that identifies a user's most common historical IP addresses for Okta. This can then facilitate alerting on activity that was previously too noisy. Being able to operationalize and improve the efficiency of alerts makes you a force multiplier within SOCs.

Similarly, **threat hunting** is also a skill. Often, you'll be pivoting in the tool that you'll be making a rule in, aggregating data together, slicing it, performing long tail analysis and investigating telemetry alerting. It is vital to develop the ability to visualize data in a way that produces high quality threat hunting leads, identifying and bringing obscure activity front and center.

Platforms for Threat Hunting & Detection Creation

- ✓ **SentinelOne XDR** - XDR allows for the ingestion of various sources.
- ✓ **ELK Stack** - Source available logstash can allow you to ingest multiple sources.
- ✓ **Splunk** - Log management platform and observability platform.

Operate With A Tool-Agnostic Mentality

SOC analysts use a variety of tools for different purposes. Learn to be flexible and adapt to different tools instead of relying on one particular tool.

SOC analysts must be proficient in various tools and technologies used in cybersecurity. However, becoming too reliant on a specific tool or technology can hinder SOC analysts' ability to analyze and respond to security incidents effectively.

Being overly reliant on a specific tool or technology can lead to several risks for SOC analysts. First, analysts may not be able to see the complete picture of their organization's security posture if they only rely on a specific tool or technology. This can result in missed security incidents and vulnerabilities. Using multiple tools that need to be integrated is a common cause of inefficiencies in SOC analysts' workflows. This can result in delayed **incident response** times and increased workload. Relying too heavily on a specific vendor's tool can result in vendor lock-in, making switching to a different tool or vendor difficult if necessary.

To effectively master the art of SOC analysis and be tool agnostic, SOC analysts should follow these best practices:

- ✓ Develop a deep understanding of different tools and technologies used in cybersecurity.
- ✓ Focus on tool integration to reduce workflow inefficiencies and improve visibility.
- ✓ Use a mix of commercial and open-source tools to reduce the risk of vendor lock-in.
- ✓ Regularly evaluate and update the toolset to meet the organization's evolving security needs.

As the threat landscape evolves, SOC analysts must remain agile and adaptable to effectively detect, respond to, and mitigate security incidents. Being tool agnostic is a crucial component of this adaptability, enabling SOC analysts to select and use the best tool for the job, regardless of vendor or technology.

Being able to communicate technical concepts to those in non-technical roles is critical. Practice breaking down complex ideas into straightforward terms and communicating them effectively.

The role of SOC analysts involves working with different teams and stakeholders, including IT, security, and management. Effective communication ensures that members of all teams are on the same page and working towards the same goal.

When a security incident occurs, SOC analysts need to **communicate** effectively to **gather information**, identify the scope of the incident, and respond promptly to mitigate the threat. Clear and concise communication is critical during incident response to avoid confusion and ensure everyone understands their **roles and responsibilities**.

SOC analysts often collaborate with different teams to gather and analyze security data, identify potential threats, and develop effective security strategies. Effective communication is crucial for establishing and promoting teamwork.

Finally, SOC analysts communicate regularly with different stakeholders, including management, customers, and partners, to provide updates on security incidents, share security reports, and discuss security policies. Effective communication is essential to build trust and maintain strong relationships with these stakeholders.

Verbal & Written Communication Tips for SOC Analysts

As a SOC analyst, you need to be proficient in verbal and written communication to communicate effectively with different teams and stakeholders.



Verbal Communication

Use clear and concise language when communicating with others. Avoid using technical jargon or acronyms that others may not understand. Active listening is the other half of effective verbal communication. Listen carefully to what others say and ask questions to clarify misunderstandings early on.



Written Communication

SOC analysts are also responsible for writing reports, creating security policies, and communicating via email or chat with others. Use simple language when writing reports or emails. Avoid using technical jargon or complex sentences that others may find difficult to understand. Use short and to-the-point sentences to convey your message and avoid using long and convoluted sentences whenever possible.

Develop Effective Questioning Skills

Asking the right questions is essential for gathering information and understanding issues. Practice asking targeted questions to gather more information and better understand problems.

By developing good questioning skills, SOC analysts can gather accurate and relevant information, identify patterns and trends, collaborate effectively with other teams, and identify and mitigate hidden **threats**. SOC analysts can become more effective and better protect their organizations through active listening, open-ended and contextual questions, and follow-up questions.

Good questioning skills enable SOC analysts to gather accurate and relevant information from various sources, including users, systems, and logs. By asking the right questions, SOC analysts can obtain the information required to understand the scope and impact of a security incident fully.

Targeted questions are key to identifying patterns and trends in security incidents that may not be immediately apparent through data analysis alone. This enables SOC analysts to understand a security incident's root cause better and implement effective mitigation strategies.

Cyber attackers often use stealthy techniques to hide their activity, making it difficult for SOC analysts to detect and mitigate threats. Good questioning skills enable SOC analysts to uncover hidden threats by asking targeted questions that may reveal otherwise undetected activity.

Developing Good Questioning Skills for SOC Analysis

- ✓ **Engage and listen actively** - Active listening is critical to good questioning skills. To gather accurate and relevant information, SOC analysts must be fully present and engaged when communicating with users, system administrators, and other stakeholders.
- ✓ **Ask open-ended questions** - Open-ended questions encourage users and other stakeholders to provide detailed information and explanations, enabling SOC analysts to fully understand the scope and impact of a security incident.
- ✓ **Ask follow-up questions** - Follow-up questions enable SOC analysts to obtain additional details and clarification, helping them to identify patterns and trends in security incidents.
- ✓ **Ask contextual questions** - Contextual questions help SOC analysts understand a security incident's bigger picture, including the business impact and related incidents or events.

Reinforce Your Knowledge

As an analyst, your “pools of knowledge” expand and connect concepts together over time. The depth and breadth of these “pools” and how they connect is what defines your expertise as an analyst.

As analysts, we benefit from having a wider exposure to different **tools**, **applications** and **architectures**. When reviewing potentially malicious activity, we're often identifying if confidentiality, integrity, or availability was impacted. "The Outdated Jenkins Master Server being public", with the context of Jenkins, how it operates, and what vulnerabilities it has suffered, creates additional avenues of implication and risk that need to be assessed.

Alternatively, this also eliminates going down time-consuming rabbit holes during investigations. Every analyst has had experience tugging on a thread for hours, just to find out that the activity was benign and expected for that particular technology.

To counter this, analysts should expose themselves to as many environments, tools, and architectures as possible. Learning new concepts, how they connect, and their ability to impact one another returns exponential value within security.

This allows analysts to speed up the ability to analyze while also exposing obscure implications from activity. While no analyst can be an expert in all domains, even “puddle-deep” knowledge can be enough to connect multiple concepts together.

Join The Cybersecurity Community

Joining the cybersecurity community can be beneficial for SOC analysts. Participate in online forums, attend conferences, and network with other professionals to learn and share knowledge.

On the journey to gaining experience, SOC analysts often find support as part of a community of like-minded professionals who can provide guidance and insights into the latest industry trends. By joining the SOC analysis community through online communities, conferences, meetups, and certifications, SOC analysts can enhance their skills, advance their careers, and stay up-to-date with the latest industry trends. Ultimately, being part of a community of professionals can help SOC analysts become more effective and better protect their organizations.

Joining the SOC analysis community provides access to a wealth of knowledge and expertise from other professionals in the field. By sharing insights and best practices, SOC analysts can learn from others' experiences and improve their skills and techniques.

Being part of a professional community can also help SOC analysts advance their careers by providing opportunities for networking, mentorship, and professional development. SOC analysts can gain valuable insights into the job market, career paths, and skills needed to advance in the field.

Joining the SOC analysis community provides access to the latest industry trends, developments, and challenges. SOC analysts can stay up-to-date with the latest threats, technologies, and techniques and learn how others address similar challenges.

How to Get Involved in the SOC Analysis Community

- ✓ **Online Communities** - Many online communities and forums are dedicated to SOC analysis, where professionals can connect, share knowledge, and collaborate on industry challenges. Some popular communities include Reddit's "SOC" subreddit and the "SOC Talk" group on LinkedIn.
- ✓ **Conferences & Meetups** - Attending industry conferences and meetups is a great way to network with other professionals and gain insights into the latest industry trends. Many conferences offer workshops and training sessions specifically for SOC analysts, providing opportunities for professional development.
- ✓ **Certifications** - Earning industry certifications, such as the [CompTIA Security+](#), [Certified Information Systems Security Professional \(CISSP\)](#), or [GIAC Certified Incident Handler \(GCIH\)](#), can also help SOC analysts become part of a larger community of professionals and gain valuable knowledge and skills.

Conclusion

As more data breaches and ransomware occupy news headlines worldwide, enterprise leaders understand the absolute need for robust cybersecurity services such as security operation centers (SOCs).

Investing in aspiring security professionals means operational teams can detect intrusions and rapidly isolate them before they move deep into a sensitive environment and create long-lasting damage. SOC analysts are an essential part of this defense, proactively monitoring for early indicators of threat, providing real-time responses to security events, triaging actions, recovering assets, and triggering incident recovery mechanisms.

For aspiring SOC analysts, a combination of technical knowledge, analytical skills, and critical thinking abilities ensure they can truly understand the digital environment they are protecting. Together with the right stack of security tools, cybersecurity strategy, and top-down support from enterprise leadership, SOC analysts can keep their businesses safe from evolving threats in the cyber landscape.

[Contact us](#) today or [book a demo](#) to learn more about how SentinelOne can augment your business's cybersecurity posture against even the most sophisticated threats, tactics, and techniques used by threat actors today.

Tomorrow's Threats Require a New Enterprise Security Paradigm

SentinelOne provides one platform to prevent, detect, respond, and hunt ransomware across all enterprise assets. See what has never been seen before. Control the unknown. All at machine speed.



Autonomous EPP + EDR

Real-time detection and remediation of modern attacks at the endpoint, at machine speed, and without human intervention.



Unprecedented Visibility

Contextualize and identify threats in real-time. Patented Storyline™ technology reduces manual effort and automatically strings together related events in an attack storyline.



Frictionless Threat Resolution

Patented 1-click remediation and rollback accelerates recovery in real-time. Storyline Active Response or STAR™ provides proactive detection and response. For threat hunters and responders, remediation is integrated as a standard EDR response.



Simplified Experience

One agent consolidates security functions and reduces agent count. One console unifies administration of devices and cloud workloads. Fast to deploy. Easy to manage.



One Platform Across Your Attack Surfaces

Extend detection and response beyond endpoints with unified, native visibility and actionability for your cloud workloads, identity infrastructure, and more.



Vigilance

Extend your team with experience and expertise, defeat threats faster, and stay adaptive to new threats that arise.

Visit the SentinelOne website for more details, or give us a call at +1-855-868-3733

[Get a Free Demo](#)

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2022 Magic Quadrant for Endpoint Protection Platforms

**MITRE
GENUINITY**

Record Breaking ATT&CK Evaluation

- 100% Protection. 100% Detection
- Top Analytic Coverage, 3 Years Running
- 100% Real-time with Zero Delays

**Gartner
Peer Insights**

96% of Gartner Peer Insights™

EDR Reviewers Recommend
SentinelOne Singularity



Contact us

sales@sentinelone.com

+1-855-868-3733

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

sentinelone.com