snare
A PROPHECY SOLUTION

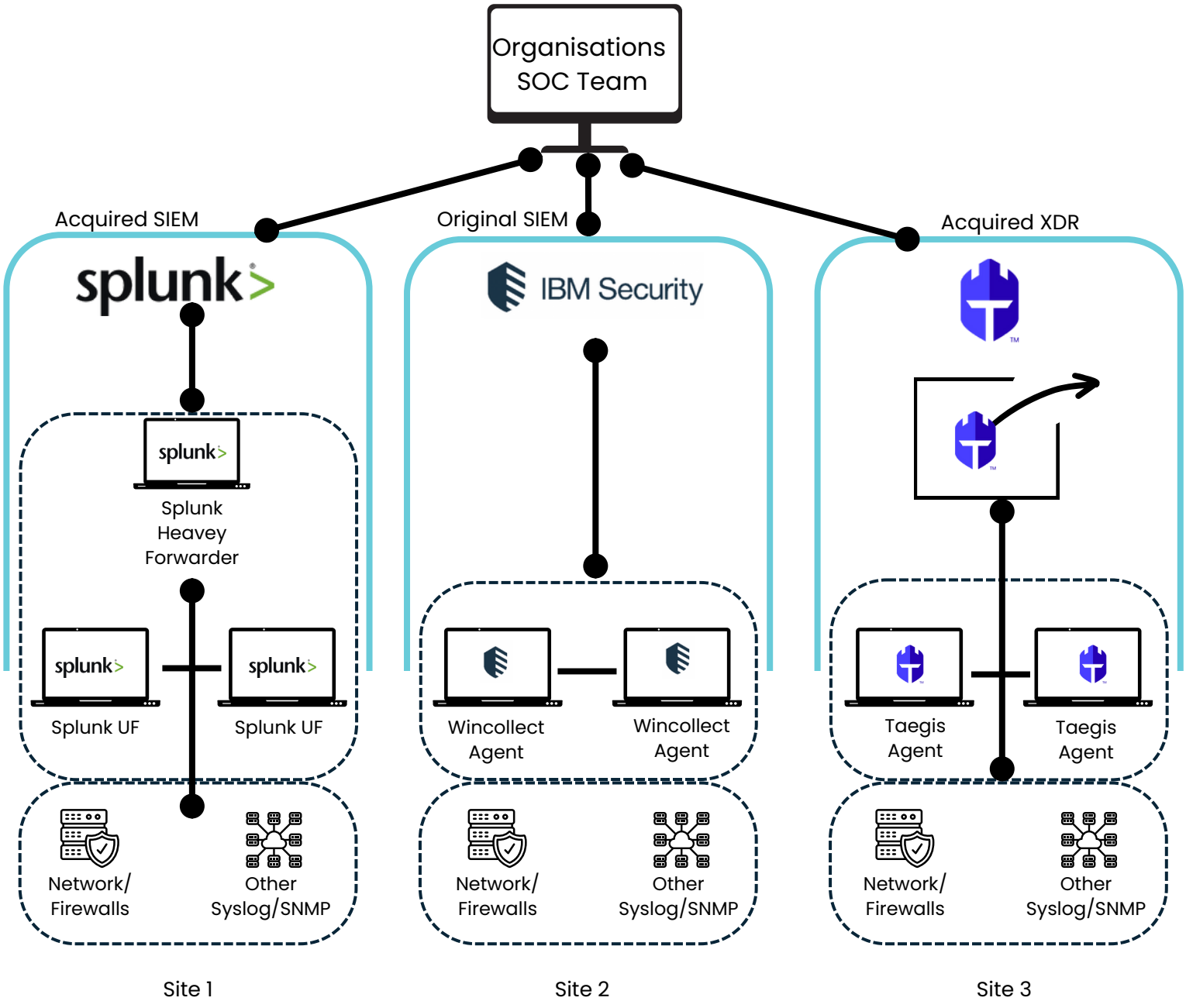
Managing and Transitioning Disparate Cyber Architectures

Managing and Transitioning Disparate Cyber Architectures

Mergers and acquisitions often lead to a complex mix of inherited technologies and solutions that lack integration, creating a fragmented cyber architecture. Organizations may end up managing multiple security information and event management (SIEM) platforms, which may eventually merge into one or remain segmented for legal or operational reasons.

Data from each platform is stored in different formats, under conflicting policies, and with inconsistent compliance and audit rules. Maintaining these architectures is costly and challenging, especially given the global shortage of cybersecurity skills.

These setups generate excessive log data, including duplicate and unnecessary logs, creating large, unmanageable data stores spread across multiple platforms. The challenge lies in consolidating these data silos into a single platform with a SIEM-agnostic log collection and data management pipeline to efficiently route data to the desired destinations.



What a Solution Could Look Like

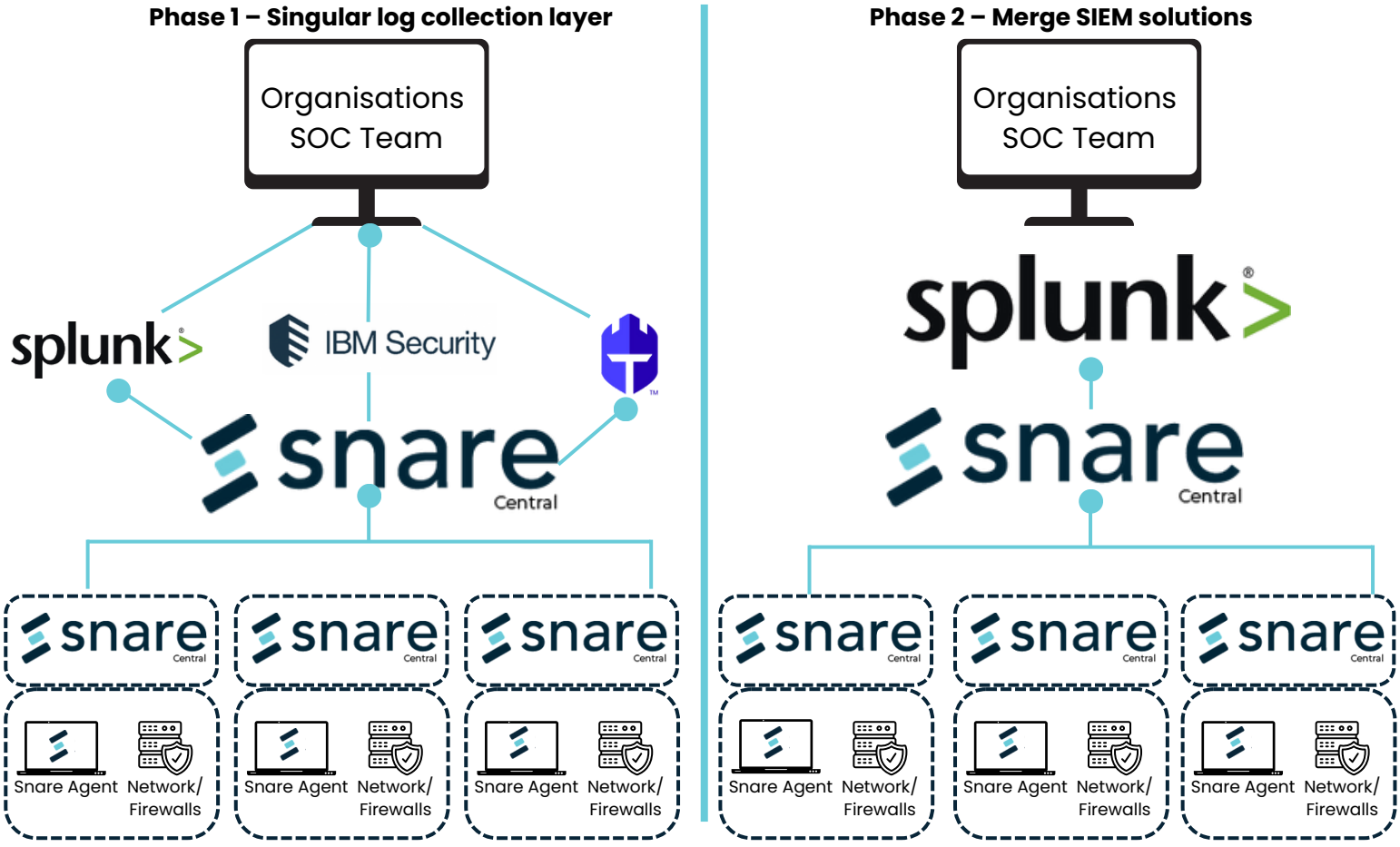
The solution must address both historical and current data sources. Historical data stored across multiple SIEMs should be merged into a single SIEM platform where possible, while current data sources must be routed to the appropriate destination, eventually consolidating into one.

Many SIEMs offer their own collection methods, including agents, agentless options, or data streaming. Introducing a SIEM-agnostic Security Data Engine (SDE) during the transition enables data ingestion and retention, supporting a phased migration of historical data. This process can be structured by event log type, compliance, or destination. Alternatively, historical data can be archived in cold storage with the capability to replay data to the final SIEM platform when needed.

It is recommended to separate the data collection approach from the SIEM platform to maintain SIEM agnosticism, preventing vendor lock-in. A consistent data pipeline management tool ensures data is collected, stored, and retained in a unified manner, either in the final SIEM platform or more cost-effectively in a Security Data Engine.

Initial discussion and technical evaluation → Proof of concept (POC) and technical walkthrough → Deployment

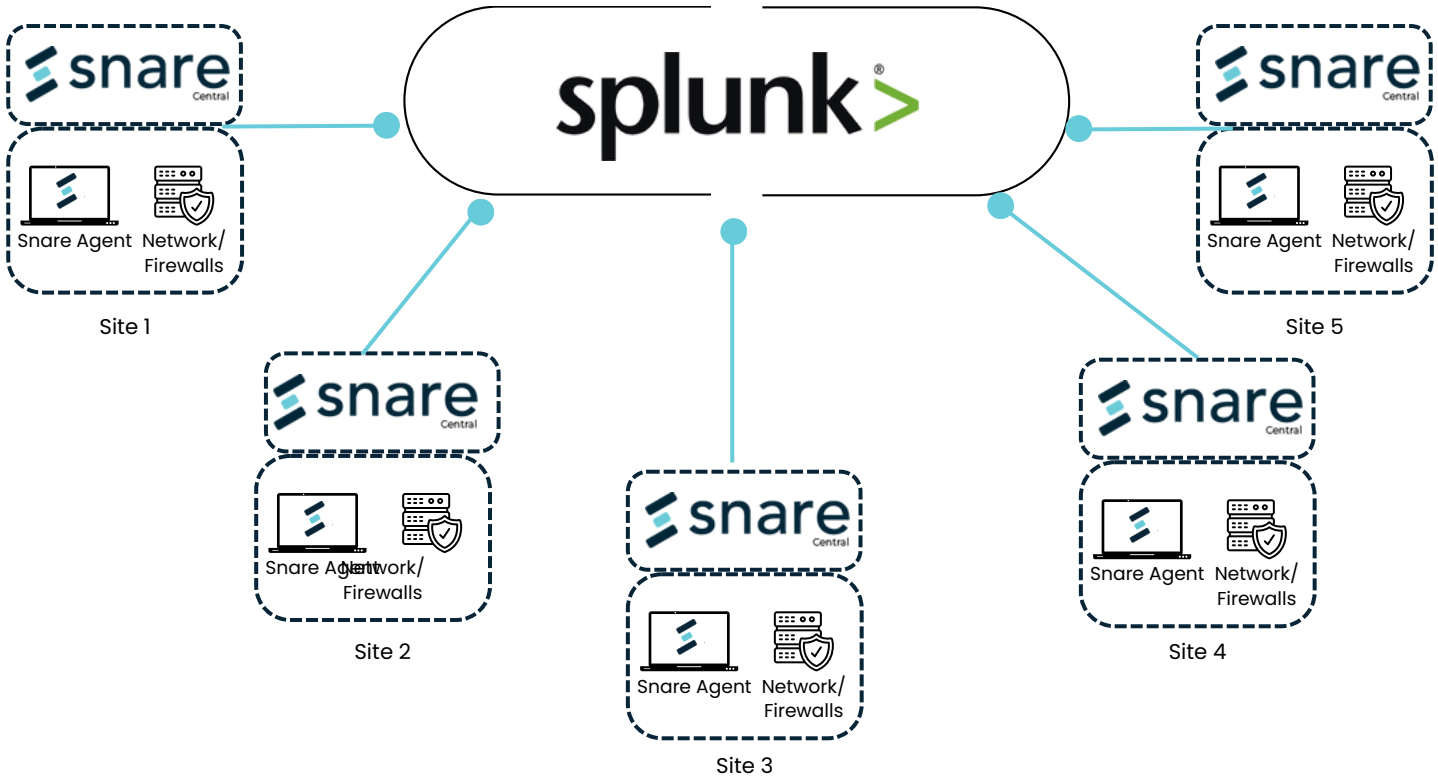
Managing and Transitioning Disparate Cyber Architectures



Vendor Agnostic SIEM Solutions

The performance of a managed, transitional cyber architecture supports:

- Managing, transitioning, and phasing historical data from multiple SIEMs to a target SIEM platform.
- Deploying a consistent, SIEM-agnostic data management platform.
- Using an SDE to retain historical and current data without incurring ingestion, storage, or retention costs.
- Replaying data into the target SIEM as needed.
- Segmenting operational or entity data to meet legal and audit requirements.
- Ensuring high availability and fault tolerance through the SDE.
- Establishing a distributed architecture with SDE assigned to operational or divisional responsibilities.
- Avoiding vendor lock-in for data collection and SIEM platforms.



Toll Free US: 1(800) 834 1060
Asia/Pacific: +61 8 8213 1200
UK/Europe: +44 (800) 368 7423

AMERsales@prophecyinternational.com
APACsales@prophecyinternational.com
EMEAsales@prophecyinternational.com