



SDR BUYER'S GUIDE

The essential guide for evaluating AI-driven SIEM detection and response for your cyber security transformation



TABLE OF CONTENTS

1. WHAT IS CYBEREASON SDR?	3
2. WHAT IS SECURITY OBSERVABILITY?	4
3. SECURITY OBSERVABILITY VS. THE DIFFERENCE BETWEEN SIEM AND XDR	6
4. SDR - THE CONVERGENCE OF SIEM AND XDR	9
5. UNCOMPROMISING ENTERPRISE SECURITY DATA STRATEGY	10
6. LEVERAGE YOUR ENTERPRISE DATA LAKE STRATEGY & EXISTING INFRASTRUCTURE	12
7. HOW CAN SDR ENHANCE CYBER RESILIENCE WITH AI-DRIVEN ANALYTICS?	14
8. WHAT ARE THE EFFECTIVE METRICS TO MEASURE SDR DEPLOYMENT?	16



1. WHAT IS CYBEREASON SDR?

Cybereason SDR, or SIEM Detection and Response, is a cybersecurity evolution by combining multiple security technologies (EDR, XDR and SIEM) to provide comprehensive threat detection, response and remediation capabilities powered by AI and Observability. It aims to enhance the efficacy and efficiency of security operations across diverse IT estates by integrating and correlating data from various security toolsets into a unified enterprise security data lake. Often augmented with managed detection and response services (MDR/MXDR), this SaaS offering provides holistic and unified cyber defense capabilities to simplify the management and operation of security technologies, processes, and data.

As enterprises continue to invest into digitalisation, they are increasingly encountering an evolving threat landscape and complex security challenges - with more workloads in multi clouds, more workforces in hybrid environments, and more intelligent devices connected in mission critical operations. This transformation journey is exacerbated by exponential increase in compute resources, data volumes and security toolings, driving up the cost of storing, managing and analyzing the data for security purposes. SDR presents a more efficient, proactive solution to address modern cybersecurity operations and data challenges. In contrast to solutions like EDR, XDR, and SIEM that emphasize on security monitoring for after the fact threat detection, SDR broadens the scope of security observability across an organization's complete attack surfaces and vulnerabilities.

When attackers use creative, modern techniques, threats can hide and weave between security data silos, spreading slowly over time to evade detection and gain stealthy persistence. This leads to security staff trying to triage and investigate the problem as it hits different parts of the IT estates. Traditional security tools, such as SIEM, typically operate in log aggregation and correlation based on limited connectors that ingest a subset of the data required including point-in-time security events and predefined thresholds for alerting, making it difficult to provide deep insights for root cause analysis and investigation (e.g. how and why) of security threats and vulnerabilities. Security analysts then need to manually retrieve missing data from different tools in order to build the true picture of a malicious operation, increasing mean time to detect and respond, which in turn increases the risk and cost of a breach that leads to material damage.

SDR addresses these limitations by taking an open, centralized data lake approach that consolidates all the trace and metrics data across all existing cyber security tools at a vastly reduced cost. In addition, broader observability is provided across this consolidated data lake to find these threats, tracing the bigger picture across multiple security layers - endpoint, server, email, identity, network, and cloud. By leveraging behavioral data analytics and AI-driven investigation, SDR can provide a more holistic view of security incidents for timely and accurate threat detection and response - to stop cyber breach earlier and assure business resilience.



2. WHAT IS SECURITY OBSERVABILITY?

Security observability refers to the ability to understand and gain real time insights into the security state and events within a system or application through the collection, analysis, and visualization (structural graph)

of relevant security data. It involves monitoring and tracking security-related logs, metrics and traces to detect, investigate, and respond to security threats and incidents effectively.

KEY ASPECTS OF SECURITY OBSERVABILITY INCLUDE:

- **Data Collection:** Collecting data from various sources such as logs, metrics, and traces to provide a comprehensive view of the security posture.
- **Analysis:** Analyzing the collected data to identify patterns, anomalies, and potential security threats.
- **Visualization:** Visualizing the analyzed data into structural graphs to make it easier for security teams to understand and act upon.
- **Alerting:** Generating alerts based on predefined rules or machine learning algorithms to notify security teams about potential security incidents.
- **Incident Response:** Providing the necessary information and context to enable security teams to perform root cause analysis and investigation, and to respond quickly to security incidents.

To achieve security observability, data must be gathered from diverse security tools and systems such as network logs, endpoint security solutions, and security information and event management (SIEM) platforms. This data is then used to uncover insights into potential threats. Unlike traditional security operations tools that only reveal ongoing events, security observability predicts likely future events. This distinction makes security observability one of the most significant advancements in cloud security technology in recent years.

Overall, observability plays a crucial role in detecting and responding to security threats, as it enables security teams to identify anomalies and suspicious activities that may indicate a security incident. This means that by monitoring and analyzing the behavior of the system, such as its network traffic, application performance, and user interactions. Cybersecurity professionals can gain insights into the system's security posture and potential vulnerabilities, enabling them to detect and respond to broader security threats more effectively.



SECURITY OBSERVABILITY VS. SECURITY MONITORING



Visibility

Logs | Point in time record



Monitoring

Metrics | Performance over time



Alerting

Alerts | Matched Condition



Observability

Traces | Root Cause Analysis



Security Monitoring:

What Happened, When & Where?

Collection, analysis and response to security related events

Security Observability:

Trace into How and Why?

Provide deep insights for root cause analysis and investigation of security threats and vulnerabilities



3. SECURITY OBSERVABILITY VS. THE DIFFERENCE BETWEEN SIEM AND XDR

Security Observability, XDR and SIEM are cybersecurity solutions that address different aspects of threat detection, response, and overall security operations.

Both XDR and SIEM solutions have their own considerations in comparison to security observability.

SIEM

- SIEMs are the cornerstone of all SOC's, but the dirty secret is that SOC teams don't receive (or see) value from their deployments. It is a system of record versus a security operations tool.
- Architecturally, SIEMs are static data warehouses that are not designed for AI-Powered real-time security data analytics.
- SIEMs are unable to keep up with the amount and diversity of enterprise data sources. SIEMs only retain the data the connector or parser was programmed to pick out as important, the rest of the data is discarded which means organizations are not able to look for new insights from the retained data as critical trace and metrics telemetry is missing hampering detections and investigations when breach occurred.
- Many security alerts generated by SIEMs are after the fact detections and alerts from security tools (e.g. malware detected). Because the SIEM holds a fraction of the less trace and metrics data (compared to Detection and Response tools like EDR, or NDR), SOC analysts are forced to use slow and manual processes to retrieve the missing data to identify indicators of behavior needed to build the entire flow of the malicious operation.
- These manual efforts take time, increase time to triage and response, and potentially lead organizations to suffer the material impact of a breach.

SIEMs are unable to keep up with the amount and diversity of enterprise data sources.



XDR

- For effective incident response, the SecOps team needs more data, with more detailed and actionable insights instead of the 'peak of the data' found in SIEMs.
- Detection and response systems came along that collect and hold full trace and metrics data (e.g. records the trail of behavioral data) that where advanced, AI-Driven analytics are applied to identify indicators of malicious behavior. EDR and NDR operationalised this in the market today, along with ITDR (identity), and CDR (cloud)
- But this created more silos of rich data held across different data systems - some tactical integration occurred in SIEMs, but because of the architectural and cost limitations, the data shared was restricted and after the fact alerts and detections, is not useful for SecOps, they still needed to work manually across these new data silos to retrieve missing telemetry and piece together the end to end malicious operation.
- Then came along XDR! - with the goal to expand the breadth and depth (quality) of data to include trace and metrics data across more sources, and correlate across these different security data sources beyond the endpoint and across the enterprise attack surfaces.
- XDR provides a holistic view of the organization's security posture and leverages advanced analytics techniques, such as AI-driven behavioral analysis, to detect and respond to emerging threats and anomalies, improving the accuracy of threat detection and reducing false positives.
- By consolidating security data and providing a unified view of incidents, XDR reduces the time and effort required for manual correlation and investigation. It enhances the efficiency of security operations by providing contextualized insights and actionable intelligence.
- XDR as a market has however met the needs of small and medium enterprises who are struggling with bridging the cybersecurity skills gap, out-of-the box integrations and correlation of data across a subset of key tools delivers the right balance between cost and protection.
- For larger enterprises though, XDR does not address the more complex use-cases demanded by their SecOps team and it cannot replace SIEMs that are used by large enterprises with complex SOC operations and compliance requirements.
- XDR has generated yet another data lake, in addition to the other data lakes from other detection and response systems and the logging systems from other security tools.



CAUTION: SIEM

- **SIEM COST:** With SIEMs you get charged on ingest, then get charged again to analyze the data. EDR's trace and metrics data is 10 to 100 times the volume of traditional log data. It is cost prohibitive for most enterprises to put enough of this data into a SIEM.
- **ALERT OVERLOAD:** SIEM solutions can generate a large number of alerts, leading to alert fatigue and potentially causing important alerts to be overlooked or ignored. Proper tuning and customization are required to manage and prioritize alerts effectively.
- **LIMITED SCOPE:** SIEM solutions primarily focus on log and event data, which may not provide a comprehensive view of security incidents. They may not capture threats that occur outside the logged events or have limited visibility into the behavior of endpoints or cloud environments.
- **RESPONSE ORCHESTRATION COMPLEXITY:** While SIEM platform with SOAR solution can automate incident response actions, implementing and configuring response playbooks can be complex. Organizations need skilled personnel to design and maintain the automation workflows effectively.
- **INTEGRATION CHALLENGES:** Integrating SIEM and SOAR solutions with existing security tools and platforms can be a complex task, requiring compatibility and proper configuration. Integration efforts may vary based on the ecosystem and APIs provided by different vendors.

CAUTION: XDR

- **XDR COST:** For many vendors, XDR has complex pricing and licensing and quickly scales up in cost for the customers as they pay per integration, and to ingest the data.
- **DEPLOYMENT COMPLEXITY:** Implementing an XDR solution may require significant integration efforts, as it involves collecting and correlating data from various security tools and platforms. Organizations need to ensure compatibility and proper configuration to achieve optimal results.
- **VENDOR LOCK-IN:** Native XDR solutions often come bundled with specific vendor ecosystems, which may limit flexibility and interoperability with existing security investments. Organizations should carefully consider vendor lock-in and evaluate integration capabilities.
- **CUSTOMIZABILITY:** XDR solutions are less flexible for creating custom correlation rules, dashboards, and reports compared to SIEM. Its main focus is on stopping attacks from progressing further, and typically offer basic traditional compliance use-cases at this stage.
- **INFRASTRUCTURE:** Many XDR vendors used SIEM-backed platforms or proprietary data lakes to deliver XDR solution, and for the same reason SIEM isn't the right platform for SecOps, XDR often still lacks the complete set of trace and metrics data to deliver enterprise security observability capabilities required by large and highly skilled Security Operations teams.

4. SDR - THE CONVERGENCE OF SIEM AND XDR

So how does the cybersecurity market solve the enterprise security data lake strategy and observability problem of detecting and responding to

attacks across the enterprise and delivering on the needs of the enterprise SOC to drive down MTTD-MTTI-MTTR, close the skills gap, and reduce costs?

APPROACH	SOLUTION
Not as common	<ul style="list-style-type: none"> ▶ Reduce the data that is pulled from the different detection and response data lakes - this compromises the comprehensiveness of the data meaning you can't see the overall picture and need to retrieve missing data during investigations.
More Common	<ul style="list-style-type: none"> ▶ Augment the SIEM with another data lake (EDR/XDR) for the high volume, high velocity data (trace and metrics data). This data lake is typically used on a per case / need basis, this is reactive and increases MTTD-MTTI-MTTR. ▶ Some lower-cost Data Lakes are often used as a cheaper way to store data (for compliance and reporting), but are not suited to real-time analytics (e.g. threat detection analytics) and automated response. ▶ Some organizations opted for a Native XDR or SIEM-based XDR which is built and provided by a single vendor as a cohesive and integrated offering. This includes all the components and functionalities required for Extended Detection and Response and their proprietary data lake with limited scalability and open system integrations, and often operates in a vendor lock-in environment. ▶ Many organizations have ended up with multiple data lakes for specific use cases like: Security detection and response, Business Applications, IT operations and Business Operations etc.
New Way Forward	<ul style="list-style-type: none"> ▶ Moving towards a unified enterprise data lake strategy (led by the CIO/CTO) for all big data across all use-cases. Paying once and getting the most value from leveraging much more cost effective data lake for multiple use-cases including security, GRC etc. ▶ Using security observability also enables data visualization and AI-Driven analytics in real time across this single data lake at a fraction of the cost of analytics of a SIEM. ▶ Applying the learnings from XDR including cross correlation between data sources, pre-build detections, guided remediation, but across the full set of raw data without the cost and performance limitations created by SIEM backed or proprietary data stores.

Convergence - The AI-driven security observability platform ("Cybereason SDR") is aims to disrupt the NG SIEM and Enterprise XDR market in the following ways:

- Addressing the very real and painful gaps that SIEM creates with the security operations team - increased MTTD & MTTR, High false positives, lack of visibility, increased risk of longer attacker dwell times, inefficient investigations, alert fatigue operations.
- Resetting the architecture of Enterprise XDR and enabling it to deliver on the promise that was made available in the open marketplace and integrate other solution vendors.
- Expanding the value of detection and response platforms beyond security to ensure they form part of the larger enterprise data lake strategies with observability capabilities.
- Balancing the exponential data growth with cost effective data costs of processing and analyzing the security data from enterprise attack surfaces for timely detection and response to cyber threats.
- Providing an unified cyber defense platform with AI assisted security operations to stop breach faster.



5. UNCOMPROMISING ENTERPRISE SECURITY DATA STRATEGY

Today's security operations teams are suffering the consequences of the business tradeoff between exponential data growth needed to remain effective vs. the exorbitant costs of processing and analyzing the relevant security data across enterprise attack surfaces to stop cyber breach.

Limited enterprise security data is driving up MTTD, MTTI and MTTR (meaning missed detections, longer

dwell times for investigation and response). With the lack of enterprise security data lake strategy and alignment with other business and IT stakeholders, organizations have ended up with multiple data repositories and siloed data lakes, each purpose built for different use cases. As a result, security operations are using data systems that are not optimized to deliver the effective outcome that they are looking for.

The adoption of Cybereason SDR could drive down data costs and improve analytics performance by consolidating your enterprise security data lakes. **The open data architecture of SDR is aiming to remove or reduce the cost barrier to migrating and ingesting all security data and gain meaningful visibility and observability across your enterprise.**



SECURITY DATA SYSTEMS

- Like SIEMs which were designed for ingesting logging for compliance purposes, with strong analytics capabilities, but over a limited data set based on point in time security events and logs.
- EDR and NDR data lakes that hold very high quality data (including trace and metrics data) but that are limited to endpoint and netflow data only, requiring console switching and manual correlation between systems.
- XDR promised the answer, but these XDR data systems that were built on top of SIEMs or proprietary data lakes are suffering the same challenges that despite having leading edge, AI-Driven analytics, the data ingested is a subset of the data, and does not include the full trace and metrics data needed to uncover indicators of behavior. Often reliant on vendor connectors where not all data is shared across connections.
- These siloed enterprise security data lakes are adding complexity and requiring more time to triage and investigations of security incidents.

EXPONENTIAL DATA COSTS

- Each data lake costs money, SIEMs are prohibitively expensive as the single source of enterprise security data lake especially for the very largest organizations due to security and compliance obligations.
- Other data platform players are charging premiums for locking in data into fewer repositories and still mandate separate data lakes for security, which does not align with the CIO-driven enterprise Data Lake strategy of consolidation for cost optimization and efficiencies around analytics and visibility between Business, IT and Security operations.



6. LEVERAGE YOUR ENTERPRISE DATA LAKE STRATEGY & EXISTING INFRASTRUCTURE

Most of the enterprise CIOs and CTOs are in progress of implementing an Enterprise Data Lake strategy to support the digital transformation journey. For CISOs - it is crucial for teaming up with CIO-driven enterprise Data Lake strategy to expand cybersecurity value to a

broader business value framework. The outcome is to drive data platform consolidation for cost optimization and efficiencies around analytics and visibility between Business, IT, Compliance and Security operations.

C-Level Personas for sponsoring the SDR solution

Identify and describe the personas of the buyers that will most likely be encountered when adopting the SDR solution.

CXO	SPONSOR	EXPECTED OUTCOME
CIO / CTO	for Data Lake Transformation projects	<ul style="list-style-type: none"> ▶ Tasked with many priorities - security is around 10% of the budget. ▶ Data Lake consolidation - centralization is a key priority (e.g. Snowflake's wheelhouse) as a cost reduction exercise & to improve data insights and value. ▶ To drive business innovation, growth, competitive edge etc.
CFO	for Data Cost problems	<ul style="list-style-type: none"> ▶ Assessing the enterprise data and its snowball effects. ▶ More tools and data mean more costs. ▶ To drive cost optimisation, prevent or reduce financial impact due to breach.
CISO	for SOC platform with Next Gen Security Architecture	<ul style="list-style-type: none"> ▶ Drive better security outcomes, in a more cost effective enterprise security architecture with scale. ▶ Timely detection, investigation and response to prevent or recover a breach. ▶ Cost savings can be plowed back into the security budget to fill the skills gap, more proactive security programs, and support more strategic business initiatives.



Why now? - Exorbitant costs, Higher security risks -

Data costs are growing exponentially, security budgets are getting squeezed and businesses are looking for cost efficiencies and returns on their investments, or at least an understanding of the value they are getting from these investments. Every month that goes by, organizations are wasting huge amounts of budget paying for storage that is not fit for purpose for their security operational needs - this is known as the cost of analytics. To do the very best analytics with the very best levels of data is cost prohibitive for most organizations which means security operations and their security posture is negatively impacted, making analysts' jobs much harder, driving up the mean time to detect, respond and recover, putting the organization further at risk.

With Cybereason SDR's Open Architecture means you can ingest structured and unstructured data across all of your existing enterprise IT and Security stacks, without needing to get locked in to restrictive vendor platforms. With our partnership with Snowflake and Observe - you can build your enterprise security data lake and observability into our SDR platform, and apply Cybereason's open APIs for third party integrations, advanced AI-driven analytics for AI assisted operations, and unified portal to gain full visibility and observability for the ease of security operations.

With our partnership with Snowflake and Observe - **you can build your enterprise security data lake and observability into our SDR platform**, and apply Cybereason's open APIs for third party integrations, advanced AI-driven analytics for AI assisted operations, and unified portal to gain full visibility and observability for the ease of security operations.



7. HOW CAN SDR ENHANCE CYBER RESILIENCE WITH AI-DRIVEN ANALYTICS?

Cybereason SDR offers Security Observability and its unique MalOp™ AI Graph Engine to analyze trace and metrics data across your enterprise security data lake in real-time, automating triage and investigation workflows to build the full narrative of the attack including the root cause, attack timeline affected devices, users and other identity and cloud assets. This helps SecOps to lower MTTD, and faster response including guided remediation - to help organizations enhance their cyber resilience against sophisticated threat actors and AI-assisted cyber attacks.

SDR can be beneficial for existing Security Operations Centers (SOCs), or organizations that outsource their security operations to managed security service providers (MSSPs), for responding to and remediating security issues faster and more efficiently with automated actions and proven playbooks embedded as part of managed security services. By adopting SDR approach, organizations can enhance their understanding of their enterprise security landscape, enabling them to:

- **Centralized Visibility and Control:** SDR solutions offer a unified view of enterprise assets, security events and incidents across endpoints, networks, cloud environments, and other data sources. This centralization of security data enables SOC analysts to have comprehensive visibility and observability into the organization's security posture and facilitates efficient monitoring, analysis, and response.
- **Enhance Detection and Response:** SDR solutions provide advanced threat detection capabilities, leveraging multiple security data sources and employing advanced AI analytics and security observability techniques. This enhances the SOC's ability to timely detect and respond to a wide range of threats, including sophisticated and evasive attacks.
- **Identify Vulnerabilities and Security Gaps:** With improved insights across enterprise IT estate and security systems, organizations can proactively assess their security posture and address potential vulnerabilities before they are exploited by malicious actors.
- **Threat Intelligence Integration:** SDR solutions often integrate with threat intelligence feeds, enriching security data with up-to-date information about emerging threats and attack patterns. This integration enhances the SOC's ability to detect and respond to new and evolving threats effectively.
- **Improved Efficiency and Automation:** SDR solutions automate several security operations tasks, such as threat hunting, investigation, and response workflows. This automation helps SOC analysts streamline their workflows, reduce manual effort, and focus on critical tasks, thereby improving overall operational efficiency and effectiveness.
- **Improve Incident Management & Collaboration:** SDR solutions often provide features for collaboration and case management, enabling SOC analysts to work together efficiently. They can share information, collaborate on investigations, and manage incidents within a centralized platform, improving communication and coordination among SOC team members. With Gen AI features embedded in the



same platform, the SOC analysts can ask questions to the AI chatbot for immediate answer and response from knowledge base or incident related information.

- **Ensure Compliance:** By collecting enterprise security data into a single data lake with search and reporting capabilities, organizations can monitor their security posture with their KPIs or compliance metrics to ensure compliance with industry regulations and standards, supporting audits and legal requirements.
- **Scalability and Flexibility:** SDR solutions used by large enterprise SOC teams and managed security service providers (MSSPs) are designed to scale and adapt

to the evolving needs of their clients. They can handle large volumes of security data, support diverse IT environments, and accommodate the requirements of multiple clients simultaneously.

- **24/7 Monitoring and Support:** SDR enables continuous monitoring of the organization's environment, allowing the enterprise SOC teams or managed security service providers (MSSPs) to deliver round-the-clock security monitoring and support. This ensures prompt detection and response to security incidents, regardless of the time zone or operational hours.

By leveraging SDR solutions, **both existing enterprise SOC's and organizations outsourcing security operations to managed security service providers (MSSPs) can benefit from improved threat detection, faster response capabilities, efficiency gains on SecOps, enhanced collaboration, optimized cost and access to advanced AI technologies.** SDR helps strengthen their security posture and enables more effective protection against evolving cyber threats.



8. WHAT ARE THE EFFECTIVE METRICS TO MEASURE SDR DEPLOYMENT?

When measuring the performance of an SDR solution, several Service Level Objective (SLO) metrics can be defined to assess its effectiveness and efficiency. These metrics help evaluate the solution's performance in detecting and responding to security threats, and measuring the total cost of ownership and its security value:

- **Event and Log Ingestion Rate:** This metric measures the SDR solution's ability to ingest, process, and analyze security events and logs from various sources. It assesses the solution's scalability and performance in handling high volumes of data.
- **Detection Accuracy:** This metric assesses the accuracy of the SDR solution's threat detection capabilities. It measures the percentage of true positives (actual threats detected correctly) and false positives (false alarms or misidentifications) generated by the solution.
- **Service Availability:** SDR should be highly reliable and available with built-in redundancy, failover mechanisms, and resilience to ensure continuous operation and minimize downtime.
- **False Negative Rate:** The false negative rate measures the percentage of security incidents or threats that were not detected by the SDR solution. It indicates the solution's ability to avoid missing potential threats or overlooked malicious activities.
- **False Positive Rate:** The false positive rate measures the percentage of alerts or notifications generated by the SDR solution that are determined to be false alarms or non-malicious events. It reflects the solution's ability to reduce unnecessary alerts and prevent alert fatigue for security analysts.
- **Mean Time to Detect (MTTD):** MTTD measures the average time it takes for the SDR solution to detect a security incident from the time it occurred. It reflects the solution's ability to identify threats promptly and initiate the investigation process.
- **Mean Time to Investigate (MTTI):** MTTI metric measures the average time it takes for security analysts to investigate a security incident or alert triggered by the SDR solution. It includes the time required to gather additional information, analyze data, and determine the severity and impact of the incident.
- **Mean Time to Respond/Remediate (MTTR):** MTTR measures the average time it takes for the SDR solution to respond or contain a security incident once it has been detected. It includes the time required for investigation, containment, eradication, and recovery processes.







- **MITRE ATT&CK Integration:** Evaluating SDR with MITRE ATT&CK integration is an effective approach to assess the solution's ability to align with and leverage the MITRE ATT&CK framework for threat detection, analysis, and response. MITRE ATT&CK provides a comprehensive knowledge base of adversary tactics, techniques, and procedures (TTPs) that organizations can use to enhance their cybersecurity defenses.
- **Total Cost of Ownership (TCO):** Evaluate the total cost of ownership associated with the SDR solution, considering factors such as licensing fees, consumption pricing, implementation costs, maintenance and support costs, and any additional costs related to infrastructure or staffing requirements. Assess the business value proposition and ROI of the solution offered in terms of improved security outcomes and operational efficiencies.

It is important to define these SLO metrics in collaboration with the SDR solution vendor and align them with the organization's specific security objectives and operational requirements. **Regular monitoring and analysis of these metrics can help track the performance of the SDR solution, identify areas for improvement, and ensure it meets the desired performance targets.**



Before and After Scenarios for comparison (capability vs business outcome)

BEFORE SCENARIOS		AFTER SCENARIOS
<ul style="list-style-type: none"> ● Siloed Security data <ul style="list-style-type: none"> ● EDR, NDR, XDR, SIEM, NGFW, IAM ● Lack of analytics on cheaper data lakes ● SIEMs lack the detail and volume of data (with static rules or limited detection rules) ● Using old log mgmt tech for observability ● Ingesting a subset of the data due to architectural and cost limitations ● Not fully optimize SIEM/XDR for complex SecOps and Compliance needs ● Alert fatigue SOC team 		<ul style="list-style-type: none"> ● Unified Enterprise Security data lake, aligning with the overall CIO-led data lake initiative ● No limitation on the number of sources of data ingested into single enterprise security data lake ● No limitation on the velocity and volume of data being ingested ● NG SIEM/XDR integrated with security observability ● Advanced, scalable, real-time, AI-Driven analytics on enterprise data lake ● Efficient and productive SOC
		
NEGATIVE CONSEQUENCES		POSITIVE BUSINESS OUTCOMES
<ul style="list-style-type: none"> ● Manual efforts increased MTTD-MTTI-MTTR <ul style="list-style-type: none"> ● High MTTD / Missed detections ● High MTTI / Dwell time to triage ● High MTTR / Dwell time to remediate ● Huge spending in data costs <ul style="list-style-type: none"> ● Data duplication (data not synced or cleaned) ● Compromise on data integrity (visibility, quality - reduced ability to detect threats, longer triage and investigations, manual efforts to retrieve missing data, incomplete remediation) ● Overspend of budgets on data ingestion and retention, taking budget away from strategic projects ● Spending too much money on data analytics (cost of analytics) ● Alert Overload - Staff not focussing on business innovation (too busy to support day-to-day security operations) ● Staff turnover (overtime), increased sick leave, employee welfare (work-life-balance) ● Higher risk of suffering material impact (reputation, financial, business continuity) from a cyber breach 		<ul style="list-style-type: none"> ● Reduced MTTD-MTTI-MTTR <ul style="list-style-type: none"> ● Detect more and more quickly ● Reduced investigation time due to cross-correlation ● Automated triage and investigation from MalOp Detection engine ● Guided remediation ● Huge reduction in data costs <ul style="list-style-type: none"> ● De-dupe, reduction on duplicated data stores ● Reduced cost of ingestion ● Reduced cost of analytics ● Reduced data retention costs ● Future-ready - all data is available for over a year for historical hunting (replay in time-travel) or future business and security analytics use cases ● Visibility & observability across broader IT & Security estate ● AI assisted operations for better efficiency gains ● More FTE resources to aligned to strategic initiatives (more innovation) ● Less SOC analyst churn, better employee wellbeing ● Enhance organization resilience to cyber threats