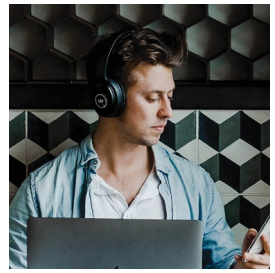
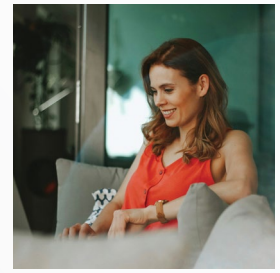
ADARMA
TOGETHER WE'VE GOT THIS

HOW TO DESIGN A FUTURE-READY SECURITY OPERATIONS CENTRE (SOC)

STAYING ADAPTABLE AND AGILE IN THE FACE OF CHANGE

Table of Contents





Introduction

This paper lays out the blueprint for a Future-Ready SOC architecture that solves new and old challenges and lays the groundwork for adaptation to future change.

We will walk through the factors pushing current security operations approaches to their limit and discuss the implications.

Finally, we'll outline an approach to ensure that whatever the future throws at you, your security operations capability is ready.

> Security operations' objective is to create proactive risk understanding to reduce threat exposure and improve detection of and response to cyber events that negatively affect the organisation.
>
> **Gartner**

Security Operations: The Journey so Far

Success in security operations demands adaptation and resilience in the face of incidents and events. This approach must also extend to effectively managing dynamic changes in the organisation, technology landscape and market.

Think back ten years: the Security Operations Centre (SOC) collected, stored, and processed alerts in a single location. Since then, there's been a steady decentralisation of the capabilities and data needed to understand and contain internal and external threats.

Changes in how organisations buy software, hardware and IT services have caused individual business units and functions to invest in, generate, and take ownership of larger volumes of data and IT services.

Externally, hyperscale cloud providers have developed security capabilities that far outpace most end-user SOCs. These in-house SOCs have had to surrender oversight and control of applications and data to external providers and service delivery teams within the business.

Maintaining the current manual process and resource-heavy approach – along with monitoring multiple vendor technologies and environments – has resulted in observability gaps, costly defence, and difficulty in hiring and retaining skilled personnel.

The next generation of SOC, which we call the "Future-Ready SOC", should be the conductor of an orchestra whose instruments and players include technology vendors, service providers, and security operations teams. It should serve as the organisation's champion and quality arbiter, especially in an environment where many core capabilities and essential data are spread across cloud providers and scattered among different business units and functions. ▶▶▶

Toward a Future-Ready SOC

The Future-Ready SOC must be flexible and elastic. It must adapt promptly to changes in the direction of the company it protects, and the emergence of new external threats.

The Future-Ready SOC must:

Handle large data volumes without high ingest, processing, and storage costs.

Monitor and protect a wider variety of environments than ever before.

Embrace a federated detection and response model.

Enable infrastructure owners to subscribe to security services, encouraging security accountability outside a centralised security operations team.

Adopt automation, coupled with Artificial Intelligence (AI) and machine-augmented decision-making, reducing the dependency on humans for repetitive or mundane tasks.

Take innovative and proactive approaches to threat hunting that leverage the latest technologies and techniques.

The Secret SOC Sauce

The key to success? Acquire the data your SOC needs affordably while gaining holistic observability across different environments.

It's time to question the traditional mass data collection approach and move to a more federated strategy, bringing detection closer to the data sources and reducing the burden of centralised search across overpopulated data stores. This approach should also allow for rapid, on-demand data collection without prior centralisation and storing extraneous data.

To realise these changes, the Future-Ready SOC will employ open and extensible architectures that allow internally developed tailored capabilities to sit alongside leading vendor technologies without historical issues with lock-in.

This approach will provide an environment for SOC analysts, threat hunters, and engineers to innovate and apply the latest research and innovation alongside established approaches to cyber defence. The Future-Ready SOC will enable collaboration and co-creation across the business and trusted partners while supporting other business initiatives such as cloud migration, legacy infrastructure re-platforming, and digital transformation.

Balancing Act

Navigating Competing Forces in Modern SOC Architecture

Challenges with Traditional SOC Design

Navigating Competing Forces in Modern SOC Architecture

There is a crucial tension between pushing for a cloud-native SOC in a digitally-native enterprise, and catering to and using the long tail of legacy technology, often the soul of an established organisation. Existing security tools and capabilities must protect on-premise and custom legacy infrastructure. There must be parity in the protection afforded to cloud-based services and legacy on-prem infrastructure.

Cloud-native applications and services, cloud migration and multi-cloud environments have changed the definition of an effective SOC over the last decade. Aside from the fundamental issues of assets and data no longer being on-premise, cloud services add multiple vectors of attack, as well as control and insight.

Cloud providers bring their controls, restrictions, conflicts, and incompatibilities, which can mean losing some security control and visibility to the provider. This can result in duplication of tools and dashboards and an array of incompatibilities and siloed insights between providers. However, hyper-scale cloud providers have security practices and capabilities that are far more significant than most customers could achieve.

Almost all large enterprises have in-house applications that are so intertwined with the operational nervous system of their organisation that they cannot be removed. These systems, present in banks, aviation companies, supermarkets and utilities, are often decades old, thoroughly embedded and resistant to transformation projects. Security teams must ensure these systems – often business-critical – are protected to the same level as modern digital-native applications and services.

There's a clear case for an open and extensible security model built for the Future-Ready SOC that can accommodate the capabilities, complexities and shortfalls of cloud service providers – and service-driven infrastructure.

“Almost all large enterprises have in-house applications that are so intertwined with the operational nervous system of their organisation that they cannot be removed... Security teams must ensure these systems — often business-critical — are protected to the same level as modern digital-native applications and services.

Challenges with Traditional SOC Design

There are a range of other challenges a Future-Ready SOC aims to overcome:

Vendor Lock-In

Vendor lock-in forces a linear roadmap due to the complexity of the problems and the breadth of solutions available. Relying on a single technology vendor and their capability roadmap can make it challenging to maintain an effective monitoring aperture relevant to the business you protect.

In addition, industry consolidation has seen monolithic vendors swallow niche players, creating a risk of poor integration and unclear and disrupted product and service roadmaps. This can be inflexible, and difficult to exit, blocking change and transformation in the security function and wider business-driven programmes.

Tool Sprawl

This is the flip side of vendor consolidation: The sheer diversity of security products, tools and services available, combined with the decentralisation of controls, visibility and data sets, has made it challenging to build a clear picture of events and incidents and take effective and prompt remediations.

Fragmented environments and unclear perimeters make data acquisition and effective monitoring even more of a challenge, and this has a further knock-on effect on the processing of alerts, evaluation of log files and the formulation of timely and appropriate response activities.

Devolution to Cloud

Getting a single, central view is challenging, with capabilities and controls split between multiple cloud providers and the organisation's own SOC. Siloed control placement and ownership stifles management and orchestration. This makes a holistic response harder to achieve.

Added to this is the growth in micro-service architecture, which has increased the complexity of security monitoring. In this scenario, security operations must undertake 'transaction stitching' to gain observability across systems composed of multiple disparate components.

Definition: Transaction stitching

The practice of combining data threads from disparate components to show the complete end-to-end transaction.

Data Explosion

Achieving parity in observability and protection across multiple environments will necessitate broader and deeper instrumentation of infrastructure, systems and applications, leading to high data collection, transfer, storage and processing volumes. ▶▶▶

Analyst Fatigue

As more data is collected, more alerts are generated. Although automation has reduced the burden on SOC analysts, there is still a constant need for prompt and precise data-driven decision-making.

Ubiquitous Encryption

There's an unintended consequence with blanket encryption: it's challenging to work out what's going on without visibility of the context. While network traffic can still play a part, it tends to be limited to metadata analysis, i.e. monitoring the signal rather than the data. The focus is now shifting back to endpoints and services, and while Endpoint Detection and Response and Endpoint Protection Platforms are effective, these are only a component of an effective cyber defence architecture.

Limitations of Automation and AI

At this point, confidence and trust in automation and near-real-time reactive interventions are limited and must be proven through measured adoption with analyst oversight of recommended actions. Early attempts at automation have sometimes created issues where more tickets, rather than fewer, are raised.

Sub-second response times with automated actions can also alert attackers early, allowing them to change tactics or cause damage when a more methodical and comprehensive detection and response process would allow complete ejection of attackers from an estate.

AI applied to cyber defence, including Machine Learning (ML) techniques for anomalous behaviour detection and augmentation of security operations processes is in its relative infancy. Organisations implementing a Future-Ready SOC approach will need to consider a purposeful adoption of AI/ML aligned to strategic outcomes and broader utilisation within their business, rather than attempting to apply generic models to their specific problems.

Six essential questions that can help prepare your organisation for a Future-Ready SOC:

01

Do you clearly understand emerging threats and whether your organisation is protected against them?

02

Can you quickly adapt your threat coverage as the business evolves?

03

Do you have in-house skills to manage and optimise security investments?

04

With the exponential increase in vulnerabilities, can you validate and prioritise these against risk?

05

Can you view all exposures, including cloud or on-premises, vulnerabilities, misconfigurations, and risky user behaviours in a single dashboard?

06

Can you demonstrate the value of your security operations to the business leadership?

The Future-Ready SOC Template

Let's focus on creating a Future-Ready SOC that can adapt to change at pace, not just fix the current set of problems. It should be able to work for various business, cyber, and technology stakeholders and any organisation as a template.

The Future-Ready SOC should also consider your organisation's investment and business transformation programs, making it specific to the business you're protecting. The three fundamentals of cyber – People, Process, and Technology – also add another modifier to how your SOC is positioned for the future.

This section will discuss the concept and components of a Future-Ready SOC and then delve deeper into the architectural adjustments needed to create your Future-Ready SOC.

What is a Future-Ready SOC?

The Future-Ready SOC is a concept that recognises the limitations of a single solution to address the diverse and complex threat landscape of modern businesses. This includes legacy systems, cloud-based infrastructure (Infrastructure-as-a-Service / Platform-as-a-Service), software applications and services (Software as a Service), and Operational Technology. Achieving comprehensive protection across all these areas requires substantial investment and compromise in terms of cost vs holistic coverage.

Open and standards-driven approaches to threat definition, control and capability integration, data acquisition, and data modelling are necessary to address these challenges. By adopting an integrated approach to SOC architecture and platform, businesses can benefit from a more effective and efficient security solution.

How Does the Future-Ready SOC Work?

The system works by leveraging open and extensible architectures that allow internally developed capabilities to sit alongside leading vendor technologies without any historical issues with lock-in. This enables collaboration and co-creation across the business and trusted partners.

Resilient SOCs of the future embrace the concept of a federated detection and response model that enhances inherent and embedded security controls within protected ecosystems and enables orchestrated autonomy to detect, act, and report within each environment, leveraging optimised available features.

Ideally, the new SOC model continually assesses controls and weaknesses to ensure adequate protection from threats, with resources focused on priority assets and business services. It ensures that indiscriminate and routine threats are addressed without analyst intervention, reporting on observed threats and actions taken to eliminate or reduce the risk of compromise.

A SOC that follows our blueprint for success also provides continuous summarised reporting of the organisation's security posture, breach likelihood of critical assets, and trend analysis of defined metrics and key focus areas, such as vulnerabilities, modelled threats, regulation, and compliance, available in real-time to a depth of detail required by each business persona.

Phased adoption of automation, coupled with innovative (AI/ML assisted) techniques for decision-making and intervention recommendations, will reduce the dependency on an increasingly transient skill pool at junior levels of the SOC, facilitating an elevation in SOC team focus on exciting and engaging tasks.

The system provides an environment for SOC analysts, threat hunters, and engineers to innovate and apply the latest research and innovation alongside established approaches to cyber defence. ▶▶▶

What are the Outcomes of the Future-Ready SOC Model?

The future SOC quickly identifies and addresses potential threats, allowing for proactive defensive measures to be implemented before any compromise can occur.

The SOC will continuously assess and improve controls and weaknesses, ensuring adequate protection against identified and predicted threats. Resources will be focused on priority assets and business services. This will enable organisations to invest at the correct scale in their SOC teams, encourage the adoption of experimental and innovative approaches to threat detection and response, and leverage the latest technology and research.

A Future-Ready SOC will ultimately facilitate other transformation initiatives that allow the business to grow and thrive.

Checklist: The Future-Ready SOC

A proactive approach is critical for a Future-Ready SOC. The following capabilities will be necessary for your security operations to achieve this.

Adopt an open architecture that allows the SOC to take advantage of new technologies and avoid vendor lock-in with one monolithic provider.

Understand which data is valuable and effectively manage the costs of ingesting, processing, and storing it.

Deploy federated detection, response, and threat hunting to enable the fast recovery of information from distributed enterprise environments.

Employ continuous posture assessment, which will allow you to understand how likely it is that specific critical assets will be breached. It will also help you take a proactive risk management approach to protect them.

Purposefully adopt AI in the SOC and experiment to see where value can be derived.

The Architecture Playbook

Adopting an Open Architecture

Data Acquisition and Storage

Federation Detection and Response

Continuous Posture Assessment

Purposeful Adoption of ML and AI

Adopting an Open Architecture

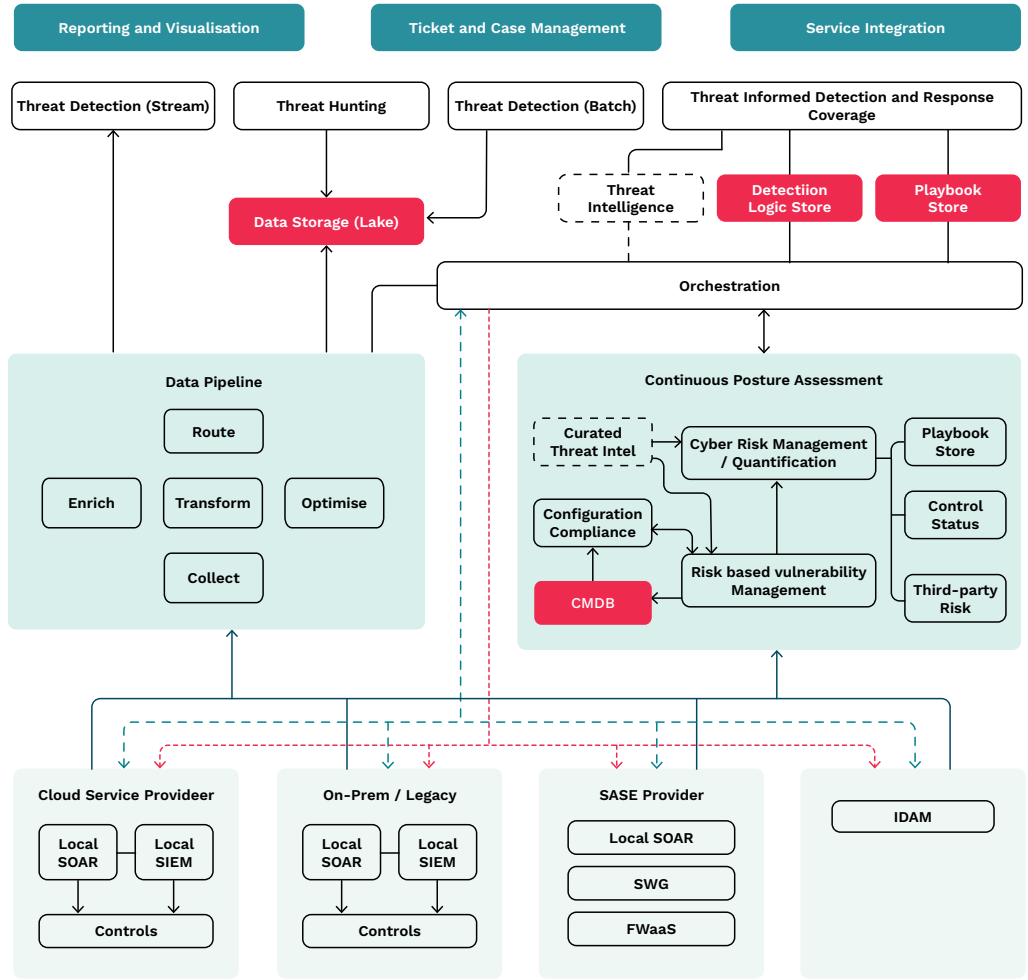
Organisations must adopt an open approach to their SOC architecture to create a Future-Ready SOC. This means integrating digitally-native capabilities alongside tooling deployed into legacy environments. The architecture should also be extensible to reduce dependence on a single vendor and facilitate the adoption of evolving technologies.

Collaboration and innovation with suppliers and partners will be crucial to future cyber defence. The open approach to SOC architecture will enable collaboration and the ability to experiment with threat detection and response.

Accommodating the needs of users is vital. Attention should be paid to how each persona, from analysts to senior executives, will consume and interact with the information generated and services offered by the SOC.

The key to the success of the Future-Ready SOC will be acquiring the necessary data required to observe, and prevent threats to the organisation and the third-parties they rely on to ensure resilient business operations.

Future-Ready SOC Architecture



Data Acquisition and Storage

A robust SOC must gather relevant data from multiple sources and use it in a way that delivers the required security outcomes.

To achieve high performance and success, it's not enough to simply have the best tools, talent, and dashboards in place. These efforts may be in vain if you don't have the right information to support them. The most important ingredient for success is high-quality data, supported by a pipeline that ensures the right information gets to the right places at the right time. Therefore, it's crucial to focus on data quality and efficient data delivery mechanisms to ensure optimal performance and progress. Extracting event data and other telemetry from an increasingly diverse set of protected environments is necessary.

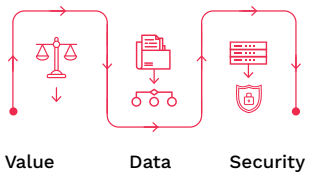
Appliance-based security controls, native cloud controls, and embedded security controls in network infrastructure generate high volumes of data.

The architecture must be realised in such a way that it can effectively support the role of the SOC in detecting security threats, indicators of compromise, and compliance issues by harnessing the available data. However, accomplishing this task is challenging due to the vast amounts of data available and the limitations imposed by acquisition, storage costs, licenses, and processing capabilities.

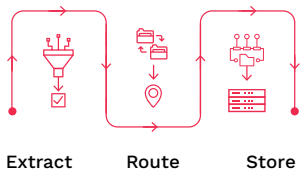
The timely consumption of data is critical to avoid a backlog. Our Future-Ready SOC must maximise detection efficacy while minimising operational costs.

There are two considerations here:

The ability to understand the value of individual data sets in supporting security outcomes.



The ability to extract, route and store this data efficiently and economically.



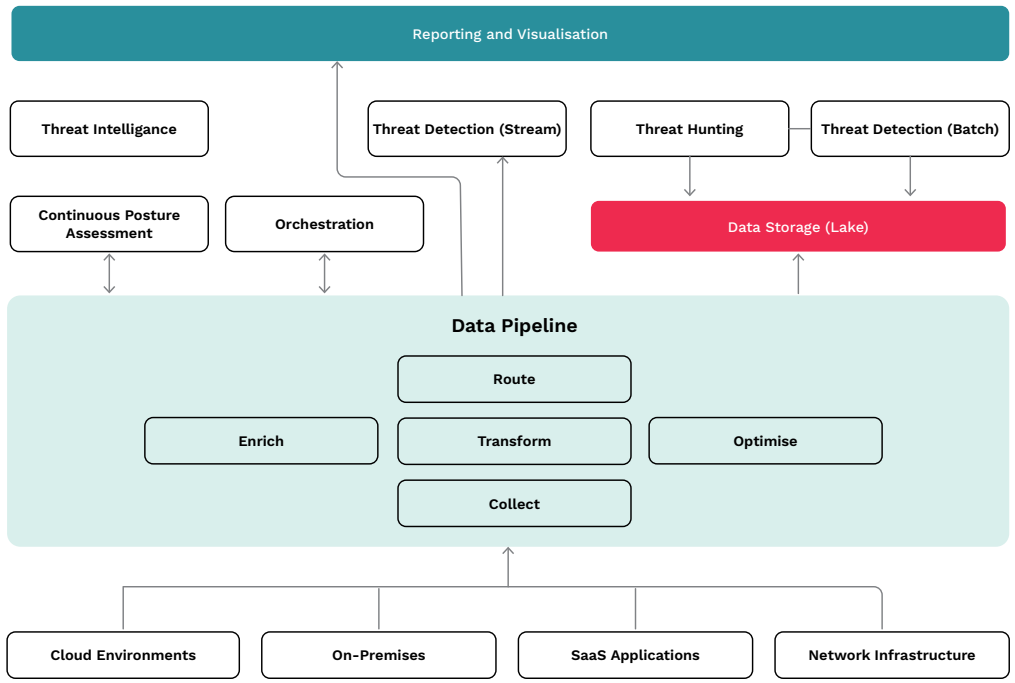
Understanding the security value of data is critical in making decisions about what data to ingest into the SOC. By linking the business context (what is being protected and why) with threat intelligence (who is posing a threat and how), we can identify the attack paths and determine the appropriate detection content. This allows us to prioritise triage and response activities and ultimately reduce business risk. By evaluating the value of the data we ingest, we can measure the return on investment in terms of risk reduction.

By prioritising your data, we can now route the data to where it is most useful, in time and store it in the correct places and formats to maximise cost efficiency. We call this Data Pipelining. ▶▶▶

What is Data Pipelining?

“At its most basic level, a data pipeline can be seen as an aggregator or even a manifold that takes data from multiple sources and distributes that data to multiple destinations, eliminating the need for multiple bespoke systems. As the data transits the pipeline, it may also be acted upon, essentially shaped based on organisational needs and the requirements of a receiving system.”

Data Acquisition and Storage Architecture



Data is the heart of any security operation. Collecting and making sense of it is vital to success. As the number of environments, data sources and formats continue to increase, so does the complexity and value of this essential SOC function.

Consider Routing your Data to more Cost-Effective Destinations

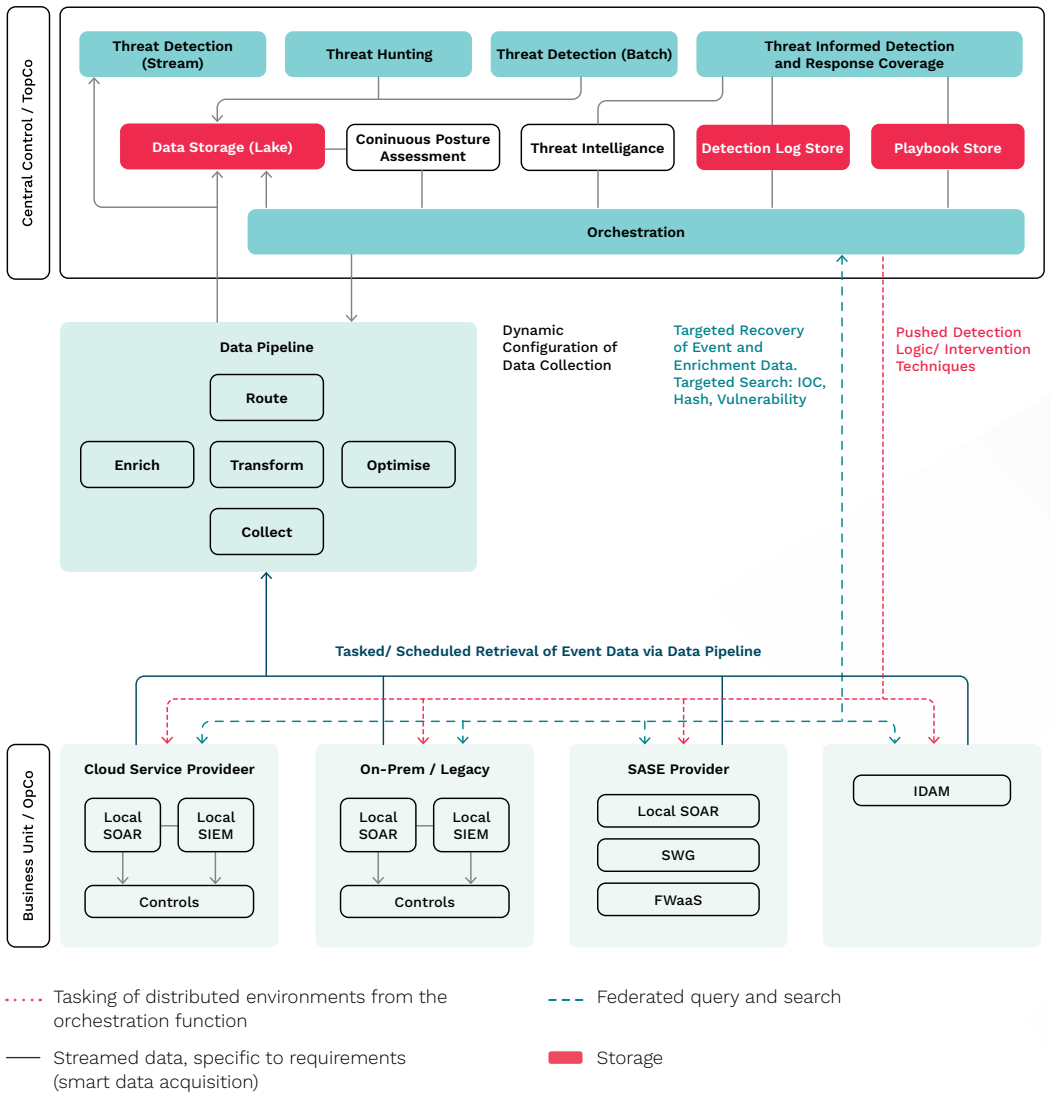
Indexed storage can take up to 12 times the resources compared to object storage, with linear costs to match. Instead of storing all the data in expensive places like Security Information and Event Management tools (SIEMs), you can route it to more affordable storage options like Azure Blob, Amazon S3 or MinIO. This way, you can retain the data separately from the important analysis, which helps to lower the overall costs whilst still complying with data retention requirements.

The increased compression ratios that are achievable tend to deliver lower costs while still complying with most technical data retention requirements. If the data is needed for threat hunting, investigation, or incident response, it can still be accessed to provide valuable insights.

Now, with this compliant and budget-saving solution, you can prioritise high-performance data to power your security program. ▶▶▶

In the past, maintaining a strong chain of custody for event data was seen as vital for future criminals prosecutions. However, this is expensive – and for most organisations – an exercise in futility. Whilst it is appreciated that there are some organisations who must store raw, probably unaltered data within log archiving technologies for regulatory purposes, for most organisations the likelihood of law enforcement successfully arresting and prosecuting a malicious actor who has compromised their network is so small that the value of this is hugely outweighed by the cost. Therefore, using cheaper storage options (like cloud-based object storage) can save a lot of money compared to storing data online in SIEM indexes.

Federated Detection & Response



There's a tension between tight focus and a bird's eye view, both are vital. Balancing this successfully on two levels – local autonomy / central control and data and information management – remains a crucial challenge for SOC owners and is unique to each organisation and situation.

Federated Detection and Response

Detection and response are often measured in Mean Time to Detection (MTTD) and Mean Time to Response (MTTR) – although the effectiveness of response is sometimes a more valuable measurement. Fast responses can sometimes be counterproductive and incomplete. The primary objective of a federated detection and response model is to enable quick recovery of information from a distributed enterprise environment, including Hybrid, Multi-Cloud and Poly-Cloud architectures.

The SOC then needs to use its own security capabilities and local storage to improve MTTD and MTTR without running up data transfer costs.

All of this must happen within each environment – each internal business team, cloud provider or supply chain partner while keeping hierarchical ownership and orchestration and the ability to prevent and detect holistically.

A secondary benefit of this approach is devolution: as detection and response federation takes force, its capabilities and learnings can be fed to individual business units or operating companies.

Finally, the federated approach should lean heavily on the central orchestration of detection logic and intervention techniques built on playbooks as far as practical.

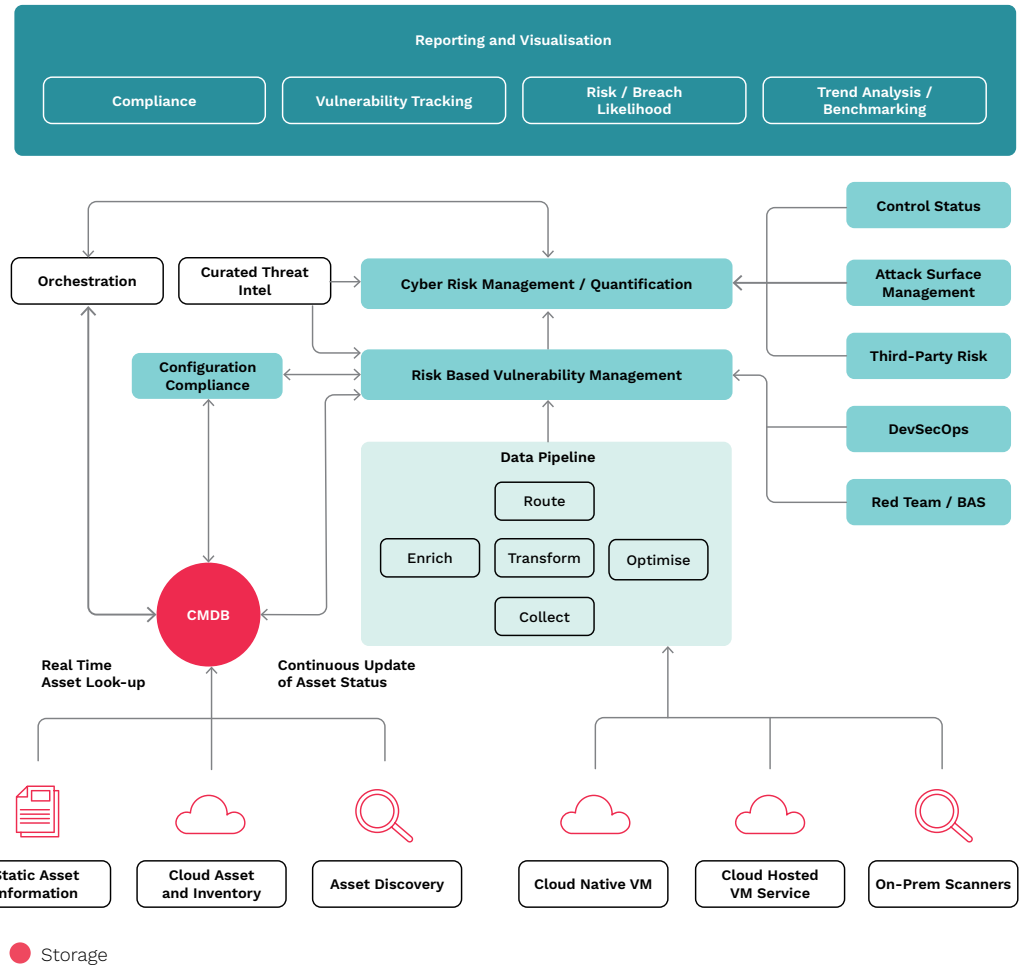
This encourages local control selection, policy enforcement and regional or national regulatory compliance, lightening the load for the central team and SOC and giving them the space to look at governance and perform high-value intervention and support during incidents. ▶▶▶

Continuous Posture Assessment

Continuous Posture Assessment (CPA) fuses the outputs from Vulnerability Management, Attack Surface Management (ASM) and Breach and Attack Simulation. With this information, the team can understand how likely it is that specific critical assets will be breached and take a proactive risk management approach to protect them. It's important to remember that when dealing with critical assets, we need to consider the users who have access to these assets. Some users may have authorised and valid access to the information stored on critical systems, which means that simply looking at the infrastructure assets alone is not enough. This emphasises the need for the SOC to have a good contextual understanding of all the components, users, and interfaces of critical systems.

CPA gives regular, sustained assessments of holistic security posture across environments, regardless of how new or outdated they are. The output is a real-time view of your organisation's security posture that accounts for present and anticipated threats and absorbs 'what if' analyses. It can also be used to plan and run proactive mitigations. The secondary benefit is understanding what techniques and remediations work best for each situation, asset or group of assets, thus improving effectiveness and reducing waste. It also gives authoritative measurements that can be used by upstream analytics and investigators via the orchestration function.

Continuous Posture Assessment Architecture



Knowing who and what you need to protect and how it might be vulnerable is the bedrock for security operations – but it is also the secret ingredient in measuring, reporting and mitigating risk, which becomes more critical when demonstrating value and arguing for strategic investment to business leaders.

Purposeful Adoption of Machine Learning and Artificial Intelligence

The potential of AI in improving security outcomes and reducing costs is immense; however, there are genuine concerns regarding trust. The market is dealing with a complex web of third-party and self-hosted models, data flows, and autonomous workers, with uncertainty about the adoption path.

Research undertaken by Adarma last year suggested that while many organisations are looking at how AI might augment their operations, at least in security circles, the book on how it will do so remains unwritten. That's not unsurprising – after all, the pace of change demonstrated by the current crop of AI-labelled applications is staggering. Adarma's survey of 500 security leaders found that 61% of respondents believed AI could effectively manage up to 30% of security operations, with 17% seeing it increasing to 50% in the next five years.

The use of AI and ML techniques in cyber defence is not a new concept, ML based behaviour analysis and established baseline deviation have been at the core of leading-edge threat detection for a number of years. The emergence and general adoption of Generative AI will expand the capability of threat actors and cyber defence teams at an accelerated pace and as a consequence drive high expectations and potential over adoption within the SOC.

Adoption of AI/ML within the future ready SOC should be based on defined and aspirational business outcomes, complimentary to established ways of working and as an enabler to innovation in cyber defence tradecraft. Organisation should look to assess and perform experiments involving candidate AI/ML tools, techniques and models prior to them being adopted within the SOC.

> **Adoption of AI/ML within the future ready SOC should be based on defined and aspirational business outcomes, complimentary to established ways of working and as an enabler to innovation in cyber defence tradecraft.**
>
> **James Todd, CTO, Adarma**

Conclusion

The journey of securing organisational assets through SOCs has evolved significantly over the past decade. From centralised alert processing to a decentralised landscape driven by technological advancements and market shifts, the challenges faced by traditional SOC architectures have become increasingly complex, expensive, and difficult to scale.

This paper has outlined the blueprint for a Future-Ready SOC architecture designed to address these challenges head-on. By embracing flexibility, resilience, and adaptability, the Future-Ready SOC is positioned to navigate the dynamic threat landscape and rapidly evolving business environments. It serves as the orchestrator, bringing together various stakeholders, technologies, and methodologies to ensure proactive risk management and effective response to cyber events.

Fundamental principles of the Future-Ready SOC include scalability for large data volumes, monitoring diverse environments, embracing a federated detection and response model, leveraging automation and AI for efficiency, and adopting innovative threat-hunting techniques.

Central to the success of the Future-Ready SOC is its ability to collect and use data effectively while maintaining observability across different environments. By shifting towards a federated data strategy and employing open and extensible architectures, organisations can empower SOC teams to innovate and collaborate while remaining agile in the face of evolving threats.

In essence, the Future-Ready SOC represents a paradigm shift in security operations, enabling organisations to enhance their cyber defence capabilities and support broader business initiatives such as cloud migration and digital transformation. By implementing the strategies outlined in this paper, organisations can future-ready their SOC architectures and ensure readiness for future challenges.

> **By embracing flexibility, resilience, and adaptability, the Future-Ready SOC is positioned to navigate the dynamic threat landscape and rapidly evolving business environments.**

Get in touch

If you would like to speak to an Adarma consultant about any issues or approaches raised in this paper, please email **hello@adarma.com.**

You may also be interested in a SOC Maturity Assessment; this takes a threat-led approach, evaluating all aspects of your SOC and building a clear roadmap for your future SOC programme.

Find out more at adarma.com

ADARMA

TOGETHER WE'VE GOT THIS

hello@adarma.com
www.adarma.com