EPIPHANY SYSTEMS

USE CASE

Responding to a Critical Microsoft Vulnerability

CUSTOMER INDUSTRY	ATTACK SURFACE	SOLUTIONS
Healthcare	Over 100K endpoints	Epiphany Intelligence Platform™ and Epiphany Scout™

Summary

Microsoft disclosed a critical domain controller vulnerability that could result in an unauthenticated attacker taking complete control of all Active Directory identity services. The customer immediately asked:

> "In my siloed, complex environment, how do I find all the domain controllers that have this vulnerability, how do I know if they're vulnerable, and how can I tell if they're already affected?"

The customer needed to look at both shared and business unit-controlled data sources—across its entire organization—to determine exposure and risk. To do this, querying APIs and comparing data might seem like a fairly simple task, but that process is fraught with potential false positives and other errors. That could result in a time-consuming risk assessment, leaving the organization exposed to attack.

Leveraging Risk Hunting with the Epiphany Intelligence Platform, the customer was able to answer critical questions, confidentially assess risk, and act quickly.

RISK HUNTING ACTIVITY

- Conducted impact-focused analysis of current risk posture.
- Connected data across the enterprise to answer key risk-related questions.
- Asked state-related questions about the IT environment.
- Reduced time to surface risk-related answers.
- Mitigated and reduced risks, improving overall organizational risk posture.
- Communicated action plan to executive team.
- Provided empirical evidence to support decision tree.

EPIPHANY ADVANTAGES

- Developed to answer business risk-related questions with quantifiable data.
- Ability to ingest nearly any data source or enterprise platform and increase risk awareness and visibility.
- Rapid deployment for organizations of any size—in cloud, on-site, or hybrid environments.
- No disruption to operations—data ingestion is agent-less.

Challenge

The customer had multiple organizational silos, each maintaining its own Active Directory structure and tools. A central security team was responsible for assessing enterprise-wide risk, yet they could not fully see or assess this risk.

Despite a highly capable, well-funded security organization, the customer could not quickly or confidently determine their risk posture, which resulted in prolonged risk exposure.

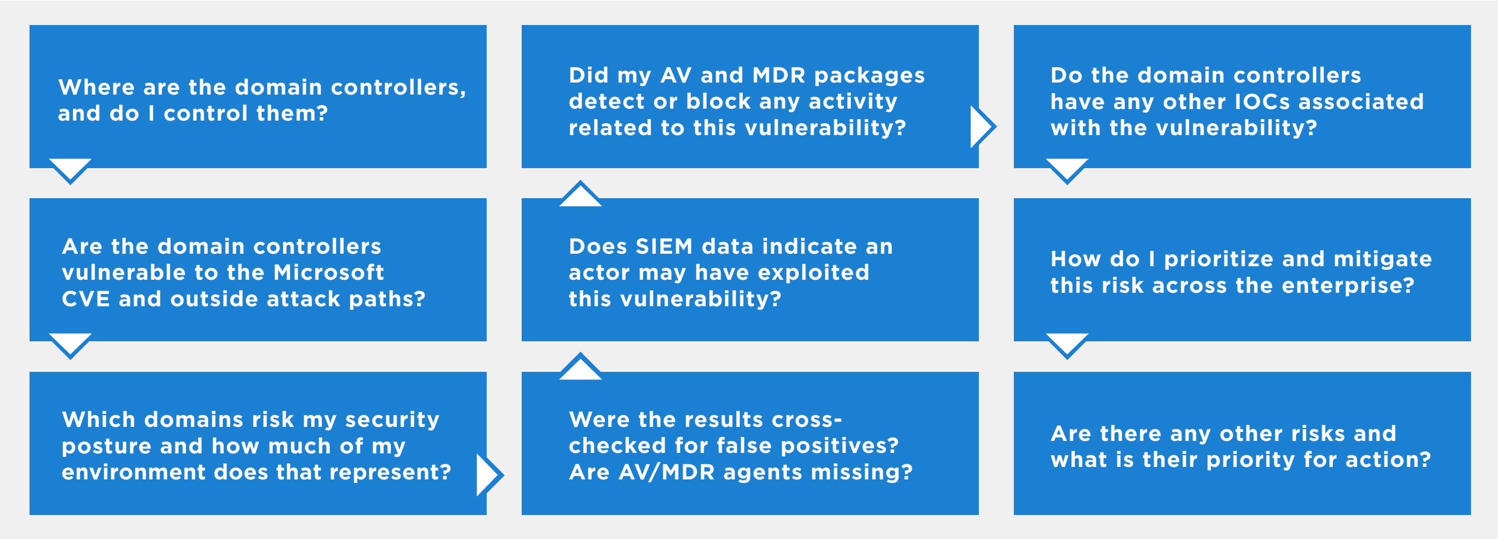
To assess its Active Directory vulnerabilities, the customer conducted a costly manual analysis of multiple data points. Given the task size and complexity however, this approach did not provide the necessary level of assurance.

To more accurately determine if any domain controllers were exposed—and how that might affect its risk posture— the customer decided they needed a different solution. That solution would have to query and unify enterprise-wide data, in near real-time, across multiple tools and data silos.

Solution

The company deployed the Epiphany Risk Hunting platform. Epiphany ingested data from across the organization, including endpoint protection suites, vulnerability scans, Active Directories, and session data sets. Epiphany analyzed both the IT environment and business risks associated with the critical Microsoft vulnerability. In near real time, Epiphany then produced the insights needed for immediate action to mitigate the vulnerabilities.

Epiphany answered the following questions:



Where are the domain controllers, and do I control them?

Are the domain controllers vulnerable to the Microsoft CVE and outside attack paths?

Which domains risk my security posture and how much of my environment does that represent?

Were the results cross-checked for false positives? Are AV/MDR agents missing?

Does SIEM data indicate an actor may have exploited this vulnerability?

Did my AV and MDR packages detect or block any activity related to this vulnerability?

Do the domain controllers have any other IOCs associated with the vulnerability?

How do I prioritize and mitigate this risk across the enterprise?

Are there any other risks and what is their priority for action?

Outcome

Epiphany worked closely with the customer to ensure greater awareness of risks—new and old—and helped the customer act quickly on those risks to avoid adverse impacts.

Epiphany reduced a task that had taken >120 hours of manual analysis down to 30 seconds of automated processing.

Epiphany earned the trust of the customer's security team to become the organization's primary source of risk knowledge and truth.

Awareness powers protection.

Contact us today to get started with Epiphany.

Contact Us