Service Providers powered by

EPIPHANY | INTELLIGENCE PLATFORM

Epiphany Intelligence Platform, empowering you and your clients

Continuous Threat Exposure Management to Predict and Prioritize Future Threats

Reveald guides organizations along their journey from reactive to proactive defense.

Reveald's AI-driven Epiphany Intelligence Platform™ empowers security teams to break free from existing reactive processes by leveraging Continuous Threat Exposure Management (CTEM), supported by the expertise to guide them on every step of the journey.

Today's security teams are struggling with context and swimming in data they can't act on. In cybersecurity, context is King!

Why does this situation exist? Modern organizations rely on a broad variety of tools and vendors, each driven to make their offerings complete and comprehensive, and to reveal as much information as possible. Unfortunately, it's usually people who must consume that information output, and though one tool's output might be acceptable, our security teams must handle the output of many tools – which conflict with each other as much as they agree.

To stay ahead of well-funded and organized adversaries is extremely complex. The job of prioritizing actions while being overloaded with new information is overwhelming cybersecurity teams. Combining this with the difficulty acquiring and retaining talent exacerbates the problem further.

Predict and Prioritize with Epiphany Intelligence Platform

Reveald's Epiphany Intelligence Platform (EIP) is an expert system allowing you to provide 24/7 continuous threat and exposure management analytics.

EIP is based on advanced attack scenarios built deeply into our AI models, leading to business risk reduction outcomes by ingesting and aggregating data from a variety of sources, automated security analysis, validation, reporting, and guided resolution.

EPIPHANY | INTELLIGENCE PLATFORM

Key Benefits

Grow Your Revenue and Profit

Continuous Threat & Exposure Management powered by EIP will allow you to attach incremental Annual Recurring Revenue (ARR) at high margin to your existing services business.

Reduce The Burden On You

When clients adopt EIP, you will reduce the incidents and operational overheads on delivering Cyber security for your clients.

Be Proactive and Valued

With Reveald's EIP, you address client issues proactively before attackers have caused concern or detriment to your clients. You will be able to measure and show the value you deliver for them.

For the first time, the client CISO can now easily answer questions from the board and CEO such as "Are we secure?" and "What threats should we be concerned with and what are we doing about them?"

Just as important is knowing how the clients' financial investment in tools and effort is based upon addressing real material risk to the business, not theory, guess work, or reacting to breaches. Elevate your customer's defensive posture with our approach to Cyber Resilience and Continuous Exposure Management—meticulously engineered, seamlessly integrated, and strategically concentrated. Our programs are designed to streamline processes, minimize operational complexities, and deliver cost-effective solutions for IT, DevOps, and Cyber Security personnel. Embrace operational excellence and safeguard your digital assets with unmatched efficiency.

Why is EIP the right fit for Service Providers?

In a landscape where your clients have diverse technologies, and you are a security business providing outcomes to clients, it is near impossible to answer the question "Are the IT systems and cyber security controls working together to protect the business the treat?". Building, marketing, and selling new services is time consuming and expensive. Partnering with Reveald removes these risks and delivers rapid results for your clients.

HOW DOES OUR EIP HELP YOU AS THE SERVICE PROVIDER?

Cyber Resilience Strategy: Typically, evaluating a client's cyber resilience involves a comprehensive consulting process to scrutinize their entire system, ensuring that protective measures are effectively shielding their operations. However, this assessment often represents merely a momentary glimpse, and with the dynamic nature of changes in policies, access rights, and system updates, the findings may be outdated by the time they're reported. By incorporating the EIP as a Service Provider, you can craft a dynamic, real-world Cyber Resilience Strategy tailored to your client in real time. This strategy prioritizes risk assessment based on actual real exposures present and the robustness of existing defenses against known threats. It's anchored in EIP's impact matrix that identifies and prioritizes the client's High-Value Assets. With this approach, you're not just diagnosing—you're delivering ongoing vigilance.

With this approach, you're not just diagnosing **—you're delivering ongoing vigilance.**

Our approach ensures you can provide continuous predictive monitoring and analysis of the client's environment, pinpointing the top 5-10 high-value, straightforward daily actions—plus alternatives—to proactively bolster their defenses and maintain a robust posture against potential breaches or cyber-attacks.

Our approach ensures you can provide continuous predictive monitoring and analysis of the client's environment, pinpointing the top 5-10 high-value, straightforward daily actions—plus alternatives—to proactively bolster their defenses and maintain a robust posture against potential breaches or cyber-attacks.

Penetration Testing: Typically, clients and their penetration test service provider will pick off high value areas of the business to test controls. The idea being to verify if the environment can be breached by an attacker. Instead of randomly picking areas to test and not knowing if the results will be productive or not, EIP provides focus for you and the customer. It allows you as the Service Provider to give specific scope guidance to the client on where the spend the funding for penetration testing. The top 10 recommendations in EIP will provide your mitigation baseline and guidance for test execution. The benefit is the penetration test will return a positive investment of time for you and the client as you know the scenario is possible and has been validated by your team to quantify the exposure.

Incident Management: An identified security threat is currently present in the client's digital landscape. The Security Operations (SecOps) team has initiated an evaluation of the incident to assess its extent and potential impact. Quick and accurate assessment during this phase is critical, as it can mean the difference between a full-scale security breach and a straightforward containment response. Utilizing EIP, the Security Analyst can leverage insights about the threat profile, potential targets, and tangentially affected systems to rapidly pinpoint the appropriate next steps. This capability enables immediate identification of the attack's potential progress and the necessary countermeasures, such as system updates or configuration modifications, to halt the attack. In essence, this streamlines the time needed to investigate and address threats. As the Managed Detection and Response (MDR) Service Provider for the client, your team's Time To Respond (TTR) reduced, and effectiveness in neutralizing threats are significantly enhanced.

Threat Hunting: As your Threat Hunting team embarks on the preparation and collection stages, Epiphany serves as a pivotal tool. It underpins the hypothesis generation and compiles pertinent resources by delivering targeted insights into attack patterns associated with specific adversaries. By streamlining the aggregation and analysis of extensive data sets pertinent

Reveald has thoughtfully designed EIP to support Service Providers' branding needs by keeping the client relationship centered on you, the Service Provider, and greatly diminishing customers' inclination to purchase and self-operate the technology.

White-labeling enhances the value of your brand and fosters client loyalty.

to the client's environment and adversary behavior, Epiphany enhances the Threat Hunting process efficiency. This optimization effectively narrows down the duration of Threat Hunting endeavors by homing in on viable activities within the client's landscape, thus sharpening the investigative focus.

Business Usage Insights: Provided the client grants access to the insights from EIP, as a Service Provider, you will obtain a detailed view of the client's entire spectrum of assets. EIP integrates and analyzes data from systems and networks, offering a comprehensive understanding of the client's systems, applications, and operating environments. This detailed knowledge empowers you to refine the scope, enhance your value proposition, and budget more effectively for the services you offer to the client. Whether it's operational managed services, asset leasing, software asset management, telecommunications, or license management, as the Service Provider, you can engage in discussions with the client with a higher degree of precision and clarity.

Heterogeneous: In contrast to the common practices of many cyber industry vendors, EIP stands out as a vendor-agnostic wholistic exposure management platform. Reveald's EIP is designed to seamlessly integrate with an array of the client's existing solutions from major players like Microsoft, CrowdStrike, SentinelOne, Rapid7, Tenable, Qualys, Cisco, and Amazon among others. This eliminates the necessity for clients to overhaul their current technologies to see results. As the Service Provider, your role is to enhance the synergy between the client's existing technological solutions. The significance? You gain the advantage of extensive industry compatibility, enabling you to serve your clients more effectively without the need for intricate transition programs. Within just a week, you can start providing tangible value to your clients.

Real Results: The Cyber Security sector is currently inundated with an array of Exposure Management and Attack Path Mapping tools, often simply integrated as additional features within vendors' existing product suites. However, these tools often fall short in delivering tangible results to clients. At the forefront of this field, Reveald has not only introduced Exposure Management but also established itself as a global authority in executing Gartner's Continuous Threat & Exposure Management (CTEM) framework, translating it into real-world outcomes. With over four years of deep-seated experience, we comprehend the intricate

tapestry of skills, resources, processes, outputs, and technological components that are essential to confer substantial advantages to clients. By collaborating with Reveald, you gain the capacity to quickly turn your service offering into a productized, operational facet of your business, propelling profitable growth. This partnership alleviates the hazards associated with costly learning curves that stem from financial missteps, contractual oversights, and client relations pitfalls.

Data Protection: Built and proven for large scale complex client environments, EIP provides a secure architecture for protecting client's data. Apart from Roll Based Access (RBAC), encryption in transit and at rest, client's data is segmented with separate instances and is never in a shared space with other clients. This ensures there is no ability for one client to see another client's sensitive data.

Rapid Results: With EIP, you don't have to wait weeks or months for the results and value to your clients to occur. Due to the already trained learning models, within the first day of operations connected to the client's environment, you will have a results and tailored recommendations for your client.

Grow revenue and profit without risk: Should there be a need to bolster your internal capacity, Reveald stands ready to enhance your delivery workforce, allowing you to amplify your revenue swiftly while maintaining uninterrupted service. As your revenue escalates and your team matures, Reveald will gradually scale back its support. We commit to educating your personnel in the nuanced "art of delivery" for Risk Hunting, bolstering your in-house service delivery profitability. By leveraging Reveald's expertise, your service offerings have the potential to achieve margins exceeding 70% and client retention rates surpassing 95%.

Make it your own: Reveald has thoughtfully designed EIP to support Service Providers' branding needs by allowing the platform to be white labeled with either your logo alone or with your logo in conjunction with "powered by Epiphany Intelligence Platform." This feature keeps the client relationship centered on you, the Service Provider, and greatly diminishes their inclination to purchase and self-operate the technology. In essence, white labeling enhances the perceived value of your brand and fosters client loyalty.

+95%

"By leveraging Reveald's expertise, your service offerings have the potential to achieve margins exceeding 70% and client retention rates surpassing 95%."

EPIPHANY | INTELLIGENCE PLATFORM

Key Capabilities

Attack Path Analysis

The Epiphany Intelligence Platform harnesses advanced artificial intelligence algorithms to perpetually scrutinize and prioritize an extensive array of potential vectors that could transition an initial exposure into a consequential security incursion.

Limited Analysis

The capabilities of EIP to aggregate and decipher intricate data from a growing array of sources are continuously evolving. With each addition of new data sources, not only does the platform's potency amplify, but your billable services also see a corresponding increase.

Be Proactive

Integrating exposure data with cutting-edge intelligence on threats and capabilities casts a revealing light on the security breaches that can occur, and potential impacts cybercriminals could cause to your client's digital environment.

Targeted Remediation

With EIP you can leverage actionable intelligence with real-time recommendations for critical risk mitigation strategies that will substantially decrease your client's exposure to significant cybersecurity threats.

Objective Metrics

The Epiphany platform rigorously quantifies a multitude of objective metrics within an environment, including the severity and exploitability of vulnerabilities, the configuration and defensive states of devices, and identity access. It meticulously evaluates not just compliance levels against industry standards, but judges the effectiveness of implemented security controls, providing a data-driven foundation for security posture assessment and decision-making.

About Reveald

Reveald guides organizations along their journey from reactive to proactive defense. Reveald's AI-driven Epiphany Intelligence Platform™ empowers security teams to break free from existing reactive processes by leveraging Continuous Threat Exposure Management (CTEM), supported by the expertise to guide them on every step of the journey. Known for its innovative and proactive approach to cyber threats, the company is powered by a client-first approach, prioritizing risk mitigation and operational efficiency. To learn more, visit reveald.com.