How CyberStash Eclipse.XDR Can Help to Deliver Shield 3: World-Class Threat Sharing and Blocking of the 2023-2030 Australian Cyber Security Strategy

Table of Contents

Abstract

The Australian Government remains steadfast in its commitment to establishing Australia as a leading authority in global cybersecurity by 2030. The success of the 2023–2030 Australian Cyber Security Strategy hinges significantly on the execution of its actionable plans. To achieve this, the Government is actively addressing critical gaps across 6 cyber-Shields, encapsulating 20 Action Plans.

In pursuit of global cybersecurity leadership by 2030, the Australian Government emphasises the cultivation of genuine partnerships, the development of lasting solutions, and continued collaboration within the industry. Within the dynamic landscape of cybersecurity, CyberStash unveils a pivotal asset in its arsenal, the **Eclipse.XDR** Cyber Defence Platform, tailored to meet Shield 3 imperatives outlined in the 2023-2030 Australian Cyber Security Strategy. This whitepaper meticulously dissects how Eclipse.XDR seamlessly integrates with Shield 3, explaining its role in realising the strategic objectives outlined in Action 11 and Action 12.

Shield 3, heralding world-class threat sharing and blocking, becomes a focal point of CyberStash's Eclipse.XDR capabilities. Within Action 11, the strategy emphasises the pivotal role of strategic threat intelligence dissemination across sectors. This initiative fosters collaboration between government and industry through the Government's newly formed Executive Cyber Council, entrusted with the responsibility of transparent co-leadership on critical cyber security issues. Eclipse.XDR embodies this strategic vision by facilitating seamless machine-to-machine exchange of cyber threat intelligence. CyberStash's Eclipse.XDR is strategically positioned to bolster the strategy by facilitating the establishment and fortification of Information Sharing and Analysis Centres (ISACs) across sectors. CyberStash already has government agencies utilising the platform in ways aligned with the strategy's envisioned objectives. These ongoing implementations serve as live examples of how Eclipse.XDR can effectively function within the context outlined by the strategy. These real-world implementations offer insights that we can replicate and tailor to support the government's pilot initiatives, especially within the health industry.

In parallel, Action 12 accentuates the necessity to scale threat blocking capabilities to fortify against cyber-attacks. CyberStash's Eclipse.XDR spearheads this mission by collaborating with industry partners to pioneer cutting-edge threat blocking capabilities. Within our ongoing Partnership Program, Eclipse.XDR takes the lead in operationalising automated, real-time threat blocking functionalities seamlessly integrated with current government and industry threat sharing platforms. Additionally, Eclipse.XDR champions the expansion of threat blocking capabilities, incentivising, and encouraging entities such as telecommunication providers, ISPs, and financial services to fortify their defenses against evolving threats.

This whitepaper is an indispensable guide designed for the Government's Executive Cyber Council, as well as CIOs, CISOs, and Cybersecurity Managers within governmental and corporate sectors. It meticulously outlines how CyberStash's Eclipse.XDR stands as an essential solution, perfectly aligned with the mandates of the Australian Cyber Security Strategy. Through the utilisation of Eclipse.XDR, stakeholders are empowered to bolster their cybersecurity infrastructure, cultivating resilience in an ever-evolving landscape of cyber threats.

References: 2023–2030 Australian Cyber Security Strategy and Action Plan

1. https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf
2. https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy-action-plan.pdf

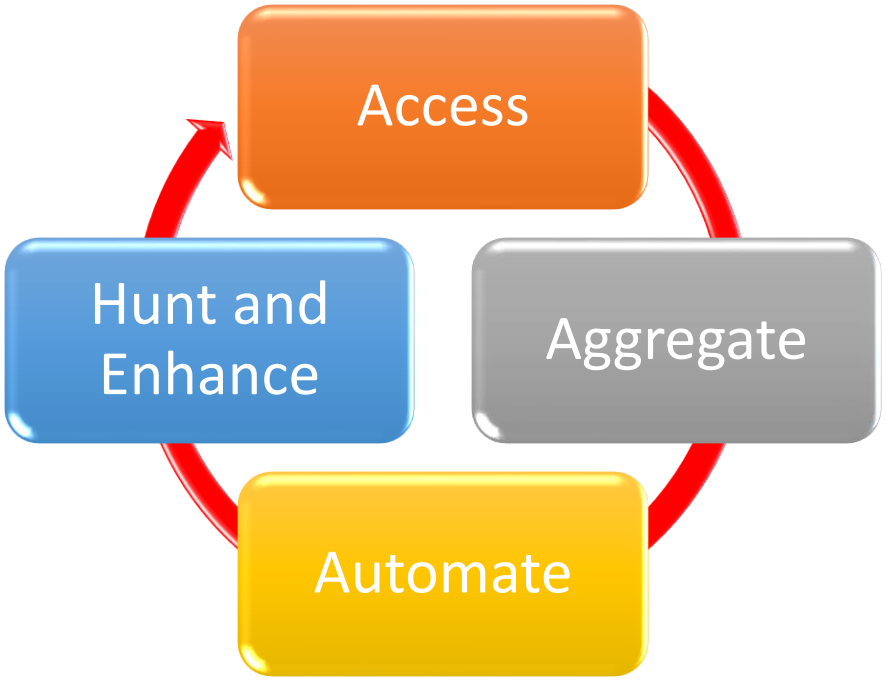
Components of an Optimal Cyber Threat Intelligence Platform

Cyber Threat Intelligence Framework

In the ever-evolving landscape of cybersecurity, the efficacy of defense mechanisms hinges upon the strength and sophistication of the tools deployed. Central to this arsenal is a robust cyber threat intelligence platform, the linchpin in fortifying organisational resilience against the onslaught of sophisticated cyber threats. This section delves deep into the essential components that construct the bedrock of an optimal cyber threat intelligence framework.

Amidst the maze of digital adversaries and evolving threat landscapes, the ability to gather, analyse, and act upon threat intelligence at scale becomes imperative for cybersecurity practitioners. This section peels back the layers of this intricate framework, outlining the core tenets that not only facilitate comprehensive threat detection but also streamline response mechanisms.

Within the multifaceted realm of cyber threat intelligence, the pillars of **access**, **aggregation**, **automation**, and **proactive hunting and enhancing** stand as the cornerstones upon which an effective defense strategy is built. Each facet holds a unique significance, not only in optimising resource utilisation and cost-effectiveness but also in navigating the complex challenges inherent in establishing and sustaining a robust threat intelligence program.



Farmwork Components

This section delves into the essential components of a Cyber Threat Intelligence Framework, revealing how each element plays a vital role in mitigating risks cost-effectively, optimising resources, and adeptly addressing the challenges inherent in establishing and maintaining a robust cyber threat intelligence program.

Access: Collecting Accurate Threat Indicators

Context: The foundational pillar of a robust threat intelligence platform lies in its access to a diverse array of threat indicators. This encompasses the capability to gather millions of accurate threat indicators from multifaceted sources, spanning commercial, open source, industry, and governmental realms. The significance of this access extends beyond volume; it ensures comprehensive coverage across various threat types, including reputation feeds, blacklists, and IPs associated with countries or organisations. Access to such extensive and varied data sources empowers organisations to fortify their defense mechanisms against a spectrum of cyber threats.

Significance: Access to a diverse array of threat indicators within a cyber threat intelligence platform stands as a linchpin in fortifying defenses and minimising risks. The comprehensive gathering of accurate threat intelligence plays a pivotal role in enhancing the accuracy and efficacy of threat detection mechanisms. It is not merely about the volume of data but the quality and accuracy that determine the platform's effectiveness. This accuracy serves as a powerful tool in reducing the exposure to potential cyber threats and their subsequent impact.

The goal of leveraging intelligence within these platforms is to minimise risk by making informed decisions that enable the proactive blocking of malicious traffic. Accurate and reliable intelligence significantly minimises the occurrence of false positives, which could otherwise disrupt business operations and affect end users. False positives not only trigger unnecessary alerts but might also lead to the blockage of legitimate traffic, impacting business continuity and user experience. The need to constantly create exceptions to accommodate these false positives increases resource efforts and could potentially create loopholes in the security posture.

Therefore, the collection of precise and validated threat intelligence becomes paramount. It not only strengthens the ability to detect and block threats effectively but also streamlines operations by reducing the need for manual intervention and exception handling. This precision not only optimises resource allocation but also ensures a more robust cybersecurity posture, safeguarding against threats while minimising disruptions to daily business operations.

Aggregate: Consolidating and Analysing Threat Feeds

Context: Aggregation within a threat intelligence platform signifies the consolidation of multiple threat feeds into a unified, easily manageable feed. An open platform that seamlessly integrates Threat Intelligence (TI) via standards like STIX/TAXII ensures interoperability and simplifies the aggregation process. Furthermore, the application of analytics on aggregated data enriches intelligence, enabling deeper insights into emerging threats and attack patterns.

Significance: Aggregation streamlines the complex task of managing disparate threat feeds, fostering a unified view of threat landscapes. This integration and analysis enhance the actionable value of threat intelligence, enabling more informed decision-making. This, in turn, optimises resources by prioritising responses based on the severity and relevance of threats.

Automate: Real-time Updates and Automated Response

Context: Automation stands as a cornerstone in the realm of cyber threat intelligence, ensuring organisations remain agile in the face of rapidly evolving threats. Real-time updates guarantee the dynamic refreshment of threat feeds, enabling constant vigilance against emerging risks. Additionally, the automated application of blocking policies based on threat intelligence and the seamless sharing of threat information facilitate swift and proactive responses to potential risks.

In the context of today's big-data challenges, traditional change approval processes become obsolete. Dealing with vast amounts of threat intelligence data demands equally robust solutions—ones that confidently and automatically block threats. Just as we no longer wait for lengthy approvals to implement antivirus signature changes, we must operate with the same confidence in automatically blocking threats using threat intelligence. The need for swift, proactive action necessitates automated responses that rely on comprehensive threat intelligence, allowing organisations to respond rapidly and decisively in the face of evolving cyber threats.

Significance: Automation reduces response time, mitigates potential damages, and minimises the strain on human resources by enabling swift and proactive threat mitigation. The ability to automatically update and apply policies streamlines operations, enhancing the organisation's resilience against cyber threats while optimising resource utilisation.

Hunt and Enhance: Proactive Investigation and Threat Mitigation

Context: The capability to pivot, investigate, and analyse suspicious network activity empowers cybersecurity teams to actively identify and neutralise potential threats. Augmenting this, the platform should furnish analytical dashboards that assist security analysts in unveiling previously unidentified threats and unauthorised traffic. These tools fortify a proactive defense strategy, enabling swift responses to evolving attack methods and fostering a more vigilant security posture.

Significance: Hunting and enhancing mechanisms play a pivotal role in empowering organisations to proactively detect and neutralise potential threats before they escalate. Notably, these mechanisms effectively reduce the attack surface, fortify overall security, and promptly block unknown threats and unauthorised traffic. Moreover, the platform's automated collection, enrichment, and real-time utilisation of telemetry data in ongoing attacks significantly enhance its capability to pre-emptively address emerging threats.

In addition to these capabilities, there's a critical need for both government and industry sectors to have a unified view that displays agencies under attack, their levels of protection, and those that remain vulnerable. This unified visibility is essential in fostering a collective defense strategy. Furthermore, the provision of insightful analytical dashboards by the platform alleviates the workload on security analysts, eliminating the necessity for them to independently develop such tools. By reducing reliance on individual skill sets, these dashboards streamline processes, minimise effort, and ensure a continuous and effective proactive defense against evolving threats.

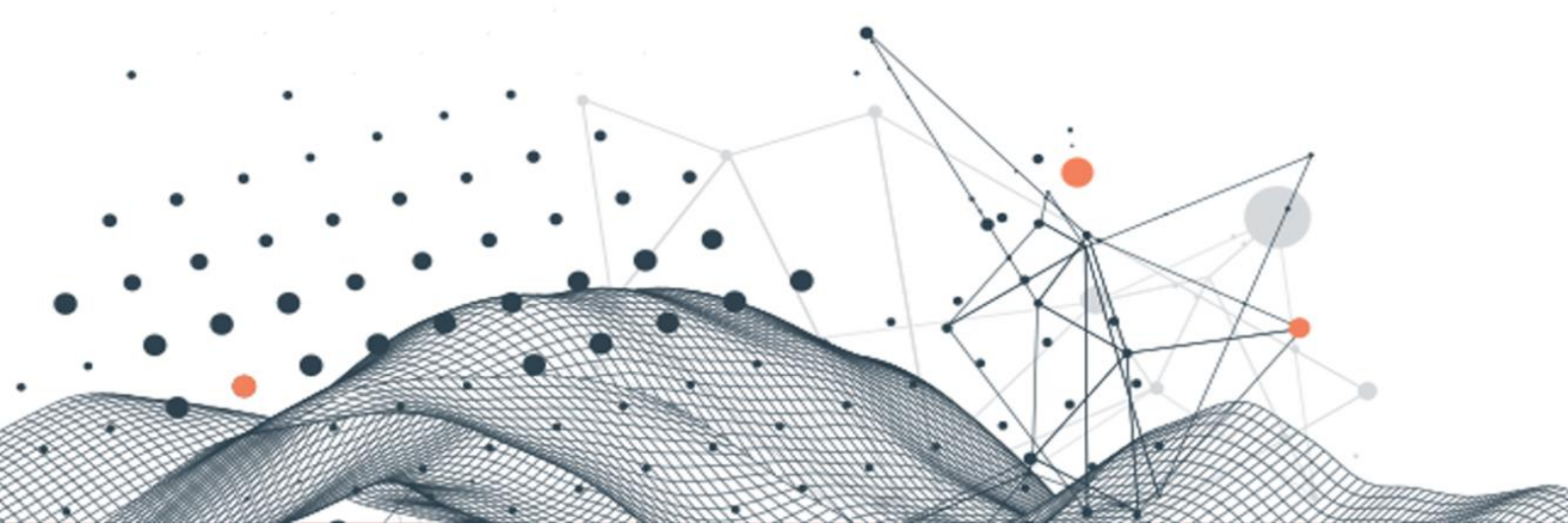
How CyberStash Can Help with Shield 3: World-class Threat Sharing and Blocking

Shield 3 in the Australian Cyber Security Strategy underscores the critical need for unparalleled threat sharing and blocking capabilities to fortify the nation's cybersecurity resilience. At its essence, Shield 3 emphasises strategic collaboration between government and industry to build a robust cyber defense mechanism. This mandate outlines pivotal actions focused on enhancing threat intelligence sharing, fostering collaboration, and scaling threat mitigation across Australia's vital digital sectors.

Action 11 within Shield 3 emphasises the urgency of strategic threat intelligence sharing with industry partners, augmenting tactical and operational intelligence collaboration. CyberStash's Eclipse.XDR Cyber Defence Platform, can play a pivotal role here, facilitating seamless sharing of strategic threat intelligence among stakeholders. With Eclipse.XDR, organisations gain the capability to aggregate and analyse diverse threat feeds, enabling enhanced intelligence sharing and collaboration in real-time. This empowers entities to stay ahead of emerging threats and foster a proactive defense stance.

Action 12 underscores the critical need to expand threat blocking capabilities to combat cyber-attacks effectively. CyberStash's Eclipse.XDR is strategically positioned to enable this objective by providing advanced threat blocking capabilities integrated within its systems. With the agility to leverage next-generation threat blocking technologies, Eclipse.XDR stands prepared for collaboration with industry partners and academic institutions to pilot automated threat blocking capabilities, seamlessly integrating with the government’s existing threat sharing platforms. This strategic initiative, once deployed, ensures the establishment of a robust defense infrastructure capable of dynamic responses to evolving threats, fortifying cybersecurity postures across vital sectors.

Our exploration through Shield 3 of the Australian Cyber Security Strategy underscores how CyberStash's Eclipse.XDR aligns seamlessly with these imperatives. By leveraging Eclipse.XDR, organisations gain a strategic advantage in fortifying their cybersecurity defenses, contributing to the Strategy's objectives, and mitigating escalating digital threats effectively.



Action 11. Create a Whole-of-Economy Threat Intelligence Network

Action	Plan
Share strategic threat intelligence with industry	**Establish the Executive Cyber Council as a coalition of government and industry leaders** to improve sharing of threat information across the whole economy, and drive public-private collaboration on other priority initiatives under the Strategy.

How CyberStash Can Help

The establishment of the Executive Cyber Council as a collaboration between government and industry leaders represents a pivotal step in enhancing the sharing of threat information across the entirety of the economy. This initiative not only aims to improve threat information sharing but also seeks to drive robust public-private collaboration on key initiatives within the Strategy.

CyberStash's Eclipse.XDR Cyber Defence Platform emerges as a beacon in achieving the objectives outlined in Action 11. As an industry leader, CyberStash offers real-world case studies illustrating how Eclipse.XDR is actively advancing the goals of this action plan across both government and non-government sectors.

Across various sectors, Eclipse.XDR is already instrumental in fostering threat intelligence sharing and collaboration. For instance, within the financial sector, Eclipse.XDR is enabling banks and financial institutions to share threat intelligence effectively, facilitating rapid response mechanisms against evolving threats. Similarly, in government entities, Eclipse.XDR is streamlining the sharing of threat data, enhancing the nation's cybersecurity posture by fostering collaboration between government agencies.

Eclipse.XDR boasts a distinctive hierarchical architecture model among its many unique capabilities. This model allows for the deployment of clustered instances tailored to specific industries while maintaining a top-level "whole of economy" instance. This hierarchical architecture enables industry-specific clusters to pull intelligence from the overarching platform, ensuring tailored threat intelligence sharing within sectors without compromising broader economy-wide collaboration.

This hierarchical architecture model isn't just about bolstering industry-specific threat intelligence sharing; it's designed to foster seamless collaboration across sectors, perfectly aligning with the Strategy's objectives. It empowers CyberStash's Eclipse.XDR to serve as a catalyst, facilitating comprehensive collaboration across the entire economy and enabling targeted sharing of threat intelligence within specific industries. This capability significantly enhances cybersecurity resilience across diverse sectors.

Action	Plan
Expand tactical and operational threat intelligence sharing	**Continue to enhance ASD's existing threat sharing platforms** to enable machine-to-machine exchange of cyber threat intelligence at increased volumes and speeds. These platforms will enable a framework within which industry-to-industry and government-to-industry cyber threat intelligence can be exchanged.

How CyberStash Can Help

CyberStash's Eclipse.XDR Cyber Defence Platform excels in its versatility, enabling simultaneous integration with existing government infrastructure, such as the Australian Signals Directorate's (ASD) threat sharing platform. Eclipse.XDR's adaptability ensures a harmonious coexistence and collaboration with ASD's established threat sharing infrastructure. By integrating seamlessly with ASD's platform, Eclipse.XDR augments the existing capabilities, fostering a more comprehensive and streamlined threat intelligence ecosystem.

Furthermore, Eclipse.XDR's integration capabilities transcend the scope of ASD's threat sharing platform. CyberStash architected the Eclipse.XDR Cyber Defence Platform to seamlessly interface with an array of commercial and open-source threat intelligence providers. Serving as a unified aggregator, this platform effortlessly consolidates a multitude of threat feeds, encompassing diverse sources such as industry-specific data, reputation feeds, open-source intelligence, and more. This comprehensive integration empowers organisations with access to an expansive mosaic of threat intelligence, enabling the utilisation of a broad spectrum of data sources to bolster and fortify their cybersecurity defenses.

Eclipse.XDR's integration capabilities do not merely stop at interfacing with diverse feeds; it goes further by applying advanced analytics and enrichment techniques. By ingesting, correlating, and analysing multifaceted threat intelligence data, Eclipse.XDR enhances the quality and depth of threat information. This enriched intelligence enables organisations to make more informed decisions, proactively identifying and mitigating emerging threats effectively.

The platform's ability to seamlessly integrate with both government-specific threat sharing platforms and a diverse array of commercial and open-source threat intelligence providers underscores its adaptability and effectiveness. This integration empowers organisations to harness a holistic and dynamic threat intelligence landscape, fortifying their cybersecurity posture against a myriad of evolving threats.

Action	Plan
Expand tactical and operational threat intelligence sharing	**Launch a threat sharing acceleration fund** to provide seed funding to establish or scale-up Information Sharing and Analysis Centres (ISACs) in low maturity sectors. This program will start with an initial pilot in the health sector to enable the sharing of actionable threat intelligence and cyber best-practice.

How CyberStash Can Help

CyberStash's Eclipse.XDR Cyber Defence Platform stands as a catalyst in expediting the strategy for expanded tactical and operational threat intelligence sharing. Its agility and comprehensive capabilities enable both government entities and agencies to leverage it as a benchmark Key Performance Indicator (KPI) for learning, improvement, and strategic advancement.

The establishment of a fund to accelerate threat sharing for Information Sharing and Analysis Centres (ISACs) in less developed sectors is a crucial step in bolstering cybersecurity in vulnerable areas. Eclipse.XDR's adaptability enables it to support this initiative by swiftly deploying and scaling up ISACs. Leveraging its capabilities, organisations can expedite setting up these centres, thus accelerating the exchange of actionable threat intelligence and best cyber practices.

Eclipse.XDR's versatility extends to various sectors. It can promptly initiate a pilot program in the health sector, fostering collaboration and resilience through the prompt sharing of actionable threat intelligence and best practices. This pilot program doubles as a learning platform, using Eclipse.XDR as a benchmark to gauge progress, identify improvement areas, and refine strategies for broader sector-wide implementation.

Its role in accelerating the strategy goes beyond immediate deployment—it constantly evolves. Eclipse.XDR learns from these pilots, refines strategies, and adapts swiftly to evolving threats and industry needs, making it a dynamic tool for continuous improvement and effective cyber defense.

By harnessing Eclipse.XDR's capabilities, organisations can expedite ISAC launches in less mature sectors and establish a framework for ongoing learning, improvement, and resilient cybersecurity practices across various industries.

Leveraging existing client case studies becomes pivotal in assessing the strategy's effectiveness. CyberStash's rich experience and successful implementations offer valuable insights. These case studies provide a solid framework for understanding the nuances of similar initiatives and aligning Eclipse.XDR's capabilities with specific goals.

Utilising real-world scenarios and client success stories offers tangible insights into how Eclipse.XDR can achieve outlined objectives. These case studies guide strategy alignment, refine approaches, and anticipate potential challenges, ensuring a more effective implementation of the strategy across diverse sectors and industries.

Action	Plan
Expand tactical and operational threat intelligence sharing	**Encourage and incentivise industry to participate in threat sharing platforms**, with a focus on organisations that are most capable of collecting and sharing threat intelligence at scale across the economy.

How CyberStash Can Help

CyberStash's Eclipse.XDR stands as a cornerstone not only in facilitating the collection, enrichment, and sharing of threat intelligence but also in empowering organisations with robust reporting, hunting, searching, and automated enrichment and blocking capabilities. This comprehensive suite of functionalities extends beyond mere aggregation and sharing, reinforcing the proactive defense stance essential in combating evolving cyber threats.

The platform's capabilities transcend traditional data handling, offering a robust reporting framework that provides in-depth insights into threat trends and patterns. These reports empower cybersecurity teams with comprehensive analytics, aiding proactive decision-making and strategic planning in fortifying cyber defenses.

Eclipse.XDR's hunting and searching functionalities heighten threat detection and troubleshooting capabilities, empowering security analysts to proactively identify and neutralise potential threats. This allows swift identification of whether threat intelligence blocking is causing reported access issues. In the background, its automated enrichment mechanisms tirelessly enhance threat intelligence with contextual insights, providing a deeper understanding of threat landscapes and adversary tactics.

Automated blocking within Eclipse.XDR not only stops threats in their tracks but also operates with precision, thanks to its automated enrichment processes. Whether blocking based on intelligence data or tactical policies, the platform's automated capabilities ensure swift and accurate threat response.

Encouraging and incentivising industry participation in threat sharing platforms becomes significantly more feasible with Eclipse.XDR's holistic functionalities. Its capabilities in reporting, hunting, searching, and automated enrichment and blocking serve as compelling incentives for organisations aiming to bolster their cybersecurity posture.

Eclipse.XDR is custom-tailored for diverse industries and agencies, enabling them not only to share threat intelligence but also to actively hunt, enrich, and automate their defense mechanisms. In the government sector, Eclipse.XDR fosters collaborative threat intelligence sharing among local government agencies, fortifying their joint defense against cyber threats specific to government entities.

By leveraging Eclipse.XDR's comprehensive functionalities, organisations and agencies participate more effectively in threat sharing initiatives, harnessing its suite of capabilities to fortify cybersecurity defenses seamlessly across the economy. This collaborative ecosystem, bolstered by reporting, hunting, searching, and automated enrichment and blocking, forms a robust defense against evolving cyber threats.

Action 12. Scale Threat Blocking Capabilities to Stop Cyber Attacks

Action	Plan
Develop next generation threat blocking capabilities	**Work with industry to pilot next-generation threat blocking capabilities across Australian networks** by establishing a National Cyber Intel Partnership with industry partners and cyber experts from academia and civil society. This partnership will pilot an automated, near-real-time threat blocking capability, building on – and integrated with – existing government and industry platforms.

How CyberStash Can Help

CyberStash's Eclipse.XDR stands as a crucial asset in advancing next-generation threat blocking capabilities, offering a head start towards achieving the objectives outlined in the National Cyber Intel Partnership. Leveraging existing partnerships, CyberStash is uniquely positioned to expedite the route to market for these enhanced capabilities.

The established partnerships CyberStash has fostered can be seamlessly leveraged within the National Cyber Intel Partnership, accelerating the collaboration with industry experts and academia. This strategic advantage significantly reduces the time required to navigate partnerships, ensuring a swift initiation of the pilot for automated, near-real-time threat blocking capabilities.

Moreover, Eclipse.XDR's readiness to integrate with the threat feeds from these established partnerships is a definitive advantage. The platform is already equipped to absorb and harmonise with the threat intelligence feeds from these partners, eliminating the need to start integration efforts from scratch. This streamlined integration process significantly reduces both time and cost, expediting the implementation of enhanced threat blocking capabilities.

The platform's adaptability and existing integrations ensure a seamless assimilation of threat feeds, fortifying Eclipse.XDR's robustness in combating cyber threats. This readiness not only accelerates the deployment but also enhances the platform's efficacy in swiftly identifying and neutralising evolving threats across Australian networks.

The repository of established partnerships, coupled with Eclipse.XDR's preparedness to integrate with their threat feeds, underscores CyberStash's readiness to contribute effectively to the National Cyber Intel Partnership. This collaboration fosters a proactive defense approach, fortifying Australia's cyber defense posture against emerging threats.

Action	Plan
Expand the reach of threat blocking capabilities	**Encourage and incentivise threat blocking across the economy**, focusing on the entities that are most capable of blocking threats – including telecommunication providers, ISPs and financial services.

How CyberStash Can Help

CyberStash's Eclipse.XDR stands as a paramount solution engineered to extend the frontier of threat intelligence blocking capabilities, operating seamlessly in diverse environments, whether on-premises or in leading public cloud infrastructures such as Asure, Google Cloud, and AWS. This adaptability ensures a crucial aspect in industry uptake: seamless integration, vital for robust cybersecurity implementation.

Encouraging entities like telecommunication providers, ISPs, and financial services to participate actively in threat blocking initiatives demands not only effective blocking mechanisms but also comprehensive real-time telemetry. Eclipse.XDR excels in this domain, offering unparalleled capabilities to produce real-time telemetry data on blocked or allowed traffic. Whether inbound or outbound, the platform provides detailed insights into the nature of blocking actions.

The platform's strength extends beyond threat blocking; it provides detailed insights into the rationale behind each action. Whether the block stems from threat intelligence data or tactical policies like GEO-IP, Autonomous System Number (ASN), or Top-Level Domain (TLD) based blocking, Eclipse.XDR generates comprehensive real-time telemetry. This level of detail is crucial for evaluating the effectiveness of threat blocking measures and ensuring the success of the program.

Seamless integration capabilities into both on-premises and public cloud environments position Eclipse.XDR as an accessible and adaptable solution for diverse entities. Its capability to offer extensive real-time telemetry data on blocked traffic types goes beyond mere blocking effectiveness. It empowers a profound comprehension of the threat landscape and the performance of applied policies. Furthermore, this system holds the potential to uncover high-risk infrastructures, shedding light on s intelligence that can reinforce existing defenses. By scrutinizing these high-risk areas, Eclipse.XDR enables the identification of emerging threats, offering valuable insights to fortify defenses and stay ahead of evolving cyber risks.

In a landscape where cybersecurity efficacy is not just about blocking threats but also about understanding the context behind these actions, Eclipse.XDR's real-time telemetry capabilities pave the way for informed decision-making and a more fortified cyber defense strategy.

Closing Remarks

Action Plans 11 and 12 within the Australian Cyber Security Strategy herald a critical era of cyber resilience, emphasising the imperative need for strategic threat intelligence sharing and scaling threat blocking capabilities. In this pivotal phase, CyberStash's Eclipse.XDR emerges as an instrumental solution, seamlessly aligning with and exceeding the mandates of these action plans.

Strategic Threat Intelligence Sharing

Strategic threat intelligence dissemination marks a cornerstone in fortifying cyber defenses across sectors. CyberStash's Eclipse.XDR, embodying the essence of the Cyber Threat Intelligence Framework, stands poised to catalyse this imperative. The platform's multifaceted capabilities align seamlessly with the Framework's essentials:

- **Access:** Eclipse.XDR collates diverse threat indicators from multiple sources—commercial, open-source, government, and industry, ensuring comprehensive threat coverage.
- **Aggregate:** By consolidating varied threat feeds into a unified platform, Eclipse.XDR ensures a centralised hub for enriched, analysed intelligence.
- **Automate:** The platform dynamically updates threat feeds in real-time, automating blocking policies, and seamlessly sharing intelligence—minimising manual efforts and time lags.
- **Hunt & Enhance:** Eclipse.XDR empowers proactive threat detection, enabling security analysts to pivot, hunt, and investigate suspicious activities—ensuring robust defense against evolving threats.

Scaling Threat Blocking Capabilities

Efficiently scaling threat blocking capabilities becomes imperative in the face of escalating cyber threats. Eclipse.XDR, with its prowess, stands as a testament to next-gen threat blocking:

- **Next-Generation Capabilities:** Eclipse.XDR pioneers next-gen threat blocking at traffic rates of 10Gbps, blocking up to 150 million indicators while maintaining real-time wire-speed—setting new benchmarks for threat mitigation.
- **Integration & Scalability:** The platform seamlessly integrates with existing government and industry platforms, harnessing partnerships and pre-established integrations to expedite deployment and reduce implementation efforts.
- **Cloud & On-Premises Integration:** Offering flexibility, Eclipse.XDR operates on-premises or in public clouds like Asure, Google, and AWS—ensuring a seamless and adaptable integration model.
- **Real-Time Telemetry:** In addition to blocking, Eclipse.XDR provides real-time telemetry on traffic—offering insights into blocked or allowed traffic, aiding in continuous improvement and informed decision-making.

Through the fusion of Action Plans 11 and 12 with the robust capabilities of CyberStash's Eclipse.XDR, organisations navigate an era of enhanced threat intelligence, initiative-taking defense, and scalable cyber resilience—a pivotal stride towards fortifying cybersecurity landscapes in line with the Australian Cyber Security Strategy's visionary objectives.

Elevate Your Cybersecurity

CyberStash presents **Eclipse.XDR**—the pinnacle of cybersecurity defense. Eclipse.XDR isn't just a solution; it's a shield fortified against the relentless evolution of cyber threats.

- **Unmatched Intelligence Empowerment**
  Eclipse.XDR redefines threat intelligence—collecting millions of accurate threat indicators from diverse sources and enriching them with contextual insights. Seamlessly aggregating this data, Eclipse.XDR provides real-time updates and automates intelligence sharing for proactive threat mitigation.
- **Pioneering Threat Blocking**
  Experience unparalleled blocking capabilities. Eclipse.XDR stands firm against threats, blocking up to 150 million indicators at 10Gbps traffic rates, ensuring real-time wire-speed protection. Its seamless integration in cloud or on-premises environments enhances adaptability and provides in-depth telemetry for comprehensive threat monitoring.
- **Future-Ready Security Solutions**
  Eclipse.XDR isn't just about meeting today's challenges—it's about securing tomorrow. With adaptable scalability and established partnerships, implementation is expedited, reducing effort and time. This platform isn't just a tool; it's the frontier of defense in the ever-changing cybersecurity landscape.

Discover **Eclipse.XDR**—a shield forged in intelligence, fortified in real-time blocking, and designed to secure your future against the unknown!

https://www.cyberstash.com