CASE STUDY DOCUMENTATION

Explore Reveald's customer case studies to learn how Reveald transitions customers from reactive to proactive cybersecurity strategies.

--

Developed in Partnership with Our Clients

Produced and Maintained by Reveald Research and Development

TECHNICAL REFERENCE

REVEALD

THE FORCE MULTIPLIER FOR CYBERSECURITY

TABLE OF CONTENTS

REVEALD

Reveald's Epiphany Intelligence Platform Provides Essential Security Posture Information for Healthcare Organization M&A Due Diligence

INTEGRATIONS

CROWDSTRIKE Microsoft Active Directory RAPID7

Epiphany's findings allow healthcare organization to address cybersecurity issues of acquisition target pre-merger

SYNOPSIS

A not-for-profit healthcare organization has been caring for local communities since the founding of its first hospital in the late 1800's. With more than 20,000 team members, including employees, providers, and volunteers, the Healthcare Organization (HCO) has grown from its original one-hospital organization into a large not-for-profit community-based, locally owned health care system. The HCO's comprehensive system of healthcare serves patients in multiple cities and includes numerous inpatient care, primary care, virtual care, urgent care, and dedicated pediatric care and specialty services in over ten hospitals. It also includes affiliated physicians and medical associates and a wide range of community outreach programs in cities where it has a presence.

Reveald used the Epiphany Intelligence Platform to provide the HCO with adversarial assessments to provide information about the HCO's security status. Based on the positive results of the HCO's initial adversarial assessment, the HCO asked Reveald to perform an adversarial assessment on a hospital it was acquiring in order to understand its security posture prior to the acquisition.

CHALLENGE: NOT-FOR-PROFIT HEALTHCARE ORGANIZATION SEEKS CYBER-HYGIENE GUIDANCE FOR ACQUISITION TARGET

Reveald performed an adversarial assessment of a not-for-profit healthcare organization's (HCO) security posture using the Epiphany Intelligence

Use Cases

EVALUATE MERGERS & ACQUISITIONS
Thorough cybersecurity assessments for potential M&A activities, ensuring seamless integrations without compromising security and avoiding surprise operating expenses.

CYBER RESILIENCE
Design a cyber strategy across IT, IoT, and OT environments to eliminate attacker potential, improve resilience, and avoid breaches.

VULNERABILITY MANAGEMENT PRIORITIZATION AND OPTIMIZATION
Identify exploitable vulnerabilities in attack paths to reduce the number of vulnerabilities that need to be patched or resolved.

PRIVILEGED IDENTITY & ACCESS MANAGEMENT (PAM) AUDITING AND RISK IDENTIFICATION
Reduce the time and effort to identify and remedy PAM that likely lead to a cybersecurity incident or breach.

INCIDENT RESPONSE, RECOVERY, AND PREPARATION
Proactive strategies and reactive case data for swift incident management.

ASSET MANAGEMENT
Comprehensive tracking and understanding of systems and devices. Management of digital assets to ensure data integrity and value preservation.

NEUTRALIZE THREAT ACTORS
Rapidly identify systems a threat actor group will attack if they have the opportunity, including how the attack will occur and what actions are required to neutralize the issues.

EXECUTIVE REPORTING
Provide executive level communications on risk posture and recommendations for improvement.

Platform. The HCO was extremely happy with the information provided by the adversarial assessment and the guidance it provided to remediate potential security risks.

Moving forward, the HCO was acquiring a hospital to add to its portfolio of healthcare facilities. As part of integrating the hospital into their organization's environment, they wanted to understand the hospital's potential attack surface and inherent risks and they wanted to understand the risks of the new environment before bringing it into the HCO's clean environment. The HCO needed to meet regulatory requirements and wanted to understand what security and compliance remediation they needed to do to have a secure integration. In the post-merger haste to integrate, security can be forgotten about, which can lead to active attackers having a path in to the acquiring organization's critical resources. It was essential for the HCO to avoid this.

SOLUTION: EPIPHANY AND M&A

Security is an important part of a successful merger. Reveald uses the Epiphany Intelligence Platform to provide guidance to functionally influence three points in a merger and acquisition:

- Due Dilligence
- Final Terms
- Integration

DUE DILIGENCE

Reveald can help at every phase of technical due diligence prior to an acquisition. Understanding the attack surface, defensive posture, and exploitability of the infrastructure an organization is potentially acquiring is essential. Having visibility into these things can minimize unwanted surprises during integration, and it can prevent the core business network from inadvertently being exposed to attack paths within an acquired organization.

To assess an acquisition target, data can be uploaded from the target organization's security and IT assessment tools when the Reveald team is onsite, or the target organization can simply export and upload data to Reveald.

Once Reveald has the data, it begins to build and analyze potential attack paths within the target organization. This information can be used to understand the potential costs to remediate those paths and bring the target network up to the acquiring organization's security standards. Using the Epiphany Intelligence Platform, Reveald can also highlight where the target company may have operational failures in its configuration management, vulnerability

Epiphany is a risk reduction platform.

It enhances an organization's existing defensive security controls by providing an offensive perspective. Epiphany exposes the most likely attack paths to an organization's most critical IT assets and users, and then delivers actionable recommendations on how to remove them.

Epiphany finds hidden risks in an organization's environment that traditional scan tools can't. It also displays attack chains between isolated networks via domain relationships and exposed services.

management, or identity management by surfacing those issues through the target organization's own data sources.

FINAL TERMS

Using the technical information provided by the Epiphany Intelligence Platform, an organization can account for the cost of reducing exposure of the target organization's critical business objects. An acquiring organization can also understand the amount of effort required—from a time-and-materials perspective—to bring the target organization into alignment with existing policies. This provides the opportunity to capitalize remediation and be proactive in integration planning, instead of reacting to new problems discovered later during the integration of the target company.

INTEGRATION

Integration is a critical phase to complete an acquisition. It's also the one where most hidden costs are found. While it's potentially easy to account for and integrate processes and workflow, it's much harder to understand the effort needed to safely integrate and secure a once-remote network.

Traditionally this is achieved by putting a firewall between networks and methodically opening one service at a time to the remote environment. This process can take many months or even years in larger acquisitions and often results in misconfigurations and over-permissioning. The Epiphany Intelligence Platform can accelerate this by showing which services are safe to integrate without generating attack paths.

Epiphany uses its attack path knowledge and its awareness of the most critical exploitable conditions in both networks to guide the integration process, ensuring no inadvertent exploitable paths are created. Epiphany can use its data processing power to merge large complex data sets within both organizations' IT and security tools to track the progress of major high-risk projects such as identity and access granting, endpoint protection migration, firewall configuration changes, vulnerability reduction, and more.

RESULTS: ADVERSARIAL ASSESSMENT IDENTIFIES KEY ISSUES TO ADDRESS PRE-MERGER

Based on their pre-merger concerns as well as the success of the previous adversarial assessment performed by Reveald, the HCO engaged Reveald to use the Epiphany Intelligence Platform to perform an adversarial assessment of the target hospital. The assessment analyzed over 6,000 users and over 8,000 devices.

KEY AREAS OF EVALUATION

- Identity management (Active Directory and Azure AD)
- Patching and vulnerability management (Rapid7)
- Endpoint protection (CrowdStrike)

Epiphany uncovered many issues for the HCO to address prior to the merger, ensuring that their systems weren't impacted by new attack paths unintentionally introduced by the target hospital. Epiphany identified that the target hospital had poor security practices, including poor vulnerability management and permissions management. Additionally, Epiphany identified numerous non-admin users who had the ability to use remote desktop protocol (RDP) to directly access domain controllers. There were also a number of high-value identities logging into areas where they shouldn't be. And there were several attack paths leading into high value roles.

Epiphany identified the specific users, devices, and locations where these risks occurred and provided prioritized guidance on where and how to remediate each issue. This enabled the HCO to address the issues prior to integration,

thus protecting the HCO's existing infrastructure.

OTHER FINDINGS

- 1,500+ User accounts with passwords that hadn't been reset for more than 90 days. This included almost 20 domain admin accounts, some of which hadn't had their passwords reset in several years.
- 3,000+ Paths from various footholds to domain admins, enterprise admins, domain controls, high value systems, and other critical areas.
- 1,000+ Stale user accounts and over 800 stale computer accounts. A stale account is one that hasn't logged into the domain for more than 90 days.
- 250+ Paths from various footholds to domain admins, enterprise admins, domain controls, high value systems, and other critical areas.
- Vulnerabilities on Domain Controllers

Epiphany identified the specific users, devices, and locations where these risks occurred and provided prioritized guidance on where and how to remediate each issue. This enabled the HCO to address the issues prior to integration, thus protecting the HCO's existing infrastructure.

CONCLUSION: DON'T GO INTO MERGERS & ACQUISITIONS BLINDLY

If your organization is embarking on an M & A journey, Reveald and the Epiphany Intelligence Platform are with you every step of the way, from the moment your tech team arrives to assess a target organization through the day your systems are fully-merged.

Reveald's **Continuous Exposure Management 360° (CEM360°)** service leverages the Epiphany Intelligence Platform coupled with expert analysts from the Reveald Fusion Center to provide 24x7 cybersecurity vulnerability prioritization based on advanced attack graph analysis. This leads to business risk reduction through data integration and automated security analysis, validation, reporting, and guided resolution.

Reveald's experts work in partnership with its clients' teams to prioritize issues that are most likely to cause cybersecurity events across identity, configuration, and defensive controls. They continuously manage and tune the Epiphany Intelligence Platform, ensuring integrations with cybersecurity toolchains work flawlessly to generate the most valuable remediation information.

Environmental Protection Department Cyber Risk Program Mitigates Attacker Potential with Reveald's Epiphany Intelligence Platform

INTEGRATIONS

CROWDSTRIKE Microsoft Active Directory RAPID7 McAfee

In one day, the Reveald Epiphany Intelligence Platform detected Issues that would have taken a Year of manual effort to find—for just that one moment in time's risk conditions

SYNOPSIS

The Environmental Protection Department is a large enterprise with nearly 6,000 employees. It manages and conserves the water supply for an extremely large municipality, distributing over one billion gallons of clean drinking water to a population of nearly 19 million. It collects and treats 1.3 billion gallons of wastewater daily through a vast network of pipes, regulators, and pumping stations. Additionally, it protects the region's environment and regulates its air quality, hazardous waste, and noise.

Reveald was retained by the Environmental Protection Department to perform a cybersecurity risk assessment and recommend solutions and actions to take to prevent a disastrous data breach or ransomware attack. Reveald used its Epiphany Intelligence Platform to perform assessments and provide continuous monitoring and ongoing awareness, guidance, and recommendations on critical issues.

CHALLENGE

Cybersecurity is imperative for the Environmental Protection Department. Its critical infrastructure—particularly its water treatment facilities—are increasingly targets of nation-state adversaries and other threat actors. Device and account hygiene is essential for the agency's security.

Fearing an attack similar to the Colonial Pipeline ransomware attack that occurred in May 2021 and shut down Colonial Pipeline's systems for several days *(see sidebar, Ransomware Attack Holds Columbia Pipeline Hostage for Several Days),* the Environmental Protection Department needed to:

Use Cases

CYBER RESILIENCE
Design a cyber strategy across IT, IoT, and OT environments to eliminate attacker potential, improve resilience, and avoid breaches.

VULNERABILITY MANAGEMENT PRIORITIZATION AND OPTIMIZATION
Identify exploitable vulnerabilities in attack paths to reduce the number of vulnerabilities requiring patches and resolution.

NEUTRALIZE THREAT ACTORS
Rapidly identify systems a threat actor group will attack if they have the opportunity, including how the attack will occur and what actions are required to neutralize the issues.

EXECUTIVE REPORTING
Provide executive level communications on risk posture and recommendations for improvement.

PROGRAM REPORTING
Provide understanding of progress on success criteria for senior management.

ASSESS SECURITY PROGRAM EFFECTIVENESS
Provide objective evaluation of existing security measures, providing actionable feedback and optimization strategies.

CONTINUOUS ANALYSIS AND ANALYTICS
Show how changes in the environment will automatically remove or add new attack paths and provide recommendations.

- Lock down accounts to appropriate privileges and access.
- Remove unnecessary administration accounts.
- Identify vulnerable accounts.
- Identify and secure service accounts.
- Assess and validate polices for password resets and then reset or lock accounts.
- Identify stale devices in Active Directory.

COMPLICATIONS

To complicate their situation, the Environmental Protection Department is greatly short-staffed and under-resourced. They lacked the staffing to address these issues and needed a solution that would address their concerns in a timely manner.

SOLUTION

The Environmental Protection Department retained Reveald to use the Epiphany Intelligence Platform to perform continuous assessments and recommend solutions and actions to take to prevent a disastrous data breach or ransomware attack.

The Epiphany Intelligence Platform uses artificial intelligence to identify areas of material risk and prioritize them based on several factors such as ease of remediation, exploitability, and the value of a target to an organization's critical business functions. This empowers an organization's IT staff to take targeted action with minimal time investment.

Reveald deployed the Epiphany Intelligence Platform in the department's IT environments. Epiphany is uniquely designed to quickly and easily ingest an organization's infrastructure and security tools' data and telemetry. Epiphany was immediately up and running.

RESULTS

Using Epiphany, Reveald delivered immediate and continuous value. In one day Epiphany detected issues that would have taken a year of effort to discover if performed manually, including identifying zombie accounts and devices and device and password policy weaknesses. It identified rogue systems and assets that lacked security controls. And it highlighted unmanaged systems that exposed the Environmental Protection Department's networks to risk.

Epiphany provided the Environmental Protection Department with the information necessary to:

- Identify and prioritize remediation of attack paths to high value targets.
- Identify and prioritize remediation of vulnerabilities that provide

Ransomware Attack Holds Columbia Pipeline Hostage for Several Days

Colonial Pipeline moves oil from refineries to industry markets. Its pipeline is one of the largest and most vital oil pipelines in the U.S. Its shutdown affected consumers and airlines along the East Coast and was deemed a national security threat and was declared a national emergency by President Joe Biden.

The attack didn't actually compromise the operational technology that moves oil. Instead it involved multiple stages against Colonial Pipeline's IT systems. The attackers stole 100 gigabytes of data within the first two hours of the attack. Next the attackers infected Colonial Pipeline's IT network with ransomware that affected many computer systems, including billing and accounting. Concerned about the ransomware spreading, Colonial Pipeline had no choice but to shut down the pipeline.

Attackers accessed the Colonial Pipeline network through an exposed password for a VPN account, and that password was likely used for the VPN in another location and was compromised during a different data breach. Password reuse is a common problem because often users use the same password more than once.

Colonial Pipeline ended up paying the hackers a ransom of approximately $4.4 million to get a decryption key that the company's IT staff used to regain control of its systems. Six days after the initial intrusion and data theft, the company restarted pipeline operations. A few weeks later the Department of Justice recovered approximately $2.3 million from the attackers.

attackers with footholds in the environment.

- Remove unused or unnecessary devices and user accounts.
- Address issues with account permissions and passwords.
- Strengthen policies to improve security.

MOVING FORWARD

The Epiphany Intelligence Platform enabled the Environmental Protection Department to quickly understand exposure in its environment. It armed the department with decision intelligence to address issues and reduce exposure, all with the department's limited resources.

Using Epiphany's continuous monitoring, the Environmental Protection Department has ongoing awareness of critical issues. Epiphany provides the ability to determine the highest priorities on a day-to-day basis.

Reveald's security analysts meet with the Environmental Protection Department's IT staff on a weekly basis. The point of this meeting is for Epiphany analysts to scrutinize the Epiphany dashboard data and make recommendations to the Environmental Protection Department's IT staff on how best to perform offensive prevention and remediation efforts, which can vary from week to week. Epiphany's security analysts can quickly identify the top attack paths or vulnerabilities and recommend what the Environmental Protection Department's IT staff should work on.

On an ongoing basis, the Environmental Protection Department's IT staff makes special requests to pull data on particular groups or user types. For example, they may want to identify all the users that have rights to a domain controller so they can ensure those rights are being used appropriately. Or they may want to identify service accounts that are used for login, which creates a lot of vulnerability.

Armed with this information on a continuous basis, the Environmental Protection Department is able to remediate not just a large number of issues, but the most important issues that pose the greatest material risk to the organization.

The Environmental Protection Department is very pleased with the process and its results. Having continuous access to the data and Epiphany's vulnerability prioritization, along with guidance from Reveald's analysts has greatly accelerated the department's ability to stay ahead of material threats and has increased its ability to prioritize, remediated, and break attack paths.

CONCLUSION: ARE YOU FINDING ATTACK PATHS BEFORE ATTACKERS FIND THEM?

The Epiphany Intelligence Platform enhances defensive security controls by providing an offensive analysis. It identifies the most likely attack paths to your critical IT assets and users and delivers specific, actionable recommendations on how to remove them.

Reveald's Continuous Exposure Management 360° (CEM360°) service leverages the Epiphany Intelligence Platform coupled with expert analysts from its Fusion Center to work alongside your team to provide 24x7 cybersecurity vulnerability prioritization based on advanced attack graph analysis. This leads to business risk reduction through data integration and automated security analysis, validation, reporting, and guided resolution.

Reveald's team walks you step-by-step through deployment, integration, and training on the Epiphany Intelligence Platform and then work in partnership with your teams to prioritize issues that are most likely to cause cybersecurity events across identity, configuration, and defensive controls. Reveald's analysts continuously manage and tune the Epiphany Intelligence Platform, ensuring integrations with your cybersecurity stack work flawlessly to generate the most valuable remediation information.

Intel® Delivers Reveald's Epiphany Intelligence Platform to Top U.S. School District

INTEGRATIONS

TREND MICRO · Microsoft Active Directory · RAPID7 nexpose®

SYNOPSIS

Reveald collaborated with Intel® to bring the Epiphany Intelligence Platform's cybersecurity solutions to identify and enhance the to address critical vulnerabilities for one of the largest school districts in the U.S. With over 650 schools and more than 40,000 employees, it has some of the most critical assets to protect—the buildings and IT infrastructure supporting over 300,000 students.

Intel is one of the most prominent companies in the world, developing technology solutions that impact every corner of the planet. With revenues of over $60 billion, it provides complete technology solutions in every industry.

Reveald is an Intel® market-ready solution partner. Intel sells the Epiphany Intelligence Platform to different companies it has relationships with. Through its relationship with Intel, the school district let Intel know it was concerned about the cyber posture of its buildings and schools and the potential risks that existed between its building systems and campus IT systems. Intel recommended that the school district consider the Epiphany Intelligence Platform.

As a state-of-the-art cybersecurity and exposure management platform, Epiphany capitalizes on powerful hardware and cloud resources to function optimally. Intel, being a leading hardware technology manufacturer, offers products and libraries that can seamlessly enhance Epiphany's performance. Integrating Epiphany with Intel's advanced hardware provides numerous benefits (see box on next page).

CHALLENGE

Driven by the desire to reduce energy and operational costs, the school district was undergoing digital transformation of its building automation systems. Its leadership team wanted to place an emphasis on management controls and monitoring its buildings' mechanical and electrical systems such as HVAC, lighting, power, fire, and security systems. However, the challenge was in gaining the benefits of improving building automation systems while at the same time managing and monitoring cyber risks.

Use Cases

CYBER RESILIENCE
Design a cyber strategy across IT, IoT, and OT environments to eliminate attacker potential, improve resilience, and avoid breaches.

VULNERABILITY MANAGEMENT PRIORITIZATION AND OPTIMIZATION
Identify exploitable vulnerabilities in attack paths to reduce the number of vulnerabilities requiring patches and resolution.

PRIVILEGED IDENTITY & ACCESS MANAGEMENT (PAM) AUDITING AND RISK IDENTIFICATION
Reduce the time and effort to identify and remedy PAM that likely lead to a cybersecurity incident or breach.

INCIDENT RESPONSE, RECOVERY, AND PREPARATION
Proactive strategies and reactive case data for swift incident management.

ASSET MANAGEMENT
Comprehensive tracking and understanding of systems and devices. Management of digital assets to ensure data integrity and value preservation.

NEUTRALIZE THREAT ACTORS
Rapidly identify systems a threat actor group will attack if they have the opportunity, including how the attack will occur and what actions are required to neutralize the issues.

EXECUTIVE REPORTING
Provide executive level communications on risk posture and recommendations for improvement.

PROGRAM REPORTING
Provide understanding of progress on success criteria for senior management.

ASSESS SECURITY PROGRAM EFFECTIVENESS
Provide objective evaluation of existing security measures, providing actionable feedback and optimization strategies.

With over 650 schools and buildings, the school district suspected there were risks they were unaware of because of the many systems and interconnections used by its platforms. This created a large threat landscape for attack. The scope of the school district network needing assessment included a combination of systems and technologies: over 120,000 computers, more than 1.2 million users, and over 300,000 devices. The school district did not have the tools nor the systems in place to comprehensibly inspect the environment for vulnerabilities, so based on Intel's recommendation they decided to use the Epiphany Intelligence Platform.

The Epiphany Intelligence Platform is uniquely positioned for organizations as large in size and scope as the school district because large environments are where Epiphany functions best. The larger and more complex the environment, the more likely that numerous small mistakes have been made, and it's the small mistakes that allow an attacker to gain full control over an environment. Epiphany focuses on thousands or millions of minutiae easily overlooked by IT analysts and analyzes large, complex landscapes that would be impossible for a single person or even an IT staff to analyze in a realistic time.

SOLUTION

The Epiphany Intelligence Platform uses modeling, heuristics, and analysis in real-time, building a database of all potential devices and user-based attack surfaces (on-prem, cloud, and remote) open to exploitation. Epiphany creates actionable intelligence in a meaningful and relevant manner, with the goal of finding exploits before there is a need

intel.

Epiphany's Performance Enhanced With Intel® Advanced Hardware

Performance and Real-Time Analysis with Intel® Xeon® Scalable Processors
Designed for high-performance computing needs, the Xeon Scalable processors can handle the rigorous data processing demands of Epiphany's AI models and data processing. This ensures real-time analysis, rapid threat identification, and immediate proactive remediations, improving the overall cybersecurity stance of a customer.

AI & Machine Learning Capabilities with Intel® Deep Learning Boost (Intel® DL)
Boost Epiphany's learning components use complex deep learning approaches and can be accelerated using Intel DL Boost, which provides enhanced AI inference acceleration. Faster learning and prediction cycles translate to quicker models that provide better remediation.

Enhanced Data Security with Intel® Software Guard Extensions (Intel® SGX)
This technology helps protect selected code and data from disclosure or modification. As Epiphany can be deployed to cloud or on-premises, security of code is critical as it is some of the most sensitive in the customer environment. Integrating Epiphany with Intel SGX ensures that sensitive data processed by the platform remains secure and tamper-proof.

Optimal Data Storage and Retrieval with Intel® Optane™ SSD
For platforms like Epiphany that constantly manage vast amounts of data, the speed of data storage and retrieval is critical. Intel Optane SSDs, with their high throughput and low latency, ensure that Epiphany can access and process data almost instantaneously while deployed within a customer data center.

Network Performance with Intel® Ethernet Network Adapters
To ensure that Epiphany communicates quickly, securely, and efficiently across networks, Intel's advanced network technology can be leveraged to enhance connectivity, reduce bottlenecks, and ensure consistent data flow from Epiphany's data sources and the customer applications.

to analyze and respond. The risk analysis then determines targets of opportunity along attack paths, identifies an attacker's transition points, explores potential outcomes, and sets prioritization based on business impact.

Epiphany follows a series of methodologies, drawing from industry best practices and its own internal tactics, techniques, and procedures (TTP's), to analyze the technical risks present in an environment.

Epiphany provided dedicated resources to accomplish tasks such as connecting Epiphany to the school district's data sources (such as vulnerability scanners), Active Directory services, and endpoint protection data, and identifying targets of material value to the functionality of the school district's infrastructure.

Epiphany evaluated potential points of exposure through automated and manual means within the school district network to determine if there were opportunities for an attacker to gain footholds into the school district's IT environment. Epiphany's adversarial assessments provided actionable reporting data that the school district was able to use to address critical vulnerabilities in a prioritized mitigation strategy, including:

- Identification, guidance, and prioritization for remediation of critical vulnerabilities on computers that allow for attackers to gain a foothold in the environment.
- Identification of high-value identities exposed on vulnerable computers that can allow an attacker to directly escalate to a higher level of privilege in the environment.
- Identification, guidance, and prioritization for remediation of attack paths starting from vulnerable computers and devices leading to high-value targets.
- Identification of permission-based misconfigurations in Active Directory that enable attack paths from footholds to high-value targets, with prioritization and guidance for their remediation.

CONCLUSION

The school district found several critical vulnerabilities within the first hour of using the Epiphany Intelligence Platform and continues to use Epiphany to ensure its lines of business applications are secure and its security tools are performing as expected.

Epiphany provided the school district with adversarial assessments of its environments, which identified attack paths between facilities and IT systems. This included analyzed and prioritized attack paths across 1M+ Active Directory accounts and more than 200,000 devices.

AFTER RECEIVING ITS INITIAL RESULTS, THE SCHOOL DISTRICT HAD ENTHUSIASTIC FEEDBACK:

"Honestly, we would not have been able to find and mitigate several very high-level vulnerabilities in the platforms and line of business systems we targeted. We were able to work with Epiphany to identify a litany of issues that we and our vendors who support the products on a consulting basis did not know existed. If we let those issues stay in place, we would have unwittingly exposed ourselves to several severe exploitations that could do a lot of damage."

Epiphany identified threats and provided actionable recommendations so the school district could begin addressing its vulnerabilities immediately. For each of Epiphany's recommendations, specific servers, hosts, and users were

identified along with exactly what needed to be upgraded, removed, or changed. This essentially became an actionable worklist for the school district to use to proactively address its vulnerabilities before an attack could occur.

With Epiphany, the school district found an affordable and efficient way to manage and report on cybersecurity risks across multiple existing platforms, bridging the information gaps in those systems. This resulted in immediate critical risk remediation through better awareness and prioritization.

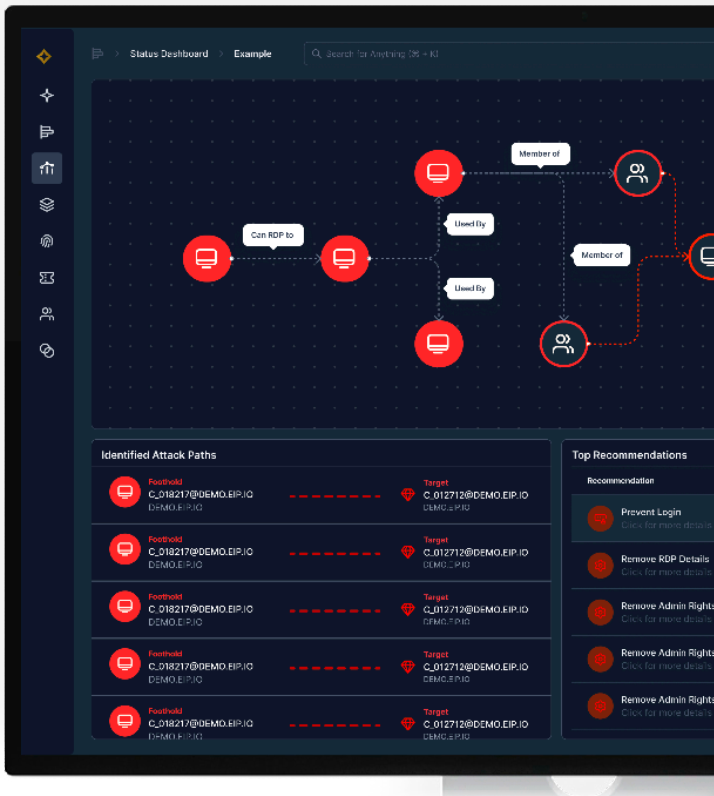
EPIPHANY | INTELLIGENCE PLATFORM

Epiphany is a risk reduction platform

Epiphany is a risk reduction platform. It enhances an organization's existing defensive security controls by providing an offensive perspective. Epiphany exposes the most likely attack paths to an organization's most critical IT assets and users, and then delivers actionable recommendations on how to remove them.

Epiphany finds hidden risks in an organization's environment that traditional scan tools can't. It also displays attack chains between isolated networks via domain relationships and exposed services.

Epiphany uses algorithms to identify areas of material risk, then prioritizes them based on several factors such as exploitability and how important a target is to the critical function of an organization. In addition to prioritizing the risks to an organization, several remediation recommendations are provided along attack paths. An IT team can take targeted action with minimal time investment on where and how to fix the problems.



Global Industrial Company (GIC) Protects Occupational Technology Systems from Security Breaches With Reveald's Epiphany Intelligence Platform

INTEGRATIONS

Microsoft Active Directory · Qualys. · CLAROTY · paloalto NETWORKS · SentinelOne

The Epiphany Intelligence Platform Identifies Attack Paths Potentially Enabled Through Computers in the GIC's Break Rooms

SYNOPSIS

A global industrial company (GIC) operating in over 80 countries with over 20,000 employees and over 200 factories needed to understand its security posture. Its ecosystem spans a broad array of holdings, technologies, and investments including public and private companies, world-class building solutions, performance materials, real estate, and next-generation solar technology.

Using the Epiphany Intelligence Platform, Reveald identified a number of issues, including several computers located in breakrooms that had the potential to enable attack paths leading to the compromise of high-value targets. Based on Reveald's guidance, the GIC was able to remediate these issues in its IT environments and its factories' OT environments.

CHALLENGE

A global industrial company (GIC) initially approached Reveald at the annual Black Hat USA cybersecurity conference. They were impressed with the Epiphany Intelligence Platform, saying they'd never seen a tool do attack path analysis like Epiphany. The GIC initially asked Reveald to use the Epiphany Intelligence Platform to help them prioritize their attack surface vulnerabilities that needed to be patched as the focus of a proof-of-concept endeavor. The GIC includes IT and operational technology (OT) environments in its over 200 factories.

Reveald initially performed an adversarial assessment on the GIC's IT side by incorporating the GIC's vulnerability scanner, Active Directory, and endpoint protection. The GIC was very impressed with the results as it immediately

Use Cases

CYBER RESILIENCE
Design a cyber strategy across IT, IoT, and OT environments to eliminate attacker potential, improve resilience, and avoid breaches.

VULNERABILITY MANAGEMENT PRIORITIZATION AND OPTIMIZATION
Identify exploitable vulnerabilities in attack paths to reduce the number of vulnerabilities requiring patches and resolution.

PRIVILEGED IDENTITY & ACCESS MANAGEMENT (PAM) AUDITING AND RISK IDENTIFICATION
Reduce the time and effort to identify and remedy PAM that likely lead to a cybersecurity incident or breach.

INCIDENT RESPONSE, RECOVERY, AND PREPARATION
Proactive strategies and reactive case data for swift incident management.

ASSET MANAGEMENT
Comprehensive tracking and understanding of systems and devices. Management of digital assets to ensure data integrity and value preservation.

NEUTRALIZE THREAT ACTORS
Rapidly identify systems a threat actor group will attack if they have the opportunity, including how the attack will occur and what actions are required to neutralize the issues.

EXECUTIVE REPORTING
Provide executive level communications on risk posture and recommendations for improvement.

PROGRAM REPORTING
Provide understanding of progress on success criteria for senior management.

ASSESS SECURITY PROGRAM EFFECTIVENESS
Provide objective evaluation of existing security measures, providing actionable feedback and optimization strategies.

identified account exposures and attack paths to critical systems. This was data no other tool was able to provide. Their representative said, “if Epiphany can do the same thing on the OT side in their manufacturing factories, it’s a huge win for us and something no other platform could do.”

This led to Reveald increasing the adversarial assessment from 10,000 endpoints in the corporate side to include all manufacturing factories on the OT side.

SOLUTION

For this adversarial assessment, Reveald used the Epiphany Intelligence Platform to analyze:

- The GIC’s Active Directory and vulnerability data from Qualys.
- CISCO and firewall data on the IT side.
- Claroty data on the OT side.

RESULTS

The Epiphany assessment reviewed firewalls and their rules, over 10 networks, many Claroty devices, and direct paths from the IT network to the OT network. Reveald identified a number of issues:

- Multiple attack paths led from the IT side into the OT’s manufacturing environment. Attack paths that originate in the IT environment and move into the OT environment can compromise the OT environment and put the GIC’s manufacturing facilities at risk of cyber breaches.
- Over 200 domain admin and enterprise admin sessions were not on domain controllers.
- Numerous Kerberoastable users with paths to domain admins.
- Over 200 computers with vulnerabilities from the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Catalog. Many of these are ones that produce footholds.
- A number of kiosks (computers in accessible areas such as break rooms) that enabled attack paths that could lead to the compromise of high-value assets.

For each of the issues that were identified, the Epiphany Intelligence Platform provided prioritized guidance on how and where to remediate the situation. This guidance made it possible for the GIC’s IT staff to focus on the issues with the greatest likelihood for material impact, thus focusing resources for the greatest results.

CONCLUSION

The Epiphany Intelligence Platform is Reveald’s advanced exposure management software platform that enables organizations to quickly and efficiently identify, prioritize, and mitigate vulnerabilities and attack paths. It exposes the most likely attack paths to an organization’s most critical IT assets and users, and then delivers actionable recommendations on how to remove them.

Epiphany finds hidden risks in an organization’s environment that traditional scan tools can’t. It also identifies and displays attack paths between isolated networks via domain relationships and exposed services.

Epiphany uses artificial intelligence to identify areas of material risk, then prioritizes them based on several factors such as exploitability and how important a target is to the critical function of an organization. In addition to prioritizing the risks to an organization, several remediation recommendations are provided along attack paths. An IT team can take targeted action with minimal time investment on where and how to fix the problems.

Major Metropolitan Transportation Agency Improves Cyber Resilience Using Reveald's Epiphany Intelligence Platform

INTEGRATIONS

Microsoft Active Directory · tenable Nessus · cisco

The Epiphany Intelligence Platform leverages existing infrastructure and security tools to analyze complex IT and OT environments and prioritize actions to significantly strengthen security posture.

SYNOPSIS

Reveald was retained by a global sustainable development Professional Services firm to perform an adversarial assessment in a large Transportation Agency. The objective was to evaluate the agency's cybersecurity posture and provide guidance on specific actions to improve cyber resilience. Reveald's team set up Reveald's Epiphany Intelligence Platform to analyze over 200 networks in 12 different physical locations in less than a week, saving tens of thousands of dollars over other solutions. The analysis included a combination of Transportation Agency systems and technologies used by tens of thousands of people and computers.

The Transportation Agency is in one of the top 15 municipalities in the world, with a transportation network covering over 2,500 square miles, serving a population of more than 7 million people. The thousands of miles of transportation infrastructure extends beyond the city limits into other adjacent municipalities and includes partner agencies for buses, bridges, and tunnels across multiple municipalities.

The Professional Services firm—which includes over 16,000 designers, advisors, and experts working across 140 countries—is a prime contractor for the Transportation Agency. It has been at the forefront of ambitious and challenging design and engineering for over 70 years.

CHALLENGE

The Professional Services firm needed to identify gaps between the

Use Cases

CYBER RESILIENCE
Design a cyber strategy across IT, IoT, and OT environments to eliminate attacker potential, improve resilience, and avoid breaches.

VULNERABILITY MANAGEMENT PRIORITIZATION AND OPTIMIZATION
Identify exploitable vulnerabilities in attack paths to reduce the number of vulnerabilities requiring patches and resolution.

PRIVILEGED IDENTITY & ACCESS MANAGEMENT (PAM) AUDITING AND RISK IDENTIFICATION
Reduce the time and effort to identify and remedy PAM that likely lead to a cybersecurity incident or breach.

INCIDENT RESPONSE, RECOVERY, AND PREPARATION
Proactive strategies and reactive case data for swift incident management.

ASSET MANAGEMENT
Comprehensive tracking and understanding of systems and devices. Management of digital assets to ensure data integrity and value preservation.

NEUTRALIZE THREAT ACTORS
Rapidly identify systems a threat actor group will attack if they have the opportunity, including how the attack will occur and what actions are required to neutralize the issues.

EXECUTIVE REPORTING
Provide executive level communications on risk posture and recommendations for improvement.

PROGRAM REPORTING
Provide understanding of progress on success criteria for senior management.

ASSESS SECURITY PROGRAM EFFECTIVENESS
Provide objective evaluation of existing security measures, providing actionable feedback and optimization strategies.

Transportation Agency's current control systems designs, architecture, and industry best practices and to understand the effectiveness of its existing security systems. It also needed to identify upgrades necessary to improve the Transportation Agency's existing security systems.

The Transportation Agency's network comprises one of the nation's largest bus fleets and more subway and commuter rail cars than all other U.S. transit systems combined. It needed to understand how to protect its bus command and control systems, customer systems, and back-office applications from cyber threats.

Ensuring the functionality and safety of an organization's networks is essential. As a way of understanding how to protect its command-and-control systems, customer systems, and back-office applications from cyber threats, the Transportation Agency required a threat, vulnerability, and risk assessment (TVRA). They were concerned with network design as well as the assets or devices on its networks and wanted to determine the extent of its attack surface and highlight any areas of concern that could affect support systems in its physical assets.

The complexity of the interconnectivity between the way the Transportation Agency's systems operate made it difficult for any one person or even any one group—such as a group of IT managers—to readily understand the complete IT and OT environment and its risks and vulnerabilities.

The Professional Services firm retained Reveald to perform a vulnerability analysis and identify attack paths within its networks. Reveald uses its Epiphany Intelligence Platform to perform adversarial assessments that evaluate the cybersecurity posture of an organization and provide guidance on specific actions to improve cyber resilience.

COMPLICATIONS

Because the Transportation Agency is a very diverse organization, understanding its entire network infrastructure was very complex. Each organization has its own projects, management chains, and organizational structure. There are different management groups or administrative groups for Windows AD (Active Directory), endpoints, network layers, firewalls, and so on. People working in one group may not understand the implications of changes to network connectivity or firewall settings for other groups. The impact of a change in one group can be profound—it can affect the entire organization.

Another complexity the Transportation Agency experienced was limited visibility into active remote systems. With COVID requiring many people to work from home at the time, this was a new problem not seen before.

Fast Analysis Means Fast Protection of Valuable Assets

Performed manually, just the Active Directory portion of Epiphany's analysis would have taken many weeks to perform, and it would have been a static, one-time analysis. Reveald completed a full analysis in under 24 hours.

With Epiphany, IT staff have the ability to do the analysis on-demand, at any time.

Prioritization of Risks Enables Targeted Response

Epiphany uses artificial intelligence to identify areas of material risk and prioritize them based on several factors such as ease of remediation, exploitability, and value of the target to an organization's critical business functions. This empowers the organization's IT staff to make targeted remediation with minimal time investment on where and how to fix the problems.

SOLUTION: EPIPHANY ASSESSMENTS

Epiphany performed assessments in two key areas: a perimeter analysis of OT networks and a network analysis of the Transportation Agency's IT environments.

OT NETWORKS PERIMETER ANALYSIS

Epiphany scanned the OT perimeter IP spaces to catalog all the devices that communicate external to the OT network. It evaluated exposed communications ports and protocols as well as services, applications, gateways, and remote access devices that are externally accessible. Reveald brought the results of these evaluations into Epiphany to identify and evaluate attack paths that could lead into the OT environment.

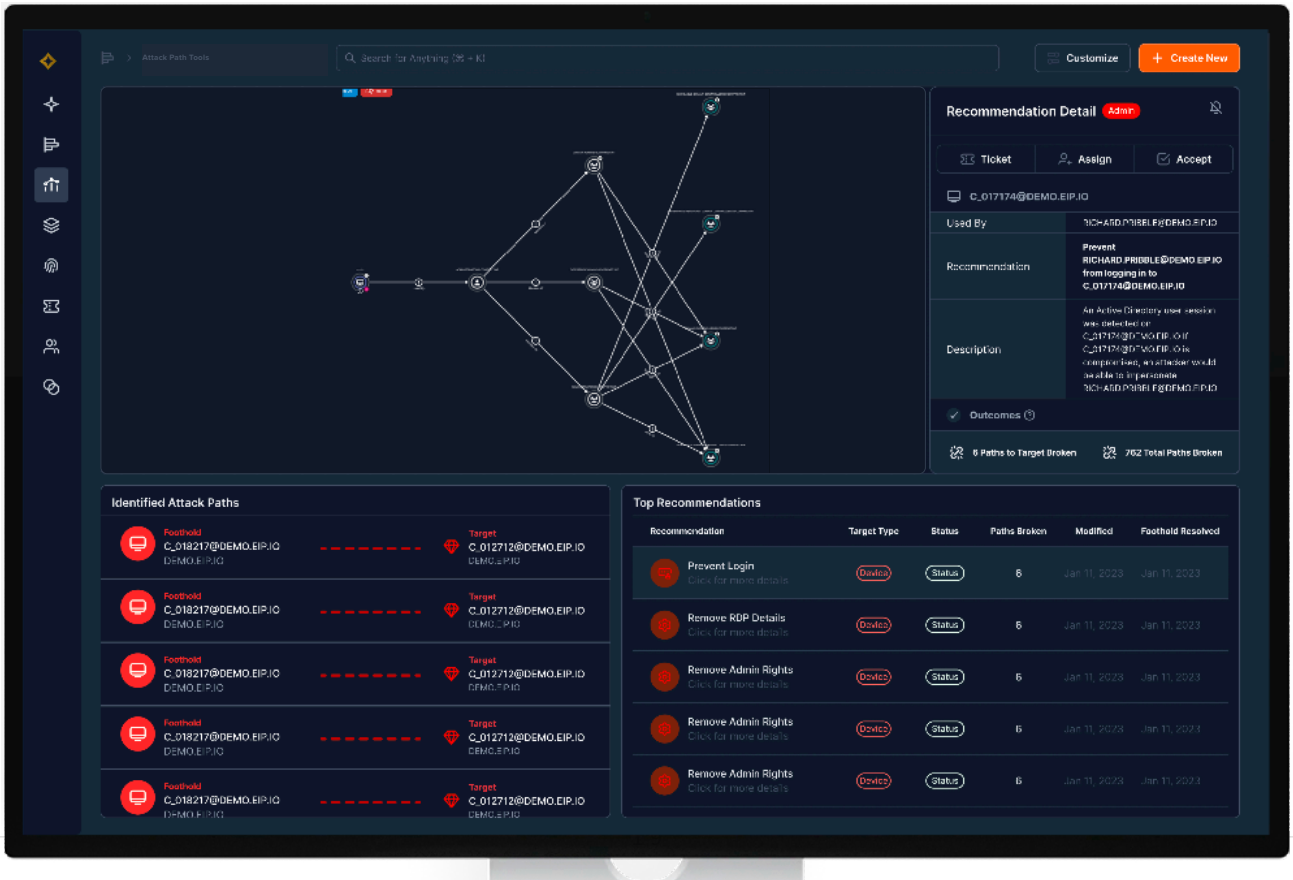
IT ENVIRONMENT NETWORK ANALYSIS

Epiphany gathered the Transportation Agency's specific business risks, threat matrix, and impact matrix. It then deployed its assessment collectors and analyzed the organization's data sources, which included its vulnerability scanner, directory services, and routing/switching/firewall data. Epiphany then identified high-value targets that could align with the objectives of a real-world attacker.

Armed with this information, Epiphany analyzed the Transportation Agency's environments for potential entry and pivot points from its general network environment into the OT environment. The scope of this analysis encompassed a combination of systems and technologies. It included tens of thousands of users and computers in over 200 networks in 12 different physical locations.

RESULTS

In under 24 hours, Epiphany found over **7,000 attack opportunities by leveraging attack path learning capabilities.** For each of these attack opportunities, Epiphany provided remediation recommendations and identified specific



servers, hosts, and users along with exactly what needed to be upgraded, removed, or changed. This essentially became an actionable worklist for the Transportation Agency to use to proactively address its vulnerabilities before an attack occurred.

To demonstrate how an attacker could move from the Transportation Agency's IT environment into its various OT environments, Epiphany created detailed maps of the organization's OT network in relation to its IT environments in order to catalog, understand, and assess the accessible OT network attack surface.

Epiphany proved that multiple attack paths existed that allowed an adversary to gain a foothold in the IT environment and move to a position of control over an OT asset through control of user sessions. Epiphany demonstrated several ways this goal could be achieved by an adversary and provided actionable strategic and tactical recommendations on the optimal remediations to implement to break the identified attack chains.

CONCLUSION

The Epiphany Intelligence Platform, Reveald's AI-driven enterprise solution, is the first of its kind. It gathers attack data from thousands of devices and provides prioritized attack path analysis. It identifies the most likely attack paths to your critical IT assets and users and delivers specific, actionable recommendations on how to remove them.

Reveald's Continuous Exposure Management 360° (CEM360°) subscription service leverages Epiphany coupled with expert analysts from Reveald's Fusion Center to provide 24x7 cybersecurity vulnerability prioritization based on advanced attack graph analysis. This leads to business risk reduction through data integration and automated security analysis, validation, reporting, and guiding resolution.

Reveald's experts work in partnership with its clients' teams to prioritize issues that are most likely to cause cybersecurity events across identity, configuration, and defensive controls. They continuously manage and tune Epiphany, ensuring integrations with cybersecurity toolchains work flawlessly to generate the most valuable remediation information.

Top 5 Global Telco Licenses Reveald's Epiphany Validation Engine

With over 50,000 employees and operations in 20+ countries, one of the largest telecommunications providers in the world sought a robust cybersecurity solution to enhance its security posture.

SYNOPSIS

The global telco, one of the largest telecomunications providers in the world, provides telecommunications products and services. It provides traditional fixed-line service, Wi-Fi networks, data, hosted services , and IT services. With over 50,000 employees, the company also owns TV networks and has acquired—and runs—several telecommunications, cable TV, Internet, and Wi-Fi network companies is over 20 countries

CHALLENGE

The global telco sought a robust cybersecurity solution to enhance its security posture. The company wanted to proactively protect its sensitive data from cyber attacks rather than respond to attacks after they occur.

SOLUTION

After evaluating various options, the global telco decided to license Reveald's Epiphany Validation Engine. They were drawn by its unique features and capabilities.

The global telco was impressed with a number of key aspects:

- Real attack emulation
- Scalability of assessments
- Positive outcomes

REAL ATTACK EMULATION

The telco was particularly impressed by the Epiphany Validation Engine's ability to trigger actual controls in real time through attack emulation. The Epiphany Validation Engine is a cloud-based simulation platform that tests the strength of an organization's cyber controls through simulated cyber attack. The telco recognized the importance of realistic scenarios in

Use Cases

VULNERABILITY MANAGEMENT PRIORITIZATION AND OPTIMIZATION
Identify exploitable vulnerabilities in attack paths to reduce the number of vulnerabilities requiring patches and resolution.

CYBERSECURITY CONTROLS VALIDATION
Evaluation and testing of the measures and protocols implemented within an organization to ensure their effectiveness.

COMPLIANCE ENABLEMENT
Implement processes and systems to ensure compliance with industry standards to mitigate risks and achieve organizational objectives.

REMOTE WORKFORCE VALIDATION
Verify the security and efficiency of remote access systems and employee practices while optimizing productivity in remote work environments.

CONTINUOUS EVALUATIONS
Show how changes in the environment will automatically remove or add new attack paths and provide recommendations.

RISK ASSESSMENT AND REPORTING
Systematically analyze potential threats and vulnerabilities, to facilitate informed decision-making and prioritize risk mitigation efforts within an organization.

OPERATIONALIZE MITRE ATT&CK
Integrate the MITRE framework into cybersecurity operations to improve threat detection, response, and mitigation strategies, improving overall security posture.

3RD PARTY SUPPLY CHAIN POSTURE
Optimize and improve the efficiency of processes and relationships with external suppliers to minimize costs and maximize overall performance.

SECURITY INVESTMENT OPTIMIZATION
Strategically allocate resources to mitigate risks, protect assets, and enhance resilience against potential threats and vulnerabilities. security measures, providing actionable

cybersecurity and appreciated the distinction between a simulator and an emulator. The live demonstration showcased the effectiveness of the solution in avoiding false positives, a critical factor in enterprise-level cybersecurity.

CONSULTATIVE APPROACH

Reveald provided consultative solutions tailored to the telco's specific needs. This approach helped address their unique challenges, showcasing Reveald's commitment to the telco's success in implementing effective cybersecurity measures.

POSITIVE OUTCOMES

Trust was solidified through the positive outcomes delivered by the Epiphany Validation Engine. The telco recognized the value not only in improving their services but also in enhancing the skills of their incident responders within their organization. The positive results demonstrated the practical impact of the Epiphany Validation Engine on the telco's cybersecurity objectives.

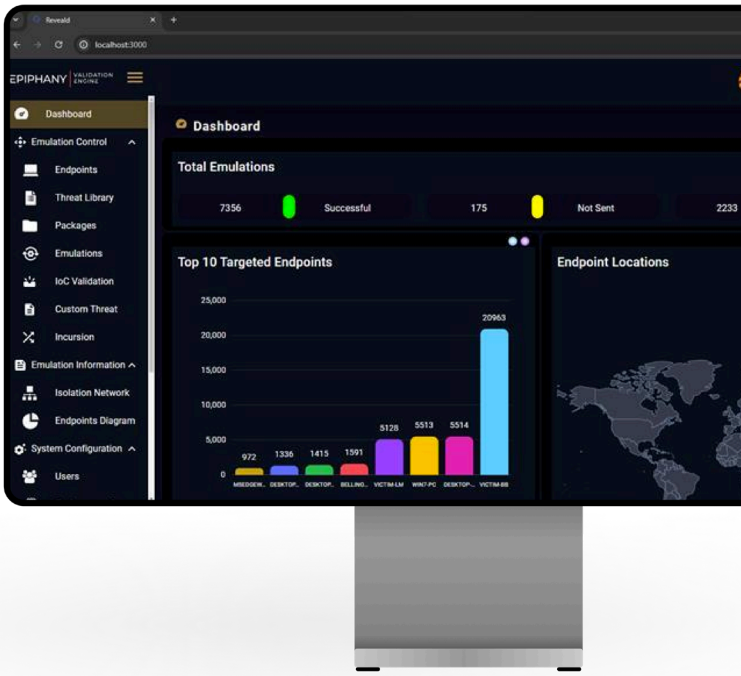
About the Epiphany Validation Engine

At the network architecture level, the Epiphany Validation Engine is installed as an Amazon Web Services (AWS) instance on the cloud. It is given access to an agent within an organization that holds all security controls—the golden image. Highlights of the platform are described below.

EPIPHANY | INTELLIGENCE PLATFORM

CALLBACK MONITORING AND VALIDATION

The Epiphany Validation Engine creates custom call-back artifacts that can be a killswitch or malware download. These callbacks are monitored and the platform's orchestrator validates and determines if the callbacks arrive successfully or not. This functionality allows for the validation of mandatory playbooks that exist in the security orchestrator.



ADVANCED NETWORK EVATION

The Epiphany Validation Engine can force the evasion of cybersecurity network elements based on sandboxing and hashes, through a shipping and control algorithm based on asymmetric encryption. This forcefully verifies the correct operation of advanced security solutions that validate each artifact that travels through the network even when they possess advanced obfuscation and encryption mechanisms.

EXECUTION RESULTS

Each package and artifact is aligned to the MITRE framework and the attack life cycle, allowing for greater visibility of the attack sent. It is also possible to validate if the artifact evaded network security, and if its execution was successful at the endpoint.

RESULTS

As a result of the deal inked between Reveald and the global telco, the Epiphany Validation Engine is driving various use cases for the organization, aligning with their security objectives:

- Security operations center (SOC) fine tuning. The Epiphany Validation Engine facilitates the fine-tuning of SOC policies, enhancing th e efficiency and effectiveness of the telco's security operations.
- Cybersecurity investments optimization. The Epiphany Validation Engine's technology is a key element in optimizing the telco's existing cybersecurity solutions, justifying the investment through tangible and appealing returns on investment (ROI).
- Incident response (IR) implementation. The Epiphany Validation Engine provides continuous validation of service level agreements (SLAs) for IR, ensuring preparedness and effectiveness during security incidents.
- Custom threat campaigns for governance, risk and compliance (GRC). The Epiphany Validation Engine's scripting module enhances the creation and execution of custom threat campaigns. This is crucial for GRC objectives.
- Cybersecurity playbook validation. The Epiphany Validation Engine validates cybersecurity playbooks across the telco's five data centers, ensuring consistency and effectiveness in response strategies.

CONCLUSION

The combination of practical demonstrations, responsive support, consultative solutions, and positive outcomes played a pivotal role in establishing trust with the customer. This trust was instrumental in securing the global telco's deal with Reveald.

The plan is to expand into Reveald's Epiphany Intelligence Platform to implement a continuous threat exposure management (CTEM) program with a subscription for risk hunting. Reveald is doing continuous training and certifying the telco's team on attack emulation.

Let us know what your needs are for measuring and evaluating your company's cybersecurity solutions. Contact us at https://reveald.com/#contact.

Reveald's Endpoint Defense Management 360° Helps City of Aurora Respond to Cybersecurity Events

INTEGRATIONS

CROWDSTRIKE Microsoft Active Directory Qualys.

The City of Aurora, Colorado enhances cybersecurity and receives expert guidance on risk minimization and vulnerability prioritization with Reveald's Endpoint Defense Management 360° (EDM360°), Reveald's Continuous Exposure Management 360° (CEM360°), and the Reveald Fusion Center

AURORA'S CISO ON CEM360°'S OUTSTANDING RESULTS

"Reveald is a partner, not a paycheck. They jumped into action when our previous MSSP left us in a bad situation and their quick response and professionalism ensured our transition was seamless. Since beginning our relationship with Reveald, our EDR tenant and process has matured significantly. So when I saw CEM360°, it was a no-brainer. CEM360° provided value within the first week of POV, finding exploit paths that had been unknowingly introduced into our environment by well-intentioned administrators.

"CEM360°'s reporting and visualization of attack paths augmented my team's threat hunting capability overnight by providing real-time, actionable information. Unlike other vendors I've used in the past, Reveald has built the platform to provide understandable reporting that explains the threat in detail and provides clear guidance on how to fix the problem. Our IT teams can now visualize complex attacks and close the holes before they become a threat. It's like having a pen tester on my team that never sleeps!"

--TIM MCCAIN, CHIEF INFORMATION SECURITY OFFICER, CITY OF AURORA

Use Cases

CYBER RESILIENCE

Design a cyber strategy across IT, IoT, and OT environments to eliminate attacker potential, improve resilience, and avoid breaches.

VULNERABILITY MANAGEMENT PRIORITIZATION AND OPTIMIZATION

Identify exploitable vulnerabilities in attack paths to reduce the number of vulnerabilities that need to be patched or resolved.

PRIVILEGED IDENTITY & ACCESS MANAGEMENT (PAM) AUDITING AND RISK IDENTIFIC ATION

Reduce the time and effort to identify and remedy PAM that likely lead to a cybersecurity incident or breach.

INCIDENT RESPONSE, RECOVERY, AND PREPARATION

Proactive strategies and reactive case data for swift incident management.

ASSET MANAGEMENT

Comprehensive tracking and understanding of systems and devices. Management of digital assets to ensure data integrity and value preservation.

NEUTRALIZE THREAT ACTORS

Rapidly identify systems a threat actor group will attack if they have the opportunity, including how the attack will occur and what actions are required to neutralize the issues.

EXECUTIVE REPORTING

Provide executive level communications on risk posture and recommendations for improvement.

SYNOPSIS

With a population of 399,000, the city of Aurora, Colorado spans 164 square miles and is Colorado's third largest city. Just minutes away from Denver International Airport, the city includes four school districts and eight campuses of higher learning.

The city's government includes over 4,000 employees across twenty-two distinct business units. The information technology (IT) department works with city departments to provide leading-edge technology to position the city of Aurora as a leader in the use of technology in local government. The IT department oversees citywide networking, telecom, servers, desktop support, technology planning, and cyber security. It manages over 6,000 endpoints (physical devices that connect to a network system such as computers, virtual machines, embedded devices, mobile devices, and servers).

To protect Aurora's network and endpoints, the city brought in Reveald to enhance its cybersecurity and provide expert guidance and advanced protection from malicious cyberattacks for all agencies in the city.

CHALLENGE

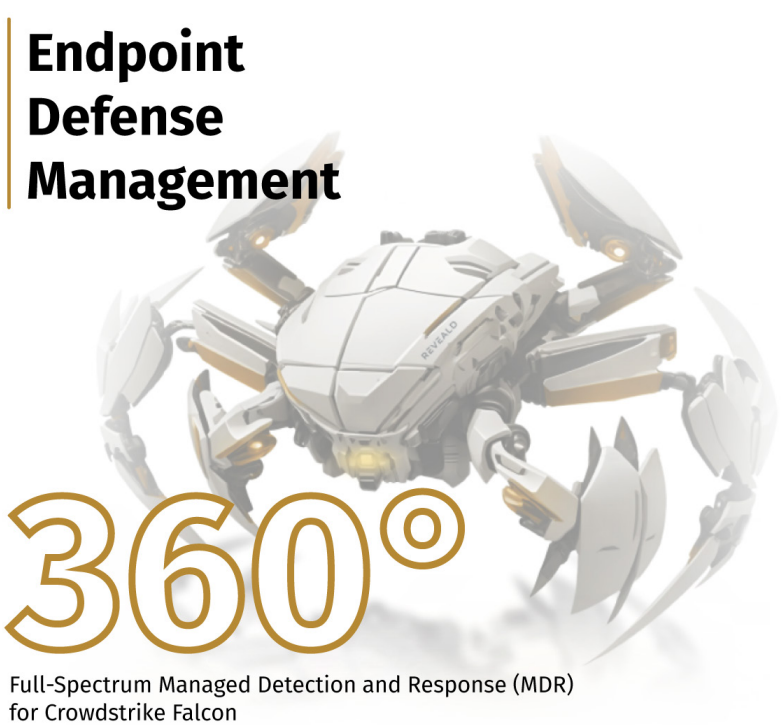
The city of Aurora was using CrowdStrike Falcon Complete for endpoint protection of its 6,000+ endpoints, real-time threat detection, and proactive threat hunting and was interested in an enhanced service solution to provide support for its CrowdStrike Falcon Complete platform.

SOLUTION

Aurora's IT department chose Reveald's Endpoint Defense Management 360° (EDM360°) subscription service and the Reveald Fusion Center to work with the CrowdStrike team to provide a complete turnkey experience. EDM360° provides managed detection and response (MDR) for CrowdStrike Falcon Complete users. It reduces costs by consolidating tools and vendors, with full visibility across a client's full set of Falcon modules. Its white glove service manages deployment, configuration, tuning, and optimization of the Falcon environment, minimizing the attack service

The experts in Reveald's Cyber Fusion Center deliver proactive management, configuration, monitoring, and hands-on response to cyber threats, in close collaboration with the CrowdStrike Falcon Complete and Security Operations teams.

Because Reveald and CrowdStrike together deliver a complete solution, Aurora was confident that EDM360°'s features combined with the Fusion Center team would provide the level of cybersecurity service and support the city required.



Full-Spectrum Managed Detection and Response (MDR) for Crowdstrike Falcon

The experts in Reveald's Cyber Fusion Center deliver proactive management, configuration, monitoring, and hands-on response to cyber threats, in seamless collaboration with CrowdStrike Falcon Complete.

RESULTS

Using a consistent and predictable onboarding approach, Reveald's client success team held weekly onboarding meetings with Aurora's IT department. One of the key benefits of the engagement is that the IT department has consistent contact with Reveald team members. Reveald's client success team ensures that relationships are formed and that everything works well throughout the engagement and surpasses expectations. By ensuring Aurora has a relationship with a Reveald client support manager willing to meet at hours convenient to Aurora's IT department, the city was confident that issues and unexpected events would be handled with remarkable responsiveness.

Once onboarding was complete, Aurora's IT department began working with Reveald's Fusion Center team and the combined group moved to bi-monthly or monthly meetings, depending on Aurora's needs.

Reveald's Fusion Center team provides 24/7 hands-on response to cyber threats in close collaboration with the CrowdStrike Falcon Complete team. Throughout the engagement, and to the present day, the Reveald Fusion Center team delivers measurements and key results against the city of Aurora's organizational objectives. Additionally, whenever things occur that need extra attention, Aurora can contact its Reveald client success manager (CSM) for a meeting and receive immediate attention and results, and the Fusion Center team is always happy and willing to spend whatever time necessary to address the city's events, often going above and beyond.

At different points during the engagement, the city experienced escalated events. Reveald's Fusion Center team partnered with Aurora's IT team on the research, resolution, and strategy for responding to these events. The city has been using EDM360° and working with the Fusion Center team for over a year and Reveald continues to provide services to the city in any way necessary for endpoint management, defense, and alerts.

NEXT STEPS

As a result of the successful EDM360° engagement, the Aurora's IT department worked with Reveald to do an on-site proof of value (PoV) analysis to demonstrate the effectiveness of a continuous threat exposure management (CTEM) program delivered via Reveald's Continuous Exposure Management package, CEM360°.

CEM360° leverages Reveald's Epiphany Intelligence Platform and expert analysts from the Reveald Fusion Center to provide CTEM around-the-clock, 24/7. This service is based on attack graph analysis, leading to business risk reduction outcomes by ingesting and aggregating data from a variety of sources, automated security analysis, validation, reporting, and guided resolution. The PoV went extremely well and the city of Aurora is embarking on a new and expanded relationship with Reveald as it begins implementing CTEM with CEM360°.

CrowdStrike® Partnership Enhances Reveald's Subscription Services

AVALIABLE NOW

CrowdStrike Marketplace

CrowdStrike® extends the successful partnership by adding the Epiphany Intelligence Platform to the CrowdStrike Marketplace.

SYNOPSIS

Launched in 2011, CrowdStrike is a multi-billion dollar cybersecurity company. It provides cloud workload and endpoint security, threat intelligence, and cyberattack response services. It has also been involved in the investigations of several high-profile cyberattacks. As a leader in cybersecurity, CrowdStrike is widely recognized for delivering top-notch cybersecurity technologies and services, setting the standard for innovation and effectiveness.

Reveald launched in 2021 as a provider of managed security services for mid- to large-sized enterprises. Reveald's initial focus was on providing end-to-end management of legacy endpoint security solutions, removing an expensive burden for large, complex organizations.

Since Reveald launched in 2021, it has transitioned from a tactical service provider to a strategic security partner. This brought opportunities for new, higher-value services and Reveald embarked on a mission to help its customers achieve mature security operations, moving from highly reactive processes to a more proactive and predictive state.

In 2022 Reveald incorporated CrowdStrike Falcon LogScale into its family of service offerings, allowing Reveald to expand beyond managed detection and response (MDR) into managed security operations center (SOC) services.

Reveald also saw the power of the Falcon data and APIs. By tapping into Falcon for endpoint detection and response (EDR) telemetry, asset metadata, and vulnerability data from Falcon Spotlight, Reveald was able to deliver an entirely new solution for continuous threat exposure management (CTEM).

CHALLENGE

While Reveald's teams are experts at deployment, configuration, and management of endpoint protection and other solutions, they encountered challenges in scaling their team to deliver real-time investigation and response for their clients. As Reveald began to expand its offerings and customer base, they identified challenges they needed to overcome:

- **Lack of visibility.** Legacy tools provided a very narrow view of the assets and activities within an organization, limiting their ability to find assets, and to identify and understand threats quickly.
- **Poor control.** In order to improve security, Reveald needed the ability to deploy, manage, and configure security controls remotely, across the organization. Positive outcomes
- **Scale.** As Reveald's customer base expanded, they quickly realized that the legacy tools they were using didn't provide the necessary capabilities to automate and scale their operations in a cost-effective manner.

SOLUTION

A large public-sector organization hired Reveald to help execute its multi-agency migration from a legacy endpoint protection solution to CrowdStrike Falcon. As a result of this effort, Reveald saw that the simplicity and open APIs provided by the Falcon platform would make it easier to scale operations and manage its expanding customer base. To make things even better, CrowdStrike provided an easy pathway for Reveald's team of analysts to become experts in the Falcon platform.

Based on this positive experience, Reveald partnered with CrowdStrike Falcon Complete to develop and deliver joint managed services, where Reveald's Fusion Center team provides white glove service and day-to-day management in close collaboration with Falcon Complete, which provides 24x7 threat hunting, investigation, and real-time response at scale.

Reveald incorporated two key CrowdStrike products into its suite of subscription service offerings: CrowdStrike Falcon Complete and CrowdStrike Falcon LogScale.

- **CrowdStrike Falcon Complete** is a full suite of CrowdStrike's managed endpoint threat and identity protection offerings with expert monitoring and remediation. It is the industry's only surgical remediation capable of carrying out the entire response, including full cleanup and restoration without costly reimaging or downtime. Falcon Complete's continuous platform management, agent maintenance, and rigorous control configuration and optimization leads to a deep understanding of a client's environment. Falcon Complete is a key part of Reveald's Endpoint Defense Management 360° (EDM360°, described below).
- **CrowdStrike Falcon Logscale** elevates the CrowdStrike Falcon platform with a centralized log management strategy that focuses on deriving insights from log data and helping organizations easily access, ingest, store, and analyze the client's critical and always-growing amount of information. Falcon Logscale is integral to Reveald's Cyber Defense Management 360° (CDM360°, described below).

Reveald's subscription service plans are built on the Reveald Epiphany Intelligence Platform and provide services from expert analysts in Reveald's Cyber Fusion Center, in conjunction with CrowdStrike Falcon Complete and Crowdstrike Falcon LogScale:

- **Reveald Endpoint Defense Management 360° (EDM360°)** provides managed services for CrowdStrike Falcon Complete, which provides managed detection and response (MDR). Reveald's Fusion Center experts act as a liaison to the client and deliver proactive management, onboarding, planning, configuration, optimization, monitoring, triage, investigation, and hands-on response to cyber threats in close collaboration with the Falcon Complete team.
- **Reveald Cyber Defense Management 360° (CDM360°)** provides managed security operations powered by CrowdStrike Falcon LogScale. Reveald's Fusion Center analysts deliver triage, investigation, and response to cyber threats, as well as management, monitoring, and tuning.

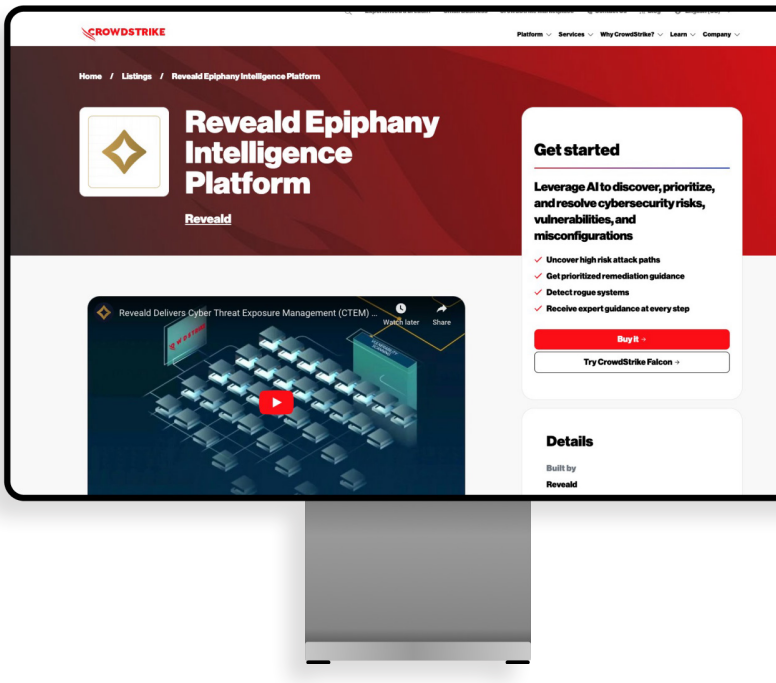
REVEALD EPIPHANY INTELLIGENCE PLATFORM AVAILABLE FOR PURCHASE ON THE CROWDSTRIKE MARKETPLACE

Due to the overwhelming success of the CrowdStrike/Reveald partnership, CrowdStrike added Reveald's Epiphany Intelligence Platform to the CrowdStrike Marketplace. This highly-revered online cybersecurity marketplace offers customers a streamlined way to discover, try, and buy security offerings that reduce risk and eliminate complexity.

Potential clients can easily discover, buy, and integrate Epiphany with the AI-native CrowdStrike Falcon XDR platform to help them identify and understand the risks that can cause a material impact.

The inclusion of Epiphany in this marketplace broadens Reveald's reach and also provides CrowdStrike customers with a streamlined process to enhance their security posture directly through their existing CrowdStrike accounts.

Being a part of the CrowdStrike Marketplace is a tremendous opportunity for Reveald because of the exposure it provides and the ease in which potential customers can find, try, and then buy products such as the Epiphany Intelligent Platform.



CROWDSTRIKE MARKETPLACE SOLIDIFIES THE REVEALD/CROWDSTRIKE PARTNERSHIP

"Our collaboration with CrowdStrike is more than just a partnership. It is a testament to our shared vision of making advanced, predictive cybersecurity accessible to all organizations. The Epiphany Intelligence Platform's availability on the CrowdStrike Marketplace signifies a leap forward in our commitment to empowering businesses with the innovation tools they need to navigate the complex cybersecurity landscape and stay ahead of threats. We are dedicated to continuous innovation and providing our clients with the most effective solutions to navigate the complex cybersecurity landscape."

RESULTS

Partnering with CrowdStrike empowered Reveald to deliver a comprehensive set of white glove security solutions for its customers, at a scale that would have been unimaginable before CrowdStrike. Since 95% of Reveald customers are also CrowdStrike customers, this is an outstanding opportunity for both companies.

Clients benefit from this partnership as well. When CrowdStrike and Reveald work together, with CrowdStrike providing technology and Reveald providing service, customers get a better exposure management outcome.

Key benefits:

- **Visibility.** Falcon and LogScale give Reveald's team easy access to deep and comprehensive context around assets and behaviors across their clients' networks, and to predict future attacks.
- **Control.** Falcon empowers Reveald to take necessary actions to proactively ensure that security controls are in place and optimized.
- **Scalability.** Falcon Complete allows Reveald to seamlessly scale operations, focusing on their key areas of strength while relying on CrowdStrike's expert threat hunters and security analysts to understand and act against threats as they emerge.

Reveald specializes in larger, more complex , geo-located organizations. In partnership with CrowdStrike, Reveald is the only company that has the ability to deliver such a complete MDR solution. Other companies provide pieces of the MDR puzzle, but none of them provides the breadth and depth of coverage.

CONCLUSION

Reveald is watching closely as CrowdStrike delivers expanded extended detection and response (XDR) offerings and looks forward to having the chance to achieve deeper visibility and response actions across its portfolio.

The availability of Reveald's Epiphany Intelligence Platform on the CrowdStrike Marketplace opens up a new channel for organizations to access its advanced CTEM solutions. This integration allows CrowdStrike customers to maximize their investment in the Falcon platform by consolidating their security solutions purchases, thereby reducing risk and enhancing operational efficiency.

ABOUT REVEALD'S SUBSCRIPTION SERVICES

MANAGED SECURITY OPERATIONS CENTER WITH CYBER DEFENSE MANAGEMENT 360°

Reveald's CDM360° subscription service allows organizations to force-multiply the success and outcomes from their CrowdStrike Falcon LogScale™ implementation with CDM360°. Organizations reduce risk and benefit from full program management and reporting with Reveald's world class Fusion Center and Epiphany technology platform.

CDM360° provides managed security operations powered by CrowdStrike Falcon® LogScale.

The experts in Reveald's Cyber Fusion Center deliver triage, investigation, and response to cyber threats, as well as management, monitoring, and tuning. Built on the Epiphany intelligence platform, CDM360° gives organizations a fast path to mature endpoint protection, and a clear path to predictive defense.

CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM) WITH CONTINUOUS EXPOSURE MANAGEMENT CEM360°

Reveald's CEM360° leverages the Epiphany Intelligence Platform coupled with expert analysts from the Reveald Fusion Center to provide 24/7 cybersecurity vulnerability prioritization based on advanced attack graph analysis. This

leads to business risk reduction through data integration and automated security analysis, validation, reporting, and guided resolution.

Expert analysts from Reveald's Fusion Center work in partnership with clients' teams to prioritize issues that are most likely to cause cybersecurity events across identity, configuration, and defensive controls. They continuously manage and tune the Epiphany Intelligence Platform, ensuring integrations with cybersecurity tools work flawlessly to generate the most valuable remediation.

Continous Exposure Management

Epiphany finds hidden risks in an organization's environment that traditional scan tools can't. It also displays attack chains between isolated networks via domain relationships and exposed services. Epiphany uses AI-powered algorithms to identify areas of material risk, then prioritizes them based on several factors such as exploitability and how important a target is to the critical function of an organization. In addition to prioritizing the risks to an organization, several remediation recommendations are provided along attack paths. IT teams can take targeted action with minimal time investment on where and how to fix the problems.