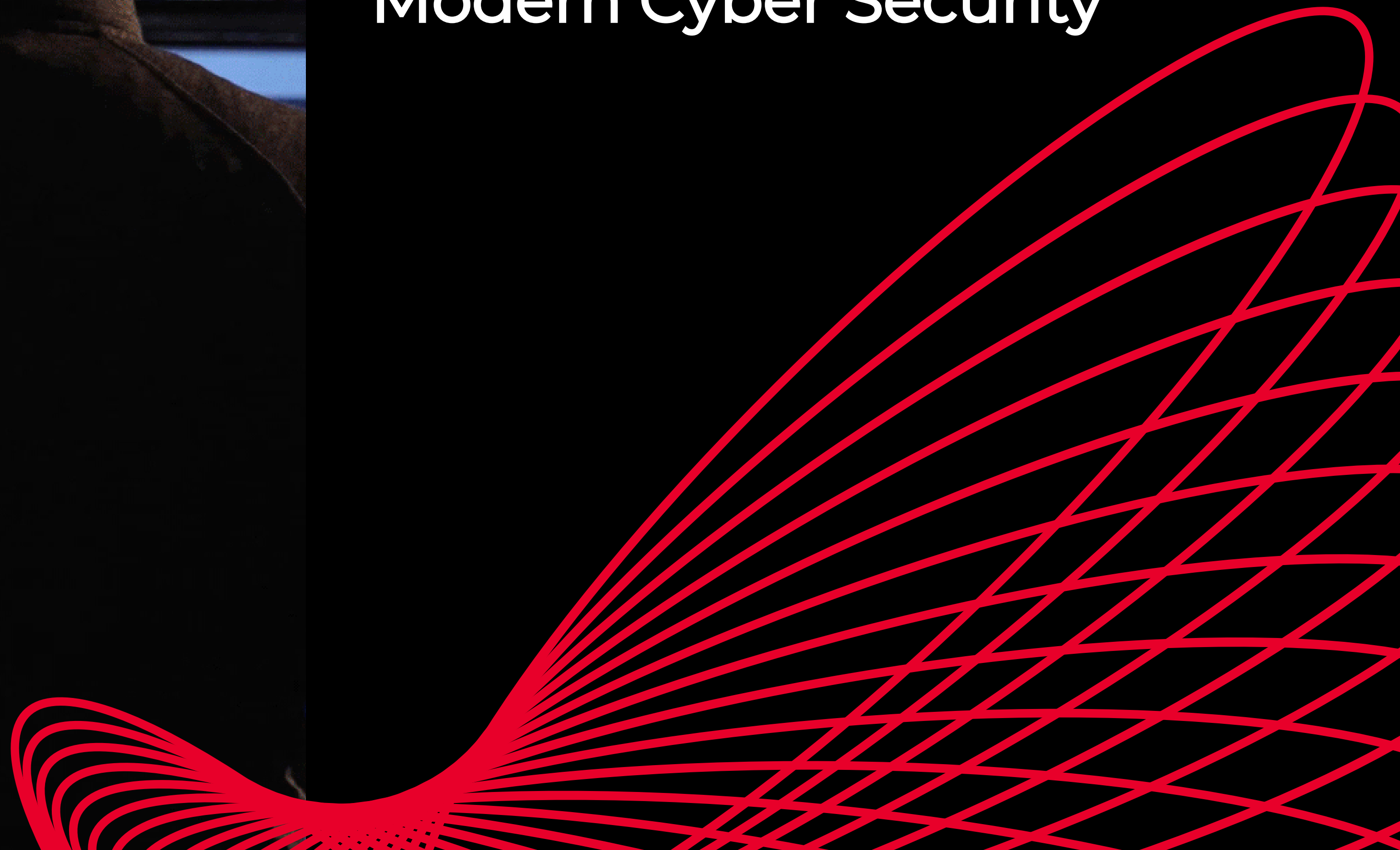




SIEM Demystified: An Essential Component of Modern Cyber Security



CONTENTS

What is SIEM?	3
SIEM Core Functions	4
Why Do You Need SIEM?	5
SIEM Options	6
How to Choose the Right Managed SIEM Provider	7
How Does Red Helix Provide SIEM Services?	8



What is SIEM?

Organisations continually face an increasing number of sophisticated cyber threats. To effectively detect, analyse, and respond to these threats, organisations have turned to Security Information & Event Management (SIEM) solutions. SIEM systems play a pivotal role in enhancing an organisation's security posture by providing comprehensive visibility and facilitating proactive threat management.

SIEM is a comprehensive security solution that aggregates data from various sources within an organisation's IT infrastructure, including security tools, network devices, applications, and operating systems. By collecting, storing, and analysing logs and events, SIEM systems enable real-time monitoring and detection of suspicious activities. They combine Security Information Management (SIM) and Security Event Management (SEM) into a unified platform, streamlining the analysis of security events and facilitating efficient threat detection and response.



SIEM Core Functions

SIEM perform critical functions to enhance an organisation's security posture. They collect and centralise logs and event data from diverse sources across an organisation's infrastructure, providing a comprehensive view of security-related information. By examining aggregated data, SIEM systems identify patterns and correlations that may indicate security incidents, enabling timely detection and response.

Advanced Threat Detection & Analytics

Through continuous surveillance of the IT environment, SIEM can detect and alert on potential threats as they occur, ensuring real-time threat monitoring. Leveraging sophisticated machine learning algorithms and artificial intelligence means that anomalies and suspicious behaviours are quickly detected across diverse environments. This includes identifying potential insider threats, compromised accounts, and unusual patterns of activity that could indicate malicious intent.

Log Management & Data Aggregation

The solution offers comprehensive log management capabilities, collecting and correlating data from a wide range of sources, including on-premises infrastructure, cloud environments (AWS, Azure, for example), endpoints, and security solutions. This holistic approach ensures that no critical log data is overlooked, enabling effective incident detection and analysis.

Incident Detection, Investigation, and Response

SIEM can provide automation capabilities that streamline incident response workflows. Security teams can employ customisable playbooks that guide them through response processes, ensuring efficient containment and remediation of incidents. Additionally, advanced forensic investigation tools allow for detailed analysis of security events, facilitating root cause identification and post-incident reviews. As a result, your organisation can save time and money which in the event of an incident, would need to be spent on data collection.

Reporting & Compliance

The SIEM platform features customisable dashboards and automated reporting capabilities which aid organisations in adhering to industry standards and regulations. The Digital Operational Resilience Act (DORA), applicable to financial entities in the EU, requires businesses to ensure their digital operational resilience. Organisations can adhere to this via incident reporting and log management which extends to a business' customers and vendors. This ensures that threats are monitored across internal and external infrastructures, maintaining a robust supply chain. The NIS2 Cybersecurity Framework provides guidelines for improving cyber security risk management. SIEM supports this by centralising log collection to facilitate real-time analysis of security events. The tool detects unauthorised access attempts and maintains central logs for forensic analysis and regulatory reports.

Real-time visibility into compliance status and automated reporting templates also significantly reduce the administrative burden associated with regulatory requirements.

Integration of Cloud Tooling

SIEM ensures proactive threat detection and enhanced compliance during your cloud migration.

Automation and ML/AI Functionality

Automatic triaging, along with the "Log Reduce" and "Log Compare" functionalities both enhance the efficiency of locating critical messages within security logs, and streamline the identification of risks and threats. Via advanced machine learning and AI technology, organisations can also use AI-assisted log analytics.



Why Do You Need SIEM?

Implementing a SIEM platform offers critical benefits that enhance an organisation's security. By correlating data from various sources, SIEM systems can identify suspicious activities that individual security tools might miss, providing a holistic view of potential threats.

SIEM enables security teams to proactively search for threats, allowing for early detection and mitigation before they escalate into significant incidents. By collecting and aggregating logs from various devices and applications, SIEM simplifies security data management and reduces the complexity associated with handling disparate data sources.

Automation of tasks such as log collection, analysis, and alerting free up security personnel to focus on higher-level strategic activities, enhancing overall operational and cost efficiency. Additionally, migrating to a cloud-native SIEM, reduces the reliance on costly on-premises infrastructure achieving significant cost savings. The scalability of Sumo Logic's SIEM allows organisations to pay only for the resources used, which optimises operational expenditure while simultaneously ensuring robust security coverage.

SIEM assists in generating the necessary reports for compliance audits, ensuring that organisations meet industry standards and regulatory requirements. It also facilitates the secure storage of audit logs for mandated retention periods, ensuring data integrity and availability for compliance purposes. By providing comprehensive security insights and automating routine processes, SIEM can optimise security operations, potentially leading to cost savings through more efficient resource utilisation.

Benefits of SIEM

SIEM	Traditional Security Services (Log Management, IDS/IPS)
Aggregates data from various security tools, network devices, applications, and operating systems	Focuses on specific data sources like network traffic (IDS/IPS) or system logs (Log Management)
Correlates events from various sources to identify security incidents	Analyses individual data sources for suspicious activity
Generates prioritised alerts based on security rules and threat intelligence	Generates alerts based on pre-defined rules
Provides comprehensive reports on security incidents, trends, and user activity	Offers limited reporting capabilities specific to the data source
Manages large volumes of data from diverse sources	Limited customisation options

SIEM Options

Next-gen SIEM

Traditional SIEM has evolved into next-generation systems that incorporate advanced technologies to address modern cyber security challenges. These enhancements include the integration of Artificial Intelligence (AI) and Machine Learning (ML), which analyse vast amounts of data, enabling the detection of unknown threats and reducing false positives.

Incorporation of up-to-date threat intelligence feeds allows for the identification of emerging threats and enhances the system's ability to respond to new attack vectors. Modern SIEM platforms are designed to scale with the organisation's growth and adapt to changing IT environments, including cloud and hybrid infrastructures.

SIEM and traditional security services such as Log Management and Intrusion Detection/Prevention Systems (IDP/IPS) are two approaches used to monitor security events. While both solutions aim to enhance security, they differ in their scope, functionality, and capabilities. SIEM provides a more advanced and centralised approach to security monitoring by integrating multiple data sources, correlating events, and offering in-depth reporting capabilities. Traditional security solutions, while effective for specific use cases, lack the breadth and analytical power of SIEM.

Cloud-based SIEM

Using the cloud for SIEM offers numerous advantages over on-premise solutions. One of the key benefits is scalability and flexibility, as cloud-based SIEM can grow with business needs, managing increasing data volumes without requiring costly hardware upgrades. Additionally, cloud SIEM ensures faster deployment and updates, eliminating the need for manual maintenance since providers automatically apply the latest security patches and features.

A cloud based SIEM is also more cost effective as it removes the need for significant upfront investments in infrastructure. Remote accessibility and centralised visibility allow security teams to monitor, analyse, and respond to threats from anywhere, making it particularly beneficial for remote working environments and global operations.

Managed SIEM for SMEs

For SMEs, investing in a managed SIEM is often the most effective way to achieve robust cyber security without the burden of building and maintaining an in-house Security Operations Centre (SOC).

Cyber threats are growing in both volume and sophistication, and SMEs are increasingly becoming targeted. A managed SIEM provides a cost-effective, scalable, and expert-driven solution that delivers enterprise-grade protection without the need for an internal security team.

By outsourcing SIEM to a managed service provider, SMEs gain complete visibility across their networks, ensuring real-time threat detection, remediation, and compliance management.

The unified log management system streamlines security processes, allowing businesses to focus on growth rather than security operations. Unlike traditional SIEM platforms that require significant investment in hardware, software, and personnel, a managed SIEM delivers continuous monitoring, proactive threat intelligence, and automated incident response at a fraction of the cost.

SMEs cannot afford to rely on reactive security. A managed SIEM empowers your organisation with proactive, 24/7 protection, ensuring business continuity, regulatory compliance, whilst maintaining peace of mind.

How to Choose the Right Managed SIEM Provider

1. Define your Needs

You should clearly set out your security objectives, needs, and constraints. Determine specific features, functionalities, and level of service you need from your Managed SIEM provider.

2. Conduct Market Research

Do your due diligence and research reputable Managed SIEM providers. Search out customer reviews and case studies to compare each provider's expertise and commitment to customers.

3. Assess Capabilities

Evaluate security expertise and qualifications of the provider's team. Look for certified security professionals, experienced threat hunters, and incident responders. Review compliance support to ensure the Managed SIEM provider is competent in supporting relevant regulatory compliance requirements such as GDPR, HIPAA, PCI DSS, etc.

4. Consider Deployment Options

Evaluate the different deployment options such as on-prem, cloud-based, or hybrid. The model you choose should align with your organisation's infrastructure, policies, and financial constraints.

5. Compare Financials

Request pricing from multiple Managed SIEM providers and compare them based on subscription fees, data volume, customisation costs, etc. Make sure you are aware of any future costs, should your organisation grow.

6. Assess Service Level Agreements (SLAs)

Evaluate each provider's level of support, incident escalation procedures, and analyst availability. You should review the provider's SLAs to ensure they are applicable for your organisation's performance requirements.






7. Request References

Each Managed SIEM provider should provide references and case studies to validate their past records and customer satisfaction.

8. Consider Long-term Partnerships

Deliberate the opportunity to build a long-term partnership and collaboration between the Managed SIEM provider and your organisation. This means they will address your evolving security and business needs.

Managed SIEM Provider Checklist

Advanced Threat Detection & Analytics Your provider should offer real-time monitoring, AI-driven threat intelligence, and behavioural analytics to detect and respond to cyber threats efficiently.	
Compliance & Regulatory Support Industry-wide regulation is becoming stricter. If your business needs to comply with GDPR, NIS2, ISO 27001, or PCI DSS, choose a provider with expertise in compliance reporting, log retention, and audit support.	
Seamless Integration with Your IT Infrastructure Your Managed SIEM should integrate smoothly with cloud environments, firewalls, EDR (Endpoint Detection & Response), NDR (Network Detection & Response), and identity management tools for a unified security approach.	
24/7 Monitoring & Incident Response Cyber threats do not follow business hours. Look for a provider offering round-the-clock monitoring, practical threat hunting, and a well-defined incident response plan to minimise damage from attacks.	
Scalability & Cost-Effectiveness A good provider should offer a scalable solution that grows with your business, ensuring you only pay for the security coverage you need.	
Transparent Reporting & Actionable Insights Access to detailed security reports, dashboards, and alerts helps you understand threats and make data-driven security decisions.	
Expertise & Customer Support Look for a provider with a proven history, certified security analysts, and responsive customer support to guide you through security challenges.	

How Does Red Helix Provide SIEM Services?

Red Helix offers a next-generation SIEM service that integrates cutting-edge technology with real-time threat intelligence to detect threats before attacks occur. To ensure optimal performance, scalability, and security insights, Red Helix has partnered with Sumo Logic, a leader in cloud-native SIEM.

This collaboration enables Red Helix to provide a flexible, highly scalable SIEM platform featuring advanced analytics, machine learning-driven anomaly detection, and rapid threat response. Sumo Logic's real-time data ingestion and security analytics enhance threat detection accuracy, equipping security teams with the insights needed to act swiftly in a dynamic threat landscape.

By leveraging Sumo Logic's expertise in security intelligence and continuous compliance monitoring, Red Helix delivers a fully managed SIEM tailored to businesses of all sizes. This integration provides powerful automation, correlation, and investigative tools, allowing security teams to focus on proactive threat mitigation rather than manual log analysis.

Implementation and Migration Plan

The Red Helix service delivery plan encompasses a comprehensive assessment of your current environment, the design of a robust migration strategy, and the execution of a phased migration process.

As part of the migration, knowledge transfer will take place to ensure security teams are comfortable with the environment. The platform also provides a comprehensive online training facility that is available for organisations to gain a deeper understanding of the platform's features, capabilities, and best practices, should they wish to.

We typically operate a four-phase approach to migrate to Sumo Logic Cloud SIEM.

Phase 1: Platform Setup and Data Collection.

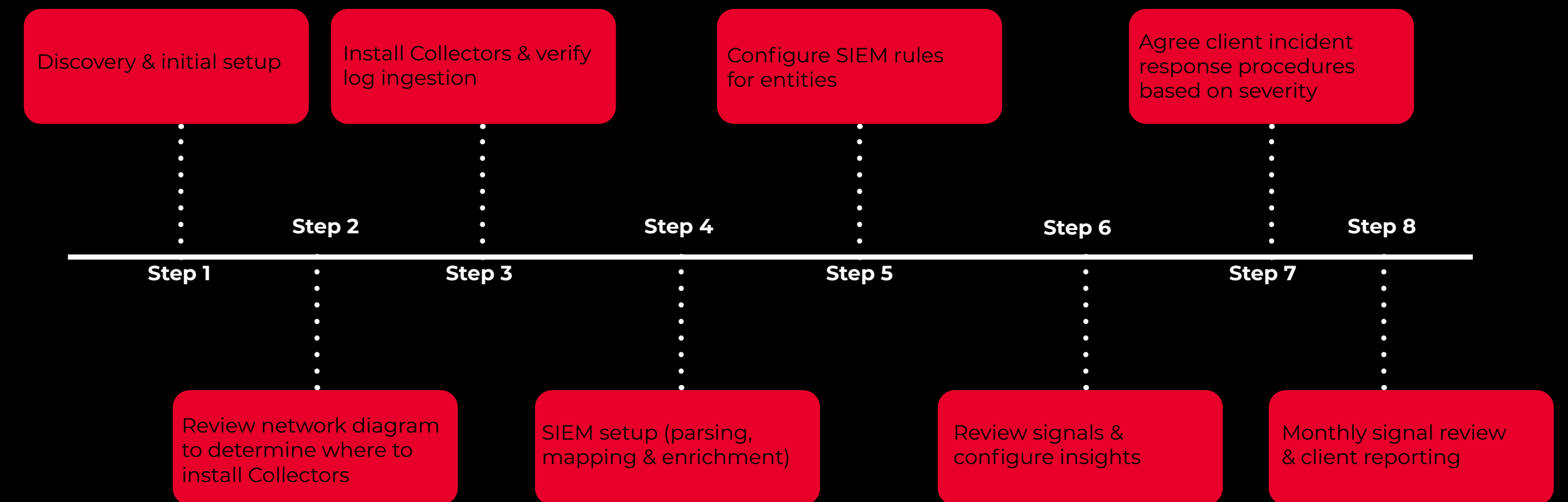
This focuses on the extraction and transfer of historical security logs and other event data from legacy SIEM to Sumo Logic.

Phase 2: Configuration. Applicable security rules, alerts, and dashboards are transferred from legacy SIEM to Sumo Logic.

Phase 3: Integration. Existing security tools (e.g. EDR, IDS/IPS etc.) are integrated into Sumo Logic, to ensure seamless operations and enhance the organisation's security posture.

Phase 4: Testing. We conduct thorough testing to validate a successful migration to Sumo Logic.

Our Onboarding Process



Additional capabilities

At Red Helix, we integrate our SIEM service with [Endpoint Detection & Response \(EDR\)](#), and [Network Detection & Response \(NDR\)](#) capabilities to accumulatively offer [Managed Detection & Response \(MDR\)](#). This comprehensive offering provides expertise from a team of analysts, 24x7x365, real-time threat detection and remediation, as well as a flexible and scalable solution which is tailored towards your needs.

[Contact us today](#) to find out how this can benefit you.

+44 (0)1296 397711

info@redhelix.co.uk

Phoenix House
Smeaton Close
Aylesbury
Buckinghamshire
HP19 8UW



redhelix.com