



The Future of SOCs: Leveraging Automation and Intelligence for Greater Efficiency

Singularity AI SIEM

White Paper

The SOC Has an Efficiency Problem

Incidents begin and end in the Security Operations Center (SOC). From identifying Indicators of Compromise (IoCs) to remediating threats, SOCs need to harness efficiencies to match the growing speed and sophistication of adversaries—30% YoY increase in cyber attacks globally, reaching 1,636 attacks per organization per week.¹ Today, security teams need a plan of how to create those efficiencies. However, tremendous roadblocks, including an overwhelming volume and variety of data within legacy security solutions, keep them caught in an exhausting cycle.

SOC teams continue to struggle to pinpoint actual risks and filter out irrelevant data. These slow, clunky processes complicate their ability to respond effectively, while providing ample opportunities for threat actors to hide, as security analysts search for a needle in a haystack.

Security Information and Event Management Innovation Has Remained Flat

With legacy Security Information and Event Management (SIEM) solutions sitting at the center of the SOC, it plays an influential role in the rhythm of securing the business. These systems aggregate, correlate, and store data from various sources, allowing SOC teams to detect, investigate, and respond to security incidents. However, when overwhelmed with excessive data, legacy SIEMs become a double-edged sword. And that first depends on a SIEM being able to scale to meet the excessive data.

With legacy SIEMs, ingesting too little puts the organization's security posture at risk. While ingesting too much—often economically unfeasible for most organizations—overwhelms analysts with a flood of alerts, leading to negative consequences. After manually sorting them all, analysts often experience burnout, frustrated by false positives and low-priority alerts.

CISOs aren't interested in a traditional SIEM model that offers minimal improvements from what they have today.²

A lack of innovation also puts a strain on the SOC's infrastructure. The growing volume of incoming data demands ever-expanding storage, processing power, and network bandwidth, creating potential bottlenecks that slow down legacy SIEMs. These performance issues not only affect the SOC's ability to analyze and respond to security incidents in real time, but can also result in system instability or downtime.

Now is the Time for an Efficient SIEM

The need for a new plan stretches beyond the tactical level. With the rising volume and complexity of cyber attacks, boards and CEOs are putting pressure on security decision makers to reduce risk—highlighting the need for a solution for all.

In this white paper, we will explore how the future of SOCs lies in the adoption of intelligent automation and advanced analytics to tackle the data overload, improve operational efficiency, and stay one step ahead of increasingly sophisticated cyber threats.

¹ <https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/#:~:text=Check%20Point%20is%20100%25%20Channel,Q2%202024%20Global%20Cyber%20Attacks>

² 451 Research, *Platforms or stand-alone tools*, January 2025

Three Challenges to Overcome

Looking closer at the needs of today's SOC, there are three challenges to address.

1 | Complexity

Complexity is a multi-pronged issue. Outside of the SOC, attackers are employing advanced tactics that easily overwhelm outdated legacy tools. They are crafting attacks to be harder to predict and identify with the help of tools like Generative AI and automation. Only adding to the challenge is the growing complexity of modern environments, with expanding attack surfaces and numerous disparate security tools.

Peel back the curtain on the other side of attacks and you'll find SIEMs failing to keep up without AI and automation, leaving analysts with long alert queues that take hours to investigate. This not only leads to missed incidents, but also makes triaging more complex. Additionally, the need for complex system administration, customizations, and configurations further compounds the strain on teams. What was once the cornerstone of security operations has become a data dumping ground, unable to deliver the timely, actionable insights needed to respond to today's evolving threats.

2 | Talent Skills Gap

The ongoing cybersecurity skills gap remains a significant challenge for businesses, with a demand for qualified professionals far outpacing supply. This issue persists despite a 12.6% growth in the global cybersecurity workforce in 2023.³ In 2024, the shortage of cybersecurity professionals stood at 4 million, and if not addressed with advanced technology and innovative solutions, this gap could grow to 85 million by 2030.

The problem goes deeper than headcount alone. The distribution of tasks amongst teams is keeping everyone from doing work that is fulfilling and efficient. At one end of the spectrum, complex investigations overwhelm junior analysts, and at the other, large shares of burdensome work run senior analysts ragged. Neither can remove enough low-level tasks to achieve proactive threat hunting and analysis. And because of this, analysts feel dissatisfaction that leads to churn. Looking forward, security teams can't afford to operate this way. In the face of economic headwinds, analysts' time and limited budgets need to be used decisively.

3 | Time Constraints

Siloed data creates manual and time-consuming investigations. Since legacy SIEMs lack integration capabilities, investigations require swivel chair work. Analysts must go in and out of different security tools to connect the dots and understand the full scope of an incident. This means that each alert can take a few hours up to several days to address, depending on the complexity and severity of the incident. Without tools to provide sufficient context and collaboration, security teams won't be able to combat fast-moving, heavily armed adversaries.

³ World Economic Forum, [The cybersecurity industry has an urgent talent shortage. Here's how to plug the gap](#), April 2024

The Autonomous SOC Journey

Is there a cure-all for these challenges? Many hint at automation as the answer to the SOC efficiency problem. Yet, we are far from a futuristic human-free hub where machines unilaterally defend an organization against attacks. This may be possible in the future, but for today, we need to ask, “What kind of autonomy is desirable, and to what degree can we realize it?”

Organizations need AI and automation to work in harmony with humans. Through a symbiotic relationship, analysts can focus on high-value work and decisions, maximizing the application of human intelligence to security operations. By doing so, SOCs transform into a team that is efficient, agile, and intelligent. Today, we call this an Autonomous SOC.

The Autonomous SOC can take immediate action, intercept events in real time, and go beyond mere visibility dashboards to leverage hyperautomation and AI.



To be Efficient, Your Data Needs to Work for You

According to the Autonomous SOC Maturity Model, for organizations to predict new attacks and automatically create detection logic with some level of autonomy using a Large Language Model (LLM)-based system, they must supply it with rich, high-quality data.

How to Achieve Rich Data

- Use a columnar database for unparalleled scalability. This allows you to retain one hundred percent of data for deeper insights, unlike legacy systems that filter out most data.
- Multi-tenancy architecture with a massively parallel query engine, leveraging microservices, breaks down complex queries into manageable tasks and swiftly aggregates results.
- Ingest structured and unstructured data with natively-supported Open Cybersecurity Schema Framework (OCSF) to convert data for consistency and clarity and allows for natural language interaction with data, removing manual query syntax building.
- Ensure data is always accessible and performant with always-on hot storage, including historical data. This approach supports rapid results when searching logs or analyzing events, enhancing system efficiency, user satisfaction, and productivity. By reducing the friction that analysts are used to from querying cold or archived data, it minimizes delays that can impede security operations and frustrate teams during critical incidents.
- Real-time threat detection on ingestion.

SQL-like queries for SIEM detections are insufficient compared to columnar format for near real-time log analytics. SQL-like queries are relatively basic, lack the flexibility needed for thorough data investigation, and fall short in deriving actionable insights.

OCSF is a standardized, open-source framework designed to help organizations streamline and improve interoperability of cybersecurity data across different security tools and platforms.

Understanding Hyperautomation

After achieving broad, enriched security-specific data, SOCs have the foundation for hyperautomation.

Legacy SOAR vs. Hyperautomation

Legacy Security Automation	Next-Generation Automation
SOAR solutions, integrating orchestration, automation, and response, have traditionally streamlined security processes through playbooks and machine-assisted human analysis.	Hyperautomation, as defined by Gartner, is a strategic approach enabling organizations to extensively automate their business and IT processes.

Advancing Beyond Automation

Hyperautomation is often viewed as an advanced or enhanced form of automation. While traditional automation focuses on streamlining specific tasks, hyperautomation takes a more comprehensive approach by leveraging a variety of technologies and tools to automate a broader range of tasks and processes.

Hyperautomation begins with identifying workflows or processes that are ideal for automation. This typically involves targeting repetitive, manual tasks or operations with high transaction volumes. The next step is selecting the most appropriate technologies and tools for automation. For instance, Robotic Process Automation (RPA) is effective for simple, repetitive tasks, while AI may be better suited for more complex tasks. Once SOC teams choose the right tools, they are integrated into existing workflows to streamline operations. To extend this benefit, hyperautomation encourages the reuse of successful automation solutions to minimize the need for reinventing automation for each new use case, saving both time and resources.

Hyperautomation Works in Many Scenarios

Hyperautomation serves to simplify automation and make it more accessible to manage the spectrum of attacks. Depending on the maturity of the solution, it can handle cyber threats, such as ransomware mitigation, as well as other tasks like asset compliance monitoring and responding to suspicious user activity and insider threats.

Because it is flexible to your needs, no job is too big or small...

This is key for when adversaries deploy a host of smaller threats to serve as a distraction from their real, hard-hitting attacks. In these cases, analysts get caught up in trying to identify, research, and respond to the events. When that happens, threat actors have SOCs right where they want them—trapped and burnt out—and best yet, distracted from the ideal target.

By integrating hyperautomation, SOC teams can eliminate bottlenecks, reduce analyst fatigue, and focus on higher-value security tasks.

How to Achieve Hyperautomation Benefits

- Automatically generate playbooks based on peer-driven insights, empowering teams to respond faster and more efficiently.
- Designed to be highly flexible and fast, allowing teams to integrate with any API and create customized actions tailored to their specific need without requiring extensive code.
- Offers no-code management so it is easy to use for every level of analyst.

Automating Opens the Door to Threat Hunting

We know swivel chair management doesn't work to spot threats early in the kill chain. And based on a report published by Cybersecurity Insider⁴, traditional security tools miss 38% of advanced, emerging threats. Without detection, those threats can lurk for months while attackers stealthily gather valuable information to steal or data to compromise. If you wait until these threats become visible or a traditional SOC tool monitoring tool sends an alert, it can be too late.

Efficiencies Through Threat Hunting

Using hyperautomation to remove the constraints that prevent meaningful threat hunting, SOCs can finally effectively manage threats. Then, analysts can focus on not only threat hunting, but doing so at a powerful level.

Successful and Efficient Threat Hunting Requires

- A clear view of the "right" data with contextualized and correlated events in unified detections.
- A data baseline to identify what is normal and what is an outlier.
- Hypothesis-driven workflows.
- Investigations of various tools and techniques to discover new malicious patterns in the data and uncover the attacker's TTPs.
- Ability to effectively respond and remediate the threat once found. And, improve security and prevent attacks of a similar manner in the future.

⁴ [Intrusion, The State of Threat Hunting, 2022](#)

What Analysts Need to Feel Like Threat Hunting Powerhouses

- **Unified workflows.** Analysts need unified data access so that they can query enterprise data from first and third-party sources and partner threat intelligence.
- **Use of natural language.** To speed hunts, analysts need to use natural language to prompt GenAI. Analysts can better investigate, make faster decisions, and reduce mean time to response if they have AI SecOps tools such as threat hunting quick starts, summaries, suggested queries, recommended responses, and more.
- **Time to focus on what's important.** Automatically generated threat summaries help quickly determine a verdict for each alert and event across security stacks. It also helps analysts save time to focus on what's important by providing easy access through its natural language interface to seamless query data for threats and identify stealthy attacker activity.

Power of AI in Security

As of the publication date of this paper, the current AI SecOps market is nascent with only a few notable players, most of which are not generally available yet. With the threat landscape becoming more volatile by the day, and threat actors using AI to craft attacks, security teams don't have time to wait for the technology they needed yesterday. Everyone, from security decision makers to analysts, needs to feel confident that they are not creating a black box of AI. They require the tools to input a natural language prompt or query and receive a query back so that analysts have peace of mind in the output and results. And to uplevel junior analysts, it should train on what the query looks like rather than requiring blind trust of the results.

Go Beyond the Standard Model and Chatbot

Without a multimodal approach, you're missing out on AI's best of breed and the newest capabilities from each vendor. At the same time, security teams may potentially fear that inputting sensitive data into foundational models will be used for training. This is essential along with how analysts interact with GenAI.

Chatbots that only answer questions will not create meaningful efficiencies in the SOC. Analysts will still struggle with limited collaboration and a lack of documentation and context among their team, which would allow them to repeat or collaborate on investigations. Instead, analysts need a dedicated workspace to leverage AI across security scenarios. Including, quickstarts with out-of-the-box threat hunts for use cases such as endpoint incident response, suspicious user activity, and cloud threat remediation, helping teams ramp up automation faster.

Understanding the Nuance of AI

AI: Systems that use advanced analysis and logic to mimic intelligent behaviors, including understanding artifacts/language, producing new artifacts/language, and taking or automating actions.

ML: Class of algorithms whose behavior changes based on the data given.

GenAI: Subset of highly-scaled ML models that can learn from a representation of artifacts, and when prompted, can generate new related artifacts.

LLMs: Type of generative AI models trained on large volumes of text to understand text inputs and generate human-like text outputs.

Advancing Past Next-Gen SIEM With AI SIEM for the Autonomous SOC

Enterprise security teams no longer have to accept manual time-consuming investigations and alert fatigue. Using traditional expensive SIEMs that provide sub-standard data enrichment ends here, opening a new door to a highly autonomous SIEM. With a cloud-native SaaS architecture and cutting-edge AI and automation tools, SentinelOne gives SOCs the tools needed to shift the security analyst role from monotonous tasks and laborious hands-on investigations to system supervision and optimization.

Driving Efficiency Starts With Your Data

SentinelOne's AI SIEM provides the foundation for unmatched data accessibility. Built in the cloud for exabyte scale, it can handle any data load your organization needs. And unlike legacy systems that discard much of the data, AI SIEM preserves data richness which is essential for advanced security analytics. This allows for:

- Immediate threat detection and ingestion for damage prevention from attacks that might be happening in real-time.
- Comprehensive investigations with faster queries.
- Pure speed without indexing.
- Long-term data storage without the exorbitant cost.

Automatically Mitigate Critical Threats So You Can Focus on High-Impact Work

Autonomous operations thrive on broad, enriched security-specific data. With AI SIEM delivering comprehensive insights, it can automatically mitigate critical threats before they can disrupt your business.

To achieve this, hyperautomation:

- Is highly customizable and flexible, allowing you to design workflows tailored to your specific security needs.
- Seamlessly integrates with any SaaS application, streamlining processes to reduce the volume of high alerts and exposures.
- Enhances efficiency by automating triage, investigation, and response.
- Enriches alerts that require further attention with valuable context, pulling data from threat intelligence feeds, vulnerability information, and historical event log.

Simplify the Complex

With Purple AI, SentinelOne translates natural language security questions into structured queries, summarizes event logs and indicators, guides analysts of all levels through complex investigations and scales collaboration with shared investigation notebooks.

Supercharge Analysts With Intelligent Tools

Conduct deeper investigations with streamlined workflows, contextual follow-up queries, and natural language support to stay ahead of attacks. Even less experienced analysts can now confidently threat hunt.

80%

faster threat hunting and investigations, as reported by early adopters.

128%

easier threat hunting, as reported by early adopters.

78%

of surveyed early adopters found the notebooks feature either very or extremely helpful.

Purple AI does not use your queries to improve its models, unless you flag a Purple response for review, feedback or support. Purple interacts with existing SentinelOne Singularity Data Lake technology and stores your data in the same way.

Detect Earlier, Respond Faster, and Stay Ahead of Attacks

Operate at peak efficiency with the following features:

Natural Language Translation

Querying your data is as easy as asking a colleague a question. Simply ask Purple AI, "Am I being targeted by FIN12?" without needing to reference data schemas or create complex queries. This enables faster and more effective threat hunting for every analyst.

➔ Am I being targeted by FIN12?

```
| filter ( src.process.image.md5 inanycase ( "0a34a2c61c6f84f178cf0035f218d79e", "17b461a082950fc633228572138b80c", "2cc79806701f1a6e877c29b93f06f1bb", "563b5372c93c74f1e0268c079ce9d43", "6798f540f3d077c3cda2f5a4a8559f7", "6a58b52b184715583cda792b56a0a1ed", "72a589da586844d7f0818ce684948eea", "a0e9f5d64349fb13191bc781f81f42e1", "aa97e84ddf87f96092e40ae29e9a63", "c0cacc5b9f7b854b6025fe0973dc076f", "c12f54a3f91dc7baf92cb59fe009a35", "c28b33f7365f9dc72cc291d13458f334", "ec74a5c51106f0419184d0d08fb05bc" ) OR tgt.process.image.md5 inanycase ( "0a34a2c61c6f84f178cf0035f218d79e", "17b461a082950fc633228572138b80c", "2cc79806701f1a6e877c29b93f06f1bb", "563b5372c93c74f1e0268c079ce9d43", "6798f540f3d077c3cda2f5a4a8559f7", "6a58b52b184715583cda792b56a0a1ed", "72a589da586844d7f0818ce684948eea", "a0e9f5d64349fb13191bc781f81f42e1", "aa97e84ddf87f96092e40ae29e9a63", "c0cacc5b9f7b854b6025fe0973dc076f", "c12f54a3f91dc7baf92cb59fe009a35", "c28b33f7365f9dc72cc291d13458f334", "ec74a5c51106f0419184d0d08fb05bc" ) OR tgt.file.md5 inanycase ( "0a34a2c61c6f84f178cf0035f218d79e", "17b461a082950fc633228572138b80c", "2cc79806701f1a6e877c29b93f06f1bb", "563b5372c93c74f1e0268c079ce9d43", "6798f540f3d077c3cda2f5a4a8559f7", "6a58b52b184715583cda792b56a0a1ed", "72a589da586844d7f0818ce684948eea", "a0e9f5d64349fb13191bc781f81f42e1", "aa97e84ddf87f96092e40ae29e9a63", "c0cacc5b9f7b854b6025fe0973dc076f", "c12f54a3f91dc7baf92cb59fe009a35", "c28b33f7365f9dc72cc291d13458f334", "ec74a5c51106f0419184d0d08fb05bc" ) OR module.md5 inanycase ( "0a34a2c61c6f84f178cf0035f218d79e", "17b461a082950fc633228572138b80c", "2cc79806701f1a6e877c29b93f06f1bb", "563b5372c93c74f1e0268c079ce9d43", "6798f540f3d077c3cda2f5a4a8559f7", "6a58b52b184715583cda792b56a0a1ed", "72a589da586844d7f0818ce684948eea", "a0e9f5d64349fb13191bc781f81f42e1", "aa97e84ddf87f96092e40ae29e9a63", "c0cacc5b9f7b854b6025fe0973dc076f", "c12f54a3f91dc7baf92cb59fe009a35", "c28b33f7365f9dc72cc291d13458f334", "ec74a5c51106f0419184d0d08fb05bc" ) OR ( src.process.image.sha1 inanycase ( "17d9200849e0b5224644a51f0d1982fac54d844", "2eb07b4bdc826c2e865931113e-d89c8bccd0042", "3477a173c2c1005a81d402802ab0f22c12a4d55", "c9d5b5f6e0f034ee40703202630694997361dec", "d1387f3c94464d811a64207315b13b578fd10c", "fac0269ee01837c1d221ad778b5f88de831aac2" ) OR tgt.file.sha1 inanycase ( "17d9200849e0b5224644a51f0d1982fac54d844", "2eb07b4bdc826c2e865931113e-d89c8bccd0042", "3477a173c2c1005a81d402802ab0f22c12a4d55", "c9d5b5f6e0f034ee40703202630694997361dec", "d1387f3c94464d811a64207315b13b578fd10c", "fac0269ee01837c1d221ad778b5f88de831aac2" ) )
```

Show More

71 results found March 4, 2025 5:21 PM - March 5, 2025 5:21 PM Open PowerQuery

Event Time	Event ID	Event type	Agent UUID	Source Process Unique ID	Site ID	Site Name
Mar 5, 2025 3:02:38 PM	01JNKYG800826GR1AZP...	DNS Resolved	pve 04a5c062-a99d-2c8d-798f-...	pihole-FTL 165a5d9b-b968-a66b-dad4-...	1292175278334071117	peti
Mar 5, 2025 3:01:56 PM	01JNKYD8GCVEMYS1GF...	IP Connect	Paulas-HP 6640413f929414095b594...	chrome.exe D1E9528228CC7528	1690846333702750315	Kse
Mar 5, 2025 2:19:36 PM	01JNKVZM827XJABGN2A...	IP Connect	DESKTOP-C1L838F 410a3e0793824f8487ae1d...	msedge.exe A0AD84658B892E9D1	507511400611377121	JKir
Mar 5, 2025 2:06:06 PM	C3F0449F-AFFF-424D-AR...	DNS Resolved	Saiyain	Arc Helper	1971007189199072784	Adr

Ask Purple AI...

Multilingual Queries

Break language barriers with multilingual threat hunting. Purple AI enables security teams worldwide to ask questions in their preferred language, delivering precise insights, faster investigations, and streamlined collaboration across global operations.

↪ Can you write a summary of this hunt in Spanish?

◆ Claro, aquí tienes un resumen en español:

Resumen de la Búsqueda:

- **Presencia de FIN12:** Se detectaron múltiples solicitudes DNS a dominios asociados con FIN12, como "ublockorigin.github.io" y "darkreader.org", lo que indica un posible objetivo por parte de este actor de amenazas.
- **Conexiones de Red:** Se registraron conexiones de red salientes significativas, particularmente a direcciones IP como 185.199.108.153, vinculadas a actividades de FIN12.
- **Diversidad de Endpoints:** Se observó una variedad de endpoints involucrados, incluyendo sistemas macOS y Windows, lo que sugiere una estrategia de ataque amplia por parte de FIN12.
- **Comunicación con IPs de FIN12:** Varios endpoints, como "Matt, the M1 Max Mac" y "Paulas-HP", han comunicado con direcciones IP conocidas de FIN12, indicando una participación activa con los recursos de este actor de amenazas.
- **Tipos de Eventos:** Los tipos de eventos incluyen principalmente solicitudes DNS y conexiones IP, destacando los métodos utilizados por FIN12 para establecer y mantener su presencia en la red.

Si necesitas más detalles o asistencia adicional, no dudes en preguntar.

Threat Hunting Quickstarts

Reduce hunting cycles from hours to minutes by starting investigations with a curated list of quick start prompts.



🔍 Threat hunting

- ↪ UNC1878 indicators present?
- ↪ MITRE T1140 related events
- ↪ User creation/modification events

35 More >

📄 Support questions

- ↪ Find install logs
- ↪ Check agent status
- ↪ Purpose of exclusions

18 More >

Summaries & Suggested Follow-Ups

Understand the results and dive deeper into investigations with smart suggestions.

- The presence of multiple DNS requests to known malicious domains, such as "ublockorigin.github.io" and "darkreader.org," indicates activity consistent with FIN12's tactics, techniques, and procedures (TTPs).
- Significant outgoing network connections were observed, particularly to IP addresses like 185.199.109.153, which are often associated with FIN12 operations.
- The variety of endpoints involved, including both Windows and Linux systems, suggests a broad targeting approach typical of FIN12's operations.

👍 🗨 ⌚ ● Question 1 out of 20

Follow-Up questions:

- ↪ What specific indicators of compromise (IOCs) are associated with FIN12 activity in my environment?
- ↪ Can you list the endpoints that have communicated with known FIN12 infrastructure?
- ↪ What are the common tactics and techniques used by FIN12 that have been detected in my network?

Alert Summaries

Natural language alert summaries help you quickly understand the context of the alert and remediate faster.

Ramnit Command and Control Traffic Detection

🔴 High | 🕒 Spyware | ⌚ Mar 5, 2025 10:07:41 AM

[Actions](#) [Mitigate](#) [Automate](#) [Event Search](#)

[Overview](#) [Indicators \(6\)](#) [Mitigation \(0\)](#) [Notes \(0\)](#) [History \(0\)](#) [Graph](#) [Raw data](#)

Alert Status: [New](#) | Assigned To: [-](#) | Analyst Verdict: [Undefined](#)

◆ **Purple AI summary**

The alert indicates a high-severity detection of command-and-control traffic associated with the Ramnit malware, originating from the internal IP address 192.168.100.2 and targeting the external IP address 44.221.84.105. The traffic was identified by a Palo Alto Networks Firewall, which flagged it due to its ability to transfer files and exploit known vulnerabilities. The detection involved outbound traffic through the ethernet1/1 interface and was linked to a VPN rule, suggesting potential tunneling of malicious activity. This incident highlights a significant risk to the endpoint, warranting immediate investigation and remediation efforts.

[^ Less Detail](#) Was this useful? 👍 🗨

Event Summaries

Natural language summaries of query results and events, including indicators. Spend less time summarizing events and writing incident reports.

Process Creation

Mar 05, 2025 17:35:23

Event Actions ▼

Agent UUID COSMOS-EP1 0ecc9268a5c6470fbfac754ab9af95a8	Source Process Unique ID UserOOBEBroker.exe B91392AF2EEAD881	OS Source Process Unique ID svchost.exe 684C91AF2EEAD881
Target Process Unique ID FileCoAuth.exe 2C8594AF2EEAD881	Source Process Command Line C:\Windows\System32\oobe\UserO...	Source Process User COSMOS1\cosmos1_user1
Target Process Command Line "C:\Users\cosmos1_user1\AppData\L...	Target Process User COSMOS1\cosmos1_user1	

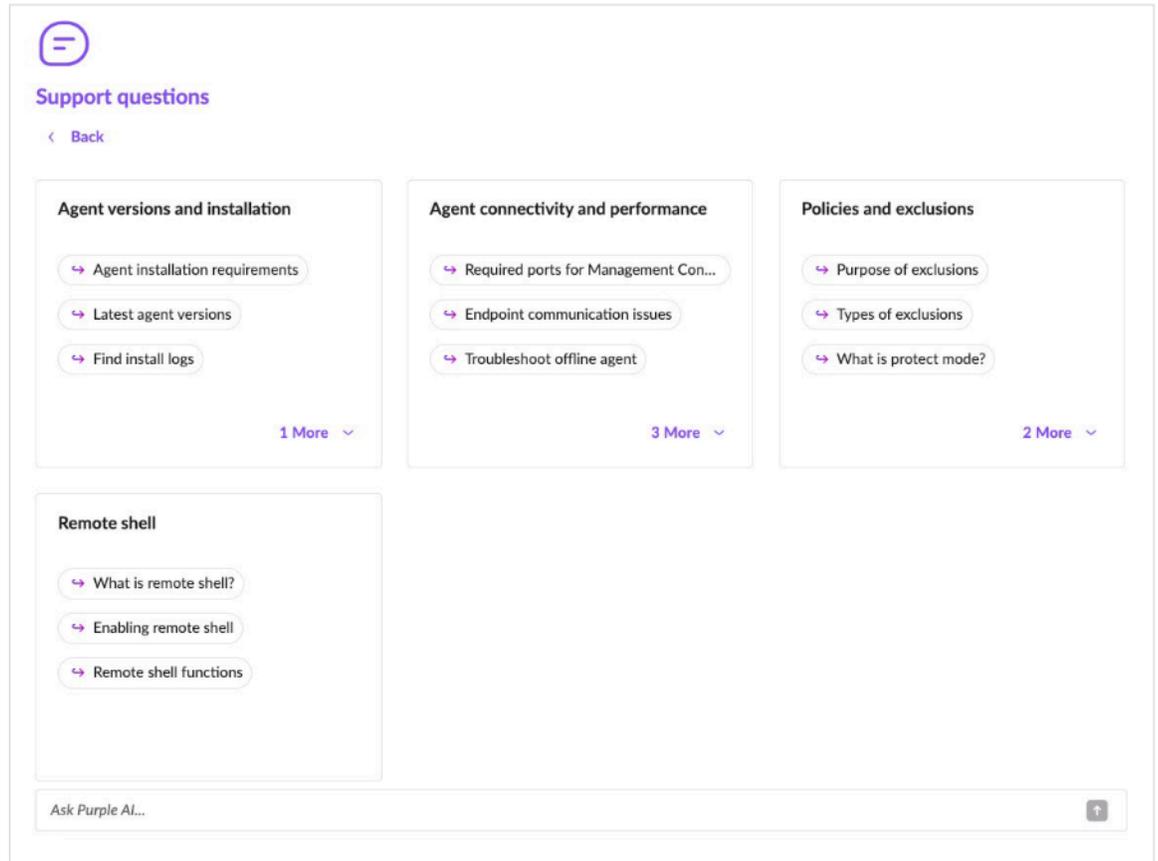
◆ Purple AI summary

The event log indicates the creation of a target process, "FileCoAuth.exe," which is associated with Microsoft OneDrive's co-authoring functionality. This process was initiated by "UserOOBEBroker.exe," a legitimate Windows process, under the context of the user "COSMOS1\cosmos1_user1." Notably, the source process "svchost.exe," which is a critical system process, was running under the "NT AUTHORITY\SYSTEM" account. The target process is signed and verified, suggesting it is a legitimate executable, and it operates at a medium integrity level. However, the source process has a high count of behavioral indicators (248), including 4 indicators of evasion, which may warrant further investigation to rule out any potential misuse or compromise. Additionally, the event log shows no file creation, modification, or deletion activities associated with either the source or target processes, indicating that the processes were not engaged in any suspicious file operations at the time of this event. The absence of network connections and the high count of duplicate process handles (5185) for the source process could suggest unusual behavior, potentially indicative of a process that is heavily interacting with other processes or system resources. Given the context and the indicators present, it is advisable to monitor this process further for any anomalous behavior or signs of exploitation.

[^ Less Detail](#) Was this useful?

Support

Instead of having to go read the Documentation, you can ask Purple a question in plain language and get a response.



Experience the Game-Changing Difference of Ingesting All Data, And Fast

Rapid MTTR and MTDD, plus more productivity with Purple AI and hyperautomation means having the power to protect your organization now and into the future.

AI SIEM provides the speed and power to stay ahead of threats. For more information, visit: sentinelone.com/platform/ai-siem/

Innovative. Trusted. Recognized.



A Leader in the 2025 Magic Quadrant for Endpoint Protection Platforms



Industry-leading ATT&CK Evaluation
+ 100% Detections. 88% Less Noise
+ 100% Real-time with Zero Delays
+ Outstanding Analytic Coverage, 5 Years in a Row



96% of Gartner Peer Insights™ EDR Reviewers Recommend SentinelOne Singularity





Contact Us

sales@sentinelone.com

+1-855-868-3733

sentinelone.com

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 2025