Predict, Explain, Retain – Data Analysis for Better Security

Getting Real About Practical Uses of AI for Cybersecurity and SecOps Teams

The Obligatory Skynet Slide

The Security Industry needs Efficiency and Productivity

58% say the security team is too busy fighting critical incidents to take a preventative approach to reduce their organizations exposures [1]

73% believe their organization would be more successful at defending against threats if they could devote more resources to preventive security [1]

Reaction

- Respond and scramble
- Resource isolation
- Steps after an attack
- Living through an attack

Vs

Prevention

- Anticipate and control
- Resource alignment
- Steps before
- Prevents successful attacks

[1] *Source: A commissioned study of 825 IT and cybersecurity professionals conducted by Forrester Consulting on behalf of Tenable, May 2023*

tenable

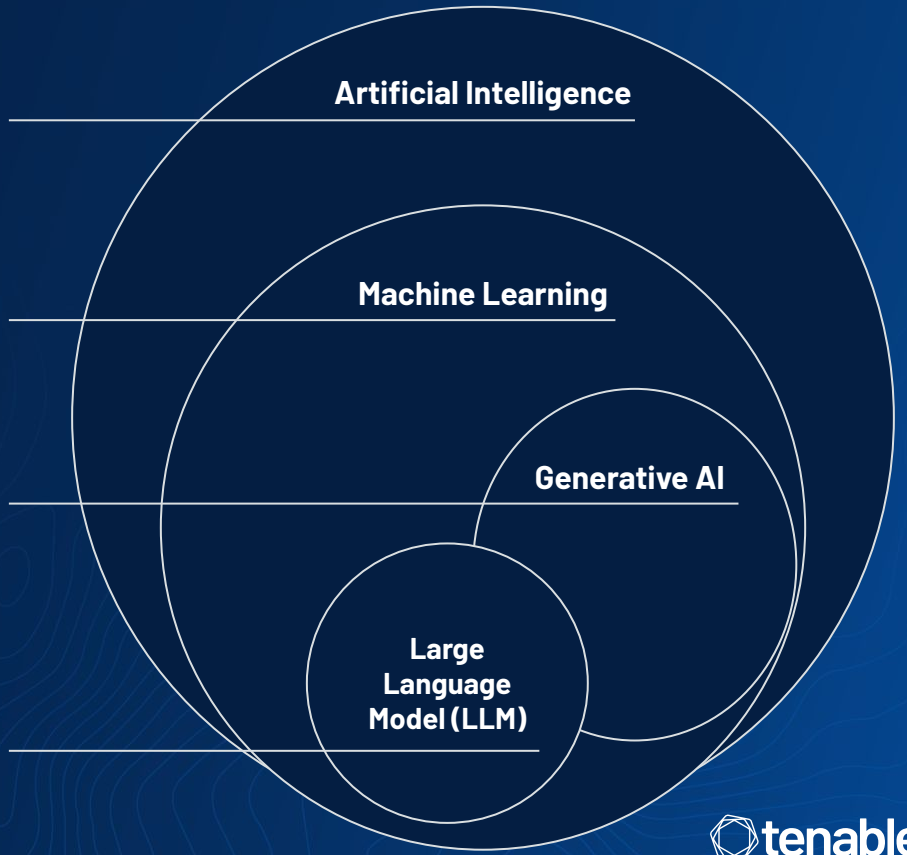
It's Not About SkyNet, It's All About Levels for AI

Artificial intelligence (AI) discipline of applying advanced analysis and logic-based techniques, including machine learning (ML), to interpret events, support and automate decisions and to take actions.

Machine Learning (ML) is a purely analytical discipline. It applies mathematical models to data to extract knowledge and find patterns that humans can miss.

Generative AI (GenAI) learns about artifacts from data and generates innovative new creations that are similar to but don't repeat the original

Large Language Model (LLM) is a type of machine learning model that can perform a variety of natural language processing (NLP) tasks such as generating and classifying text, answering questions in a conversational manner, and translating text from one language to another.



tenable

FINDING ANOMALIES IN PATERNS

Tenable has been a leader in AI-based cybersecurity

Vulnerability Priority Rating February 2019	**OS Prediction** January 2020	**Predictive Scoring** October 2020	**Gen AI Research Tools** April 2023	**Identity Exposure** June 2023
ML-based algorithms identify vulnerabilities most likely to be exploited in the next 28 days, analyzing each vulnerability daily to predict the likelihood of an exploit actually being used against it.	ML-based algorithms predict an unauthenticated asset's operating system via host response to TCP packet data to improve assessment and inventory accuracy.	ML-based algorithms predict an asset's risk from limited, unauthenticated scan data using data derived from authenticated scans and exposure characteristics of similar assets.	Four new tools developed by Tenable Research that create efficiencies in processes such as reverse engineering, code debugging, web app security and visibility into cloud-based tools.	Several identity-aware features that harness the power of artificial intelligence (AI) and machine learning to provide a unified view of all user identities and entitlement risks, whether on-prem or in the cloud.

tenable

AI Benefits to Efficiency and Effectiveness

PREDICT

Leverage ML to automate the identification of threats, exploits and the likelihood of attack for vulnerabilities, misconfigs and code flaws

EXPLAIN

Gen AI and LLMs are ideal to translate complicated technical data into more human-readable content for quicker and more accurate decision making

RETAIN

Security practitioners want to stay on the hunt for threats and flaws, rather than focusing on mundane manual tasks and long-term training engagements

tenable

AI Benefits to Efficiency and Effectiveness

PREDICT

Leverage ML to automate the identification of threats, exploits and the likelihood of attack for vulnerabilities, misconfigs and code flaws

EXPLAIN

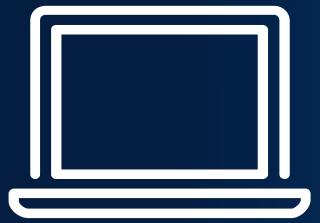
Gen AI and LLMs are ideal to translate complicated technical data into more human-readable content for quicker and more accurate decision making

RETAIN

Security practitioners want to stay on the hunt for threats and flaws, rather than focusing on mundane manual tasks and long-term training engagements

tenable

Normalization and Contextualization



Traditional IT Devices

Vulns = CVEs

CVSS 0 - 10

Web Applications

Vulns = SQL Injection

Cloud/AD Configuration

Vulns = Compliance check

Which is the greater risk? CVSS 8.2 *vs.* **SQL Injection rated "High"** *vs.* **KMS configuration fails policy check**

Machine Learning Automates Data Analysis

- Tenable Vulnerability Priority Rating (VPR) is calculated using:
  - 11 threat intel data sources
  - ~130 individual data points/categories
- Factored against over 220,000 CVEs =

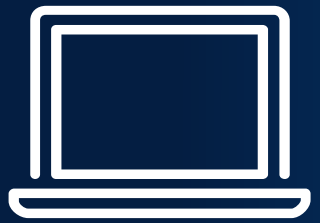
  ~28 Million data points to review
- Process repeats every ~8 hours

Data Gathering and Normalization

Contextualization and Analysis

tenable

Normalization and Contextualization



Traditional IT Devices

Vulns = CVEs

VPR = 9.2
ACR = 7

AES = 827

Web Applications

Vulns = SQL Injection

VPR = 7.5
ACR = 10

AES = 901

Cloud/AD Configuration

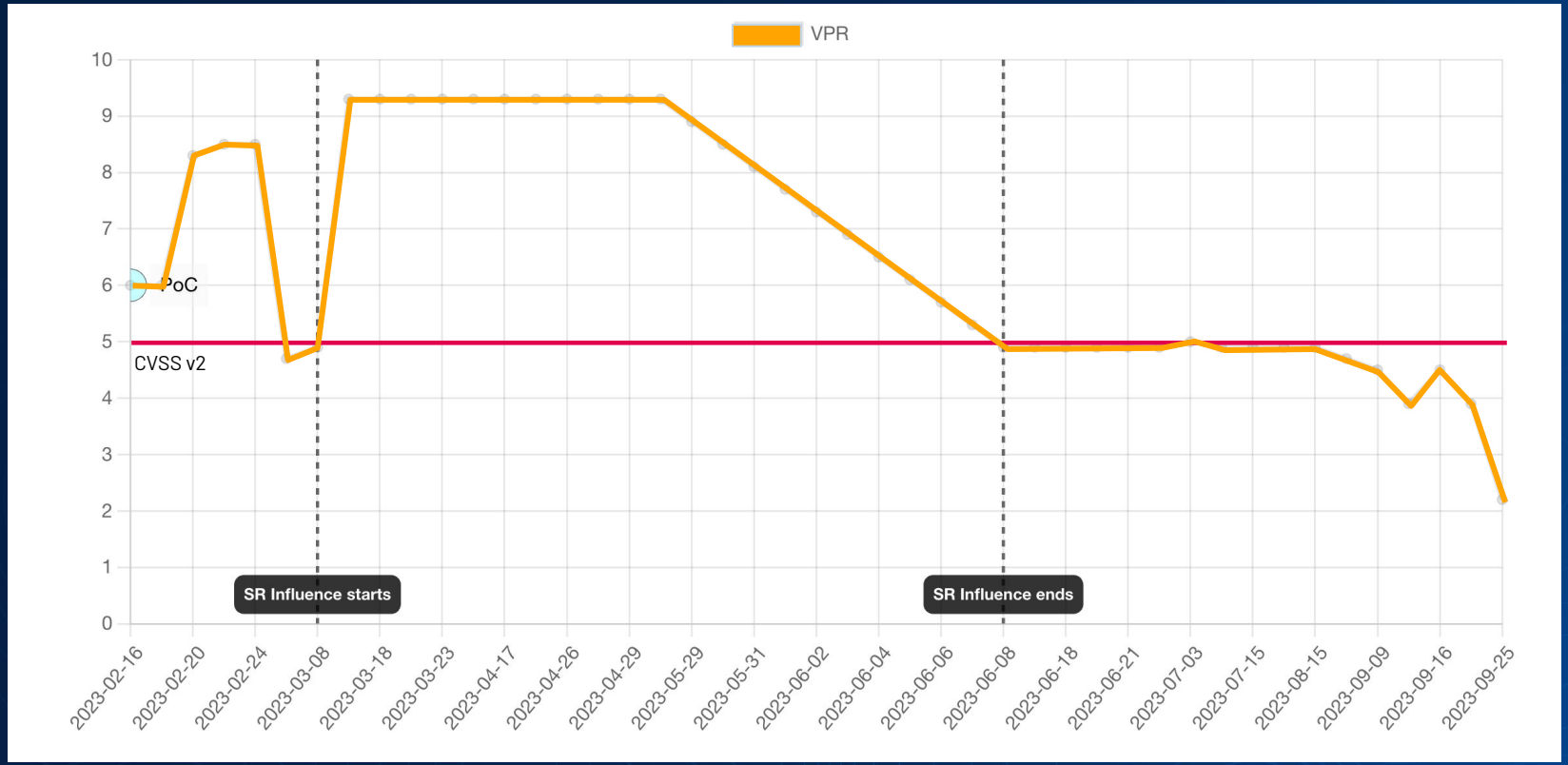
Vulns = Compliance check

VPR = 9.5
ACR = 3

AES = 250

Vulnerability Priority Rating (VPR) + Asset Criticality Rating (ACR) = Asset Exposure Score (AES)

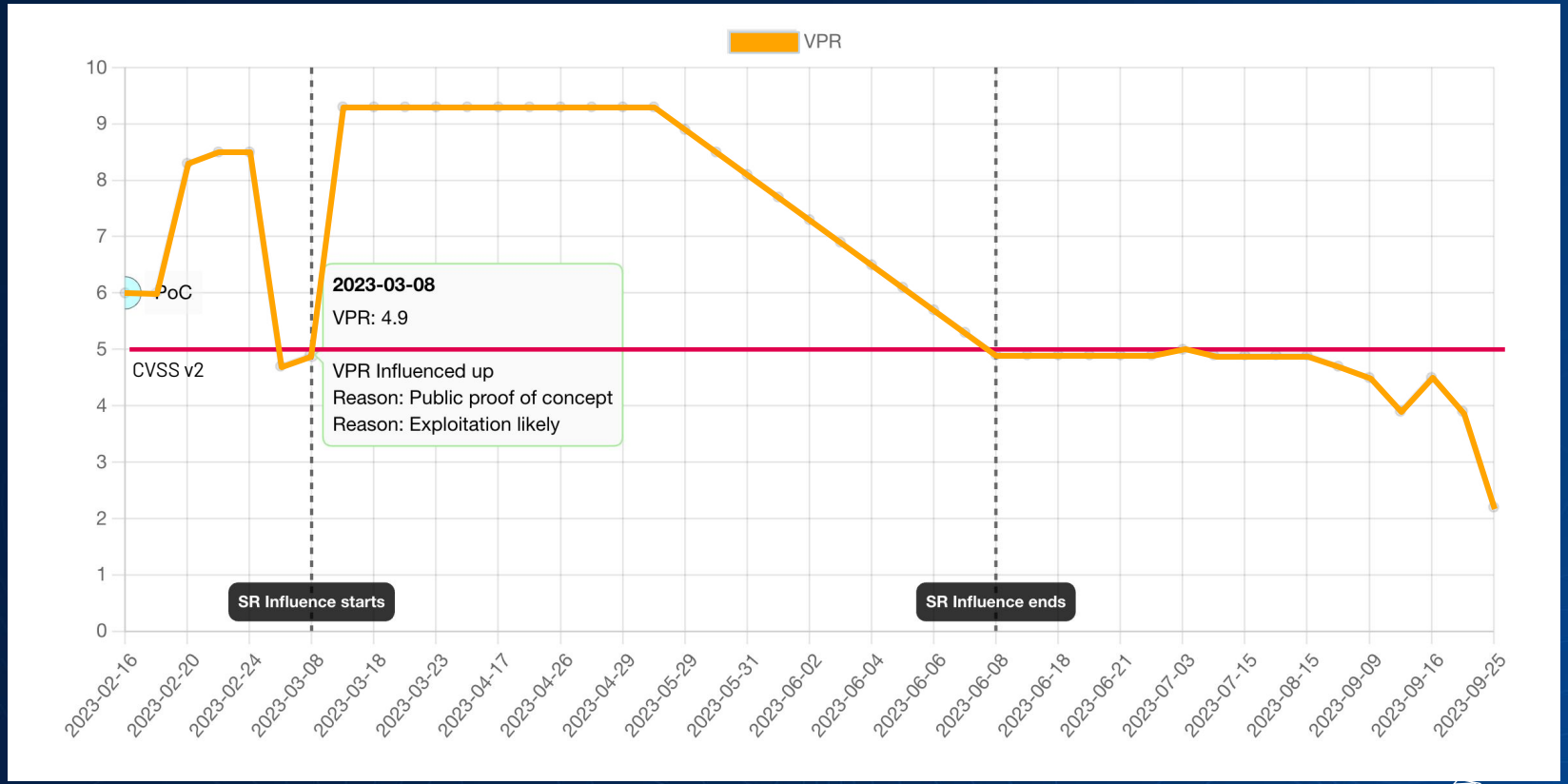
Dynamic Risk Scoring Predictions Driven by ML



CVE 2023-23572 – Joomla Vulnerability

tenable

Dynamic Risk Scoring Predictions Driven by ML



CVE 2023-23572 – Joomla Vulnerability

tenable

AI Benefits to Efficiency and Effectiveness

PREDICT

Leverage ML to automate the identification of threats, exploits and the likelihood of attack for vulnerabilities, misconfigs and code flaws

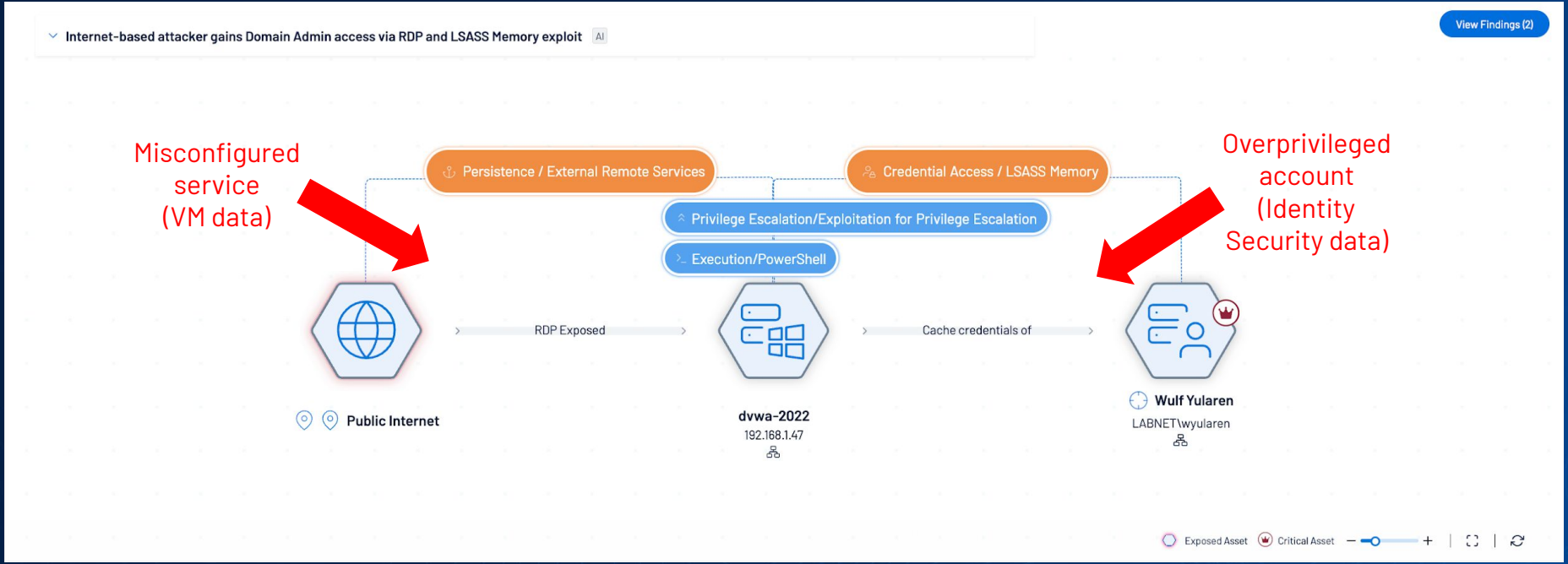
EXPLAIN

Gen AI and LLMs are ideal to translate complicated technical data into more human-readable content for quicker and more accurate decision making

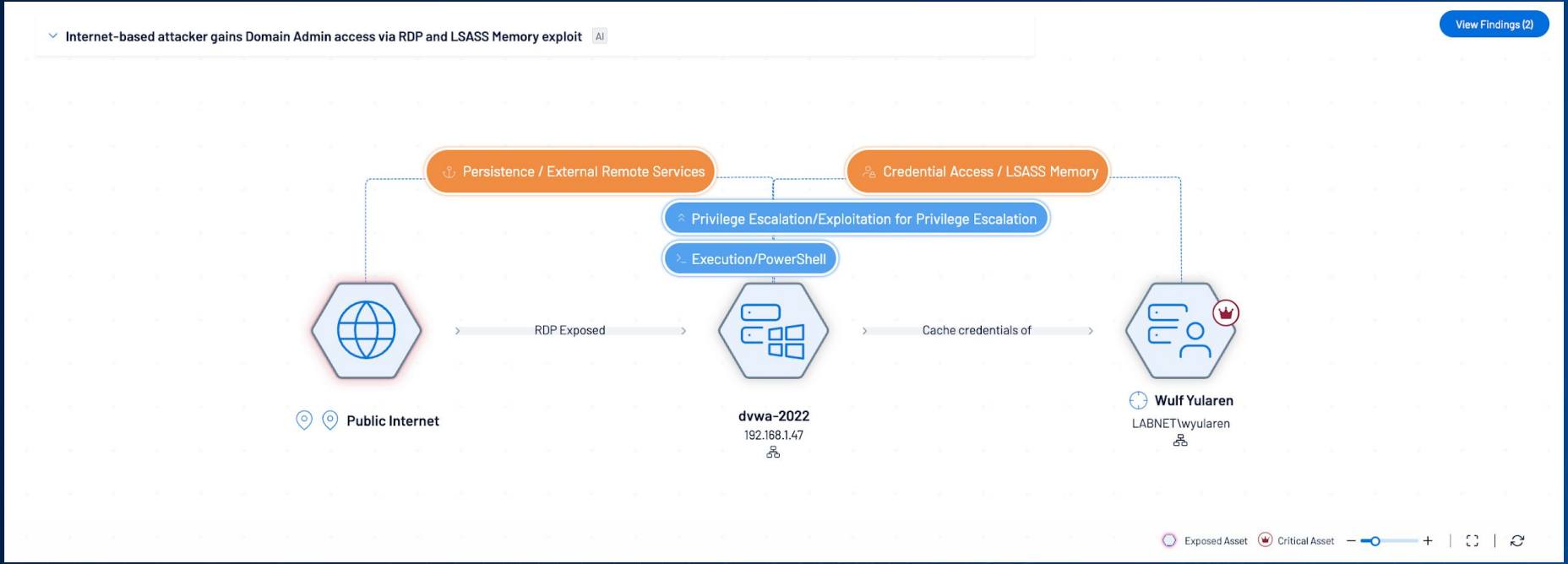
RETAIN

Security practitioners want to stay on the hunt for threats and flaws, rather than focusing on mundane manual tasks and long-term training engagements

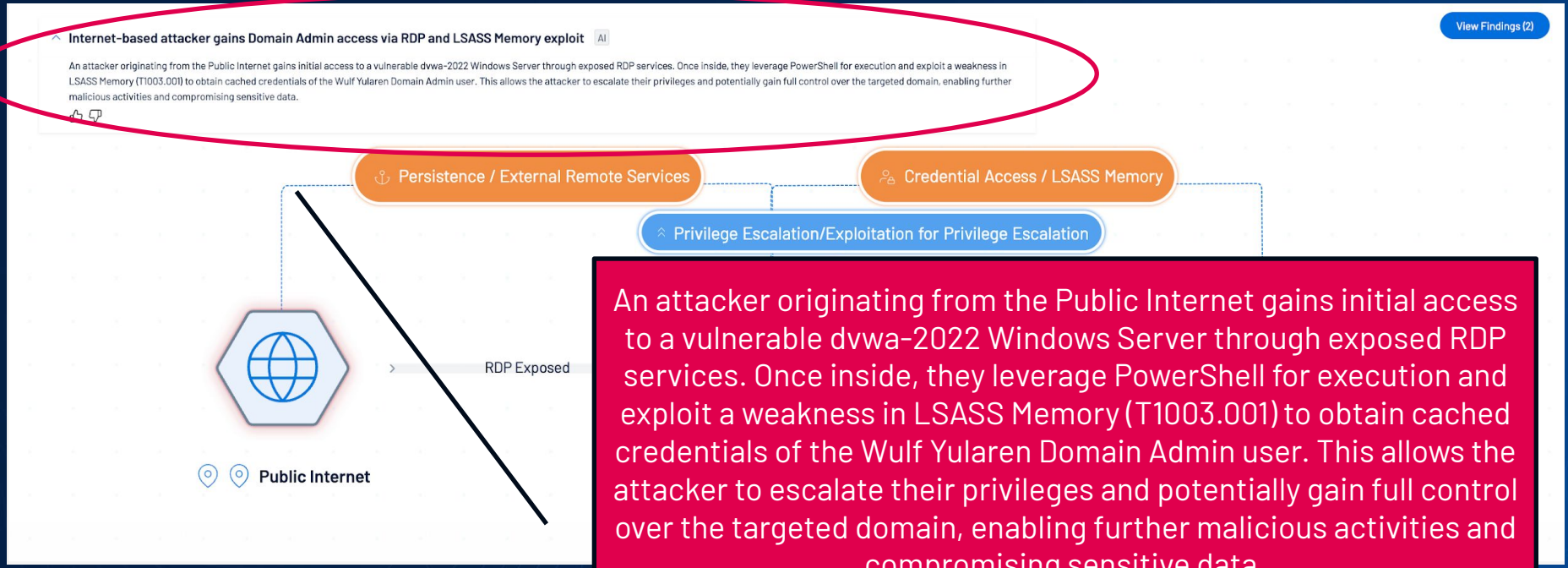
Attack Path Analysis w/Multiple Weaknesses



Attack Path Analysis w/Multiple Weaknesses

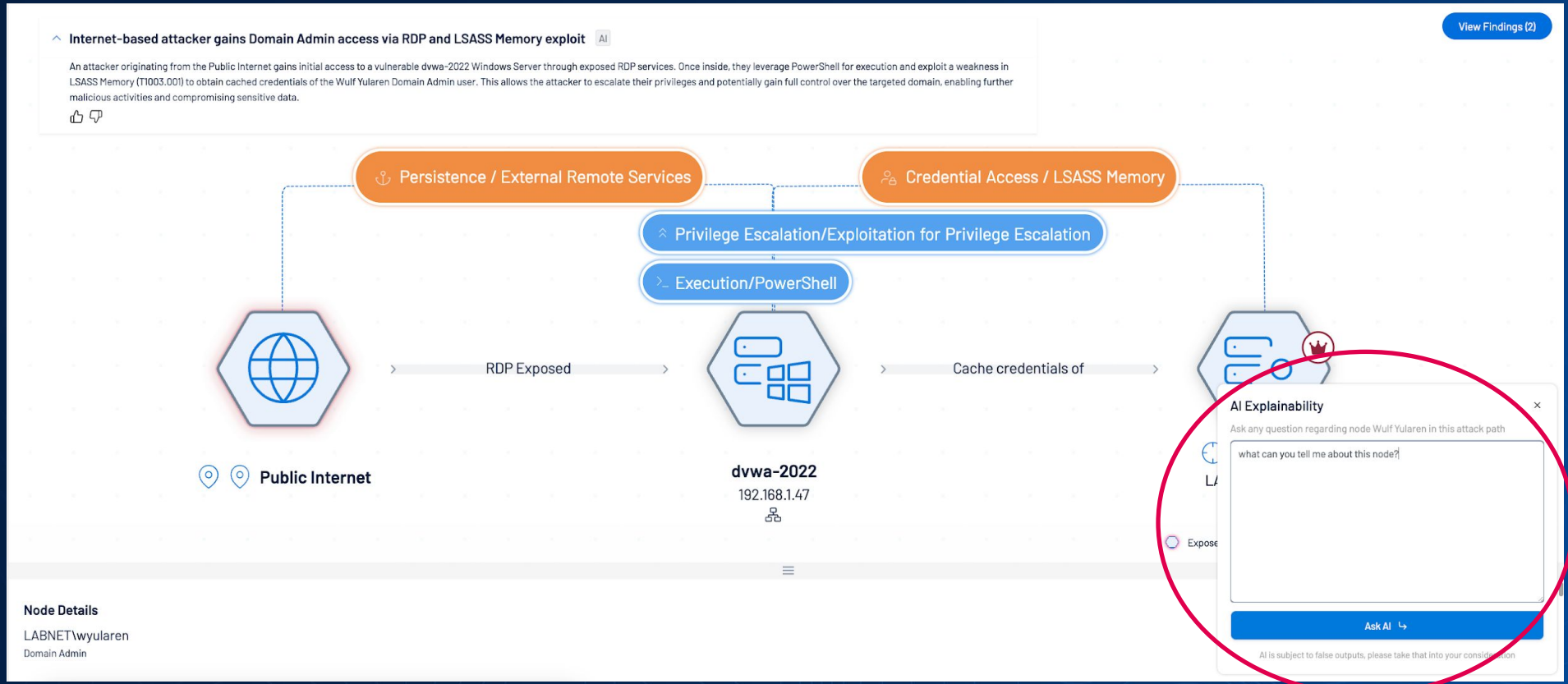


Generative AI Creates Easy Explainability

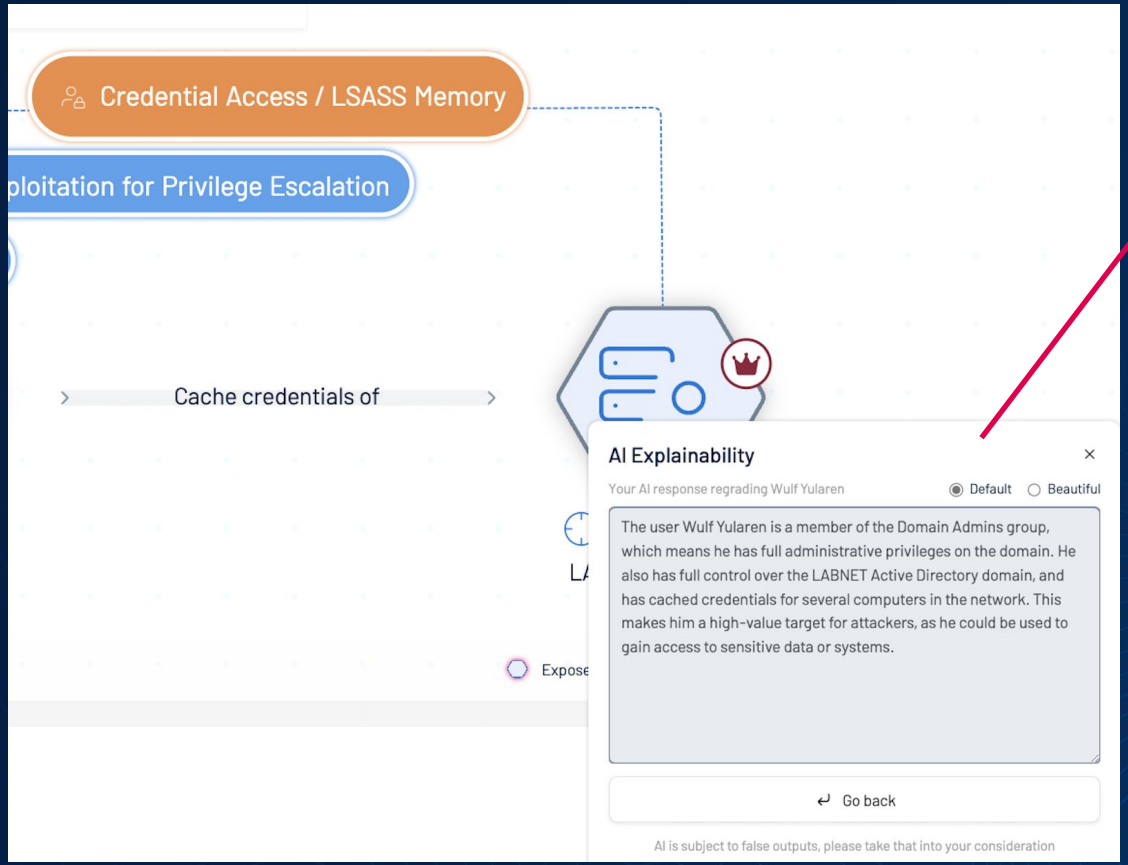


An attacker originating from the Public Internet gains initial access to a vulnerable dvwa-2022 Windows Server through exposed RDP services. Once inside, they leverage PowerShell for execution and exploit a weakness in LSASS Memory (T1003.001) to obtain cached credentials of the Wulf Yularen Domain Admin user. This allows the attacker to escalate their privileges and potentially gain full control over the targeted domain, enabling further malicious activities and compromising sensitive data.

LLMs Can Help Analysts Understand More Quickly



LLMs Can Help Analysts Understand More Quickly



The user Wulf Yularen is a member of the **Domain Admins** group, which means he has full administrative privileges on the domain. He also has full control over the LABNET Active Directory domain, and has cached credentials for several computers in the network. This makes him a high-value target for attackers, as he could be used to gain access to sensitive data or systems.

AI Benefits to Efficiency and Effectiveness

PREDICT

Leverage ML to automate the identification of threats, exploits and the likelihood of attack for vulnerabilities, misconfigs and code flaws

EXPLAIN

Gen AI and LLMs are ideal to translate complicated technical data into more human-readable content for quicker and more accurate decision making

RETAIN

Security practitioners want to stay on the hunt for threats and flaws, rather than focusing on mundane manual tasks and long-term training engagements

tenable

It's Not All Tools and Process Problems in the SOC

Stats from SANS and Devo:

- **53%** of respondents say they have considered walking away from their job due to pressure
- Average time to fill a SOC role: **7 months**
- "Onboarding, training and fully operationalizing a SOC analyst usually takes several months leaving your organization with less eyes on glass and security expertise to respond to those threats"

More Stats from a recent Tenable and Forrester report:

- **58%** say the cybersecurity team is too busy fighting critical incidents to take a preventive approach to reducing their organization's exposure
- On average, organizations spend **15 hours per month** creating security reports for business leaders.

Sources: https://www.devo.com/resources/analyst-research/the-sans-2022-threat-hunting-report/
https://www.tenable.com/analyst-research/unlock-proactive-cyber-defence-for-your-australian-business

In Review…

- AI doesn't solve everything, but it can improve efficiency and effectiveness
- Reduce Mean Time to Discover (MTTD) and Mean Time to Remediate (MTTR)
- Context is the key
  - Vulnerabilities alone don't define risk
  - Vulnerabilities + Identities + Entitlements + Business Context = True Risk to the Organization
  - Better prioritization of remediation efforts
- AI tools can educate junior staff members and free senior staff for more complex tasks
- ROI for new hires goes up, better retention of senior analysts

tenable