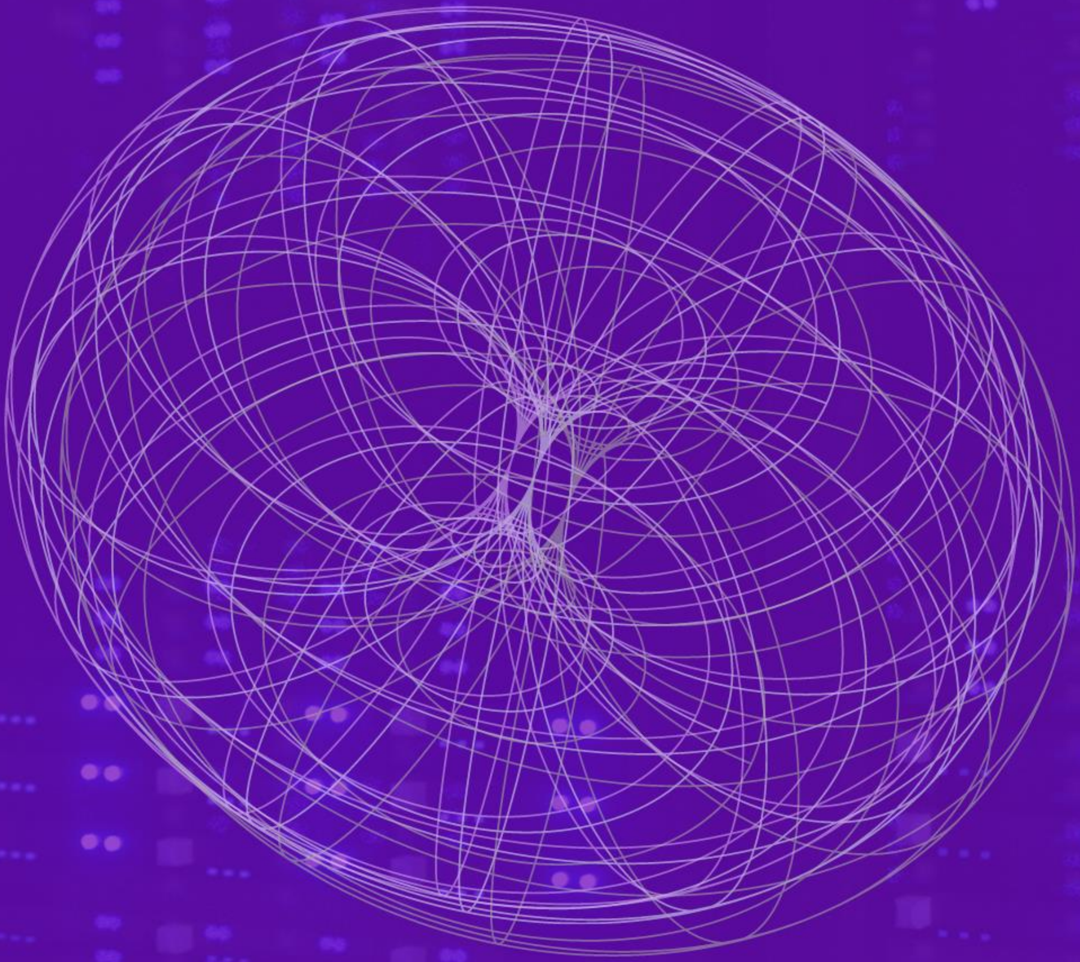
FLOW
the smart choice

Evolving Cyber Defences:



Mastering the New Era of Vulnerability Management

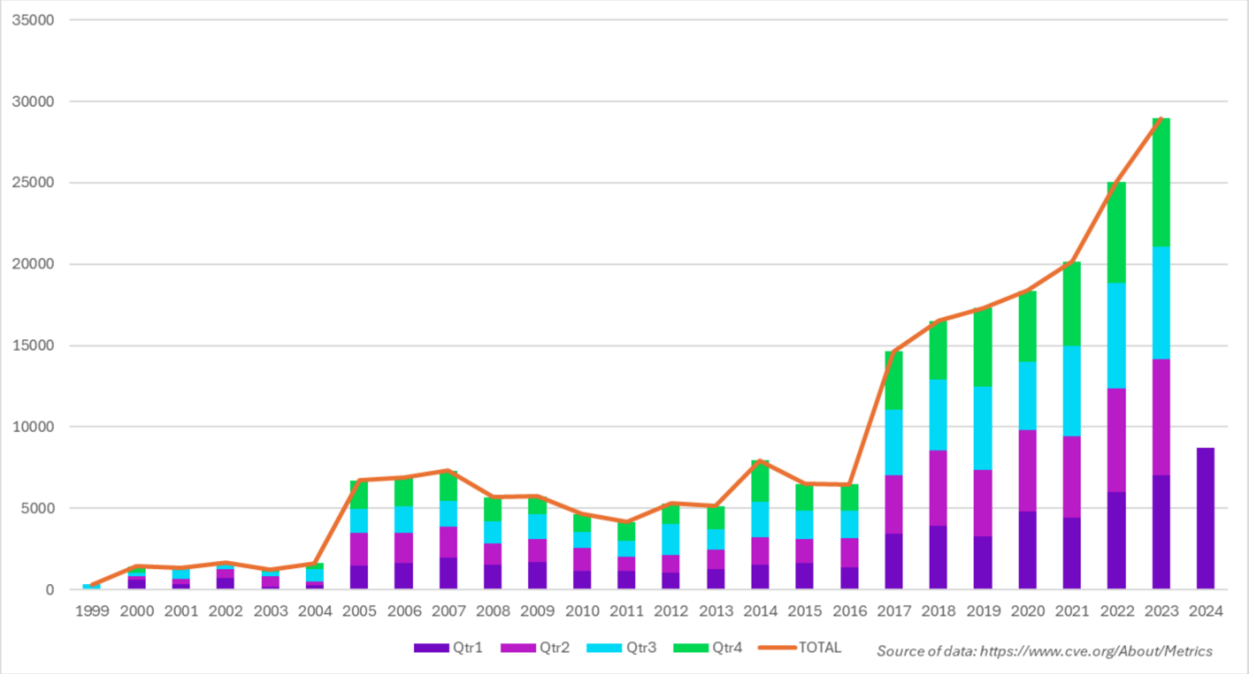
Strategic Insights

Evolving Cyber Defences: Mastering the New Era of Vulnerability Management

Vulnerability Management stands as a critical element of cybersecurity defence, which has been evolving to meet the relentless advancements of cyber threats. Over the past two decades, the National Vulnerability Database NVD has grown to contain over 250,000 vulnerabilities.

When we look at the data, the exponential growth in the rate of vulnerabilities being added to the NVD is accelerating. We have seen the steepest rate of growth every year since 2017, and looking at Q1, 2024 will be no exception.

This highlights the ever-growing need for robust and efficient vulnerability management.



Source of data: https://www.cve.org/About/Metrics

Managing vulnerabilities, specifically prioritising vulnerability remediation, remains a challenge for many organisations. This challenge is only going to become greater as the volume of published CVEs increases.

A Brief History of Vulnerability Management

Through an understanding of the historical context and evolution of related standards and tools, we gain a clearer picture of the journey that led us to the challenges we face today. This knowledge helps us prepare to safeguard our digital assets and networks against these ever-present and evolving threats.

1998

Nessus

Creation of The Nessus Project as a free remote security scanner. It's open-source status will ultimately be discontinued in 2005, resulting in several forks including OpenVAS (Open Vulnerability Assessment System).

1999

CVE List

Groundwork for the CVE List was laid by MITRE Corporation through their white paper, Towards a Common Enumeration of Vulnerabilities. This led to the creation of the initial 321 CVE Records.

2005

NIST National Vulnerability Database

Introduction of the Common Vulnerability Scoring System (CVSS) Version 1, established with the aim of providing standardized severity ratings for software vulnerabilities.

CVSS v1

Introduction of the Common Vulnerability Scoring System (CVSS) Version 1, established with the aim of providing standardized severity ratings for software vulnerabilities.

2007

CVSS v2

Version 2 was unveiled marking a significant upgrade from v1. This release was announced collaboratively by the Forum of Incident Response and Security Teams (FIRST) and the Common Vulnerability Scoring System-Special Interest Group (CVSS-SIG).

2015

CVSS v3

This iteration brought about numerous changes, including modifications to the numerical formulas, metrics, and the introduction of new severity ratings, providing a more refined and effective tool for assessing software vulnerabilities.

2019

CVSS v3.1

A minor but important update aimed at improving clarity and usability without introducing new metrics. This version incorporated valuable insights from industry experts and refined various aspects of the CVSS standard to better align with the evolving cybersecurity landscape.

2021

CISA KEV

The Known Exploited Vulnerability (KEV) catalogue, maintained by CISA, serves as the authoritative source for vulnerabilities successfully exploited in the wild.

EPSS v1

The Exploit Prediction Scoring System (EPSS) Version 1 offered a data-driven approach to estimating the likelihood of a vulnerability being exploited. With the objective of aiding network defenders in prioritizing remediation efforts.

2022

EPSS v2

A significant evolution with the integration of over 1,100 variables in a centralized, API-driven model. This enhanced version offered improved accuracy and performance in predicting vulnerability exploitations in the next 30 days.

CTEM

Gartner introduced Continuous Threat Exposure Management (CTEM) program. We talk more about this later.

2023

EPSS v3

An improved version that offers a more comprehensive, efficient, and effective model for prioritizing vulnerabilities. EPSS 3.0 shows an 82% improvement over previous versions and provides a strong data-driven approach to evaluating threats.

CVSS v4

Introduced various enhancements including new nomenclature, metrics, and values to provide a more nuanced understanding of vulnerabilities. With additional focus on OT/ICS/Safety, this version offers a comprehensive tool for assessing and scoring vulnerabilities.

Vulnerability Measures

There are two key vulnerability scoring systems that can be used to inform organisations of where to prioritise their vulnerability remediation efforts. These are the Common Vulnerability Scoring System (CVSS) Base Score and the Exploit Prediction Scoring System (EPPS) Score.

CVSS Base Score

Introduced in 2005 to standardise the severity rating of vulnerabilities. It has undergone a series of refinements over the years; the last version, version 4, was released in 2023. The CVSS Base Score is a numerical value from 0 to 10, measured in the following severities:

- Critical (9.0-10.0)
- High (7.0-8.9)
- Medium (4.0-6.9)
- Low (0.1-3.9)
- None (0.0)

EPSS Score

EPSS (Exploit Prediction Scoring System) estimates the likelihood (probability) that the vulnerability will be exploited in the wild. It was first introduced in 2021 and is now in its third version, which was released in 2023. The probability scores range between 0.0 and 1.0 (0% and 100%).

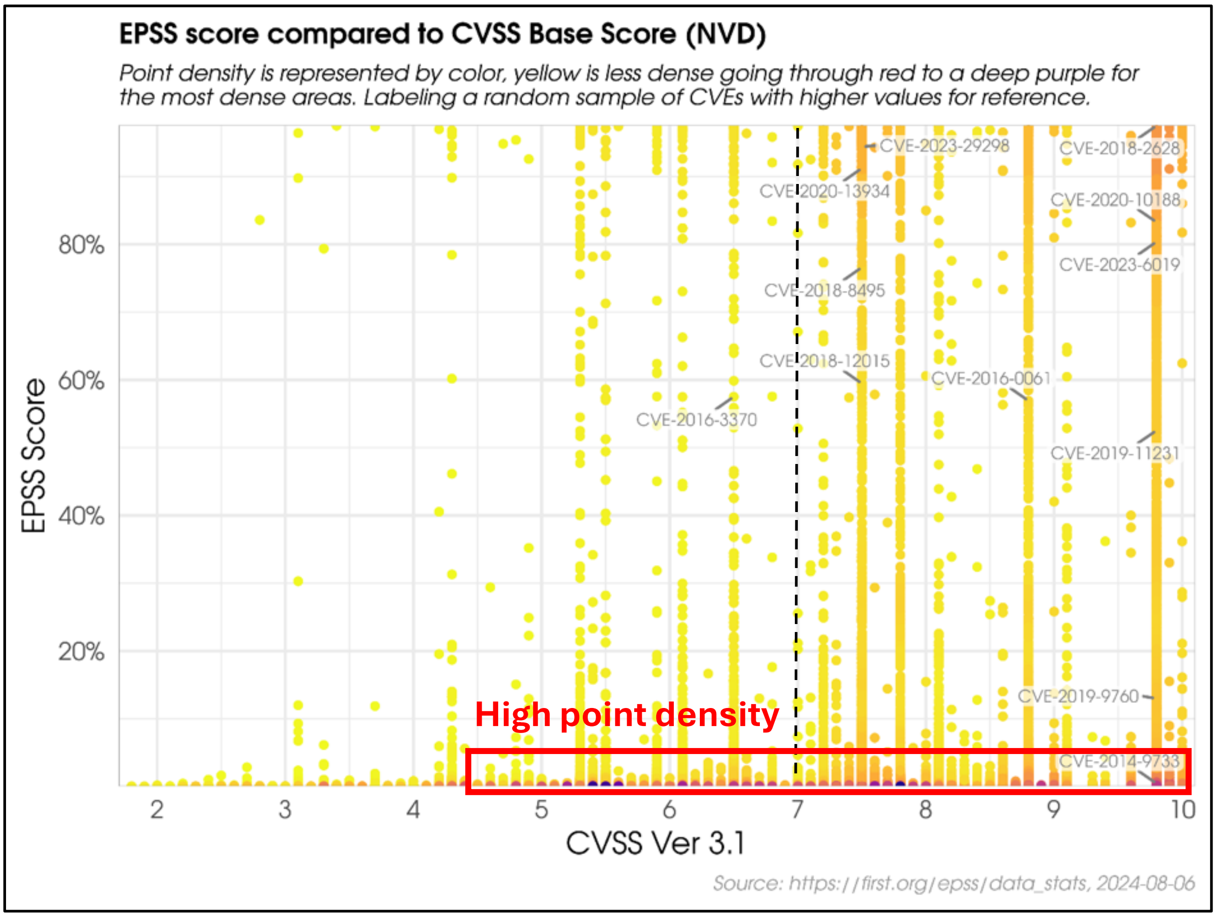
Evolution of Prioritisation

As we saw in the above timeline, many new developments have been made to improve the information we all have to help prioritise vulnerabilities. Despite this progress, identifying the vulnerabilities that are causing organisations the greatest exposure continues to be a challenge. In an ideal world, we would remediate all vulnerabilities as soon as possible, but this is simply not feasible.

Many organisations will have compliance standards to adhere to, which will dictate their approach to vulnerability management. This will vary depending on the compliance standard in use. Some will require that you have a process for timely identification and remediation. Others, like Cyber Essentials, will have very specific requirements.

Cyber Essentials requires that all high and critical security updates be applied within 14 days. On audit day, any vulnerabilities with a CVSS Base Score of 7 or higher would be marked as failures.

Focusing on severity alone can leave you addressing a high volume of vulnerabilities with a low likelihood of exploitation and potentially missing that one lower severity vulnerability with a high likelihood of exploitation that unlocks an attack path into your organisation.


EPSS score compared to CVSS Base Score (NVD)

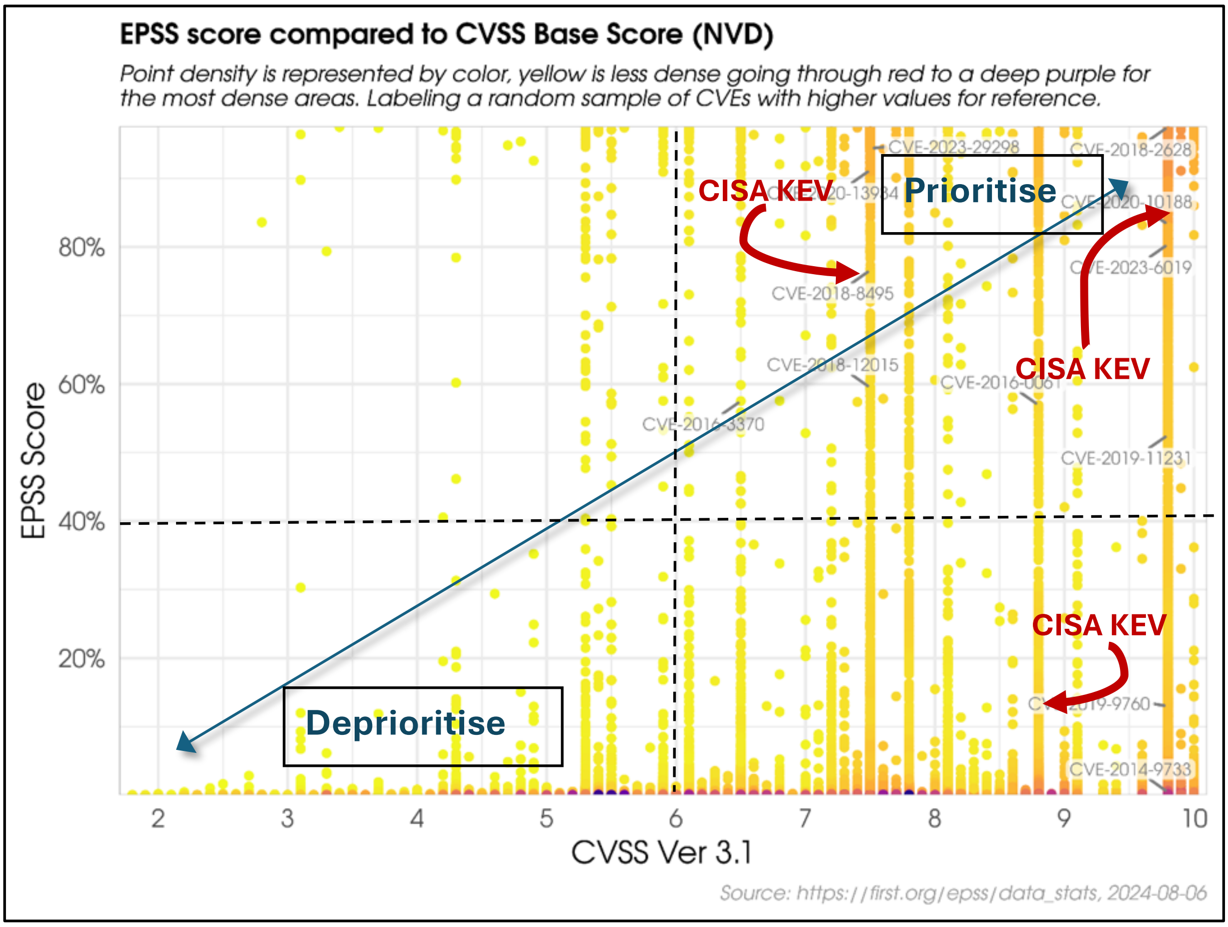
Point density is represented by color, yellow is less dense going through red to a deep purple for the most dense areas. Labeling a random sample of CVEs with higher values for reference.

Source: https://first.org/epss/data_stats, 2024-08-06

The point density in this chart is represented by colour; yellow is less dense going through red and to a deep purple for most dense areas. The highest density of vulnerabilities commonly falls into the sub 5% EPSS likelihood score.

A more balanced approach would be to map a vulnerability's CVSS Base Score against its associated EPSS score. Using these two data points, we can build a quadrant chart for prioritisation, as shown below.

This can be enhanced further by integrating the Known Exploited Vulnerabilities catalogue produced by CISA, a data set which has also been incorporated into the NIST NVD. This catalogue contains entries for every vulnerability known to be exploited in the wild, regardless of severity.



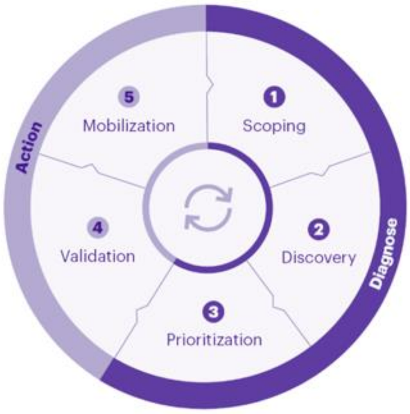
Source: https://first.org/epss/data_stats, 2024-08-06

With all this in mind, we could adopt a prioritisation plan along the lines of the following:

- 1st Priority – CVEs found in the CISA's KEV Catalogue
- 2nd Priority – CVEs in the upper-right quadrant.
- 3rd Priority – CVEs in the lower-right quadrant.
- 4th Priority – CVEs in the upper-left quadrant.
- 5th Priority – CVEs in the lower-left quadrant.

This is just one example of how vulnerability remediation efforts can be prioritised. Compliance will be crucial in guiding organisations, but the approach must also fit the business and the resources available to perform remediation actions. When resources are limited, organisations can look at other tools to help refine the focus further.

The Advent of CTEM



CTEM was introduced in the Gartner® report "Implement a Continuous Threat Exposure Management (CTEM) Program," published on 21 July 2022. The report describes CTEM as a "program that surfaces and actively prioritises whatever most threatens your business."

It is important to note that the CTEM framework cannot be implemented through a single tool or platform. It is achieved by combining technologies, people, data, controls and processes.

The CTEM approach comprises five steps spanning over Diagnose and Action areas.

Diagnose

1. **Scoping**
   Scoping is a vital first step in understanding your organisation's attack surface. It extends beyond the focus of typical vulnerability management programs, covering traditional devices and applications along with less tangible elements like corporate social media, online code repositories, SaaS security posture, and integrated support chains.

2. **Discovery**
   The discovery process should focus on areas of the business that were identified during scoping. This should identify visible and hidden assets, their vulnerabilities, misconfiguration, and other risks.

3. **Prioritisation**
   The goal here is to factor in urgency, security, availability of compensation controls, tolerance for residual attack surface, and the level of risk posed to the organisation. It is key to identify the business's high-value assets and focus on the plan to remediate them.

Action

4. **Validation**
   This is a key step that makes this approach stand out. We don't just take our initial prioritisation in isolation. We go further and validate that the vulnerability can be exploited. To do this, we need to analyse potential attack pathways to the vulnerable asset(s), verifying the effectiveness of the detection and subsequent response and remediation processes.

5. **Mobilisation**
   At this point, we can begin mobilising the required teams to operationalise the CTEM findings. Remediation can be through automated tools or manual effort via security teams or other business stakeholders.

“By 2026, organisations prioritising their security investments, based on a continuous threat exposure management program, will realise a two-third reduction in breaches”.

Gartner Top Strategic Technology Trends for 2024: Continuous Threat Exposure Management, Published 16 October 2023

Adopting a CTEM approach provides organisations with a proactive and continuous risk mitigation process, helping them stay ahead of the ever-evolving cybersecurity landscape and mobilise promptly to emerging risks.

Though enriching discovered vulnerabilities with business context and validated attack paths, organisations can focus on their most significant threats, optimise their resources to mitigate them, and ultimately maximise the effectiveness of these efforts.

Taking a more holistic approach to the discovery of risks beyond vulnerability scanning alone, including cloud misconfiguration, SaaS security posture, and security identities, provides a comprehensive approach to assessing an organisation's overall security posture.

WithSecure Exposure Management

As mentioned above, CTEM cannot be implemented with a single tool. Organisations may, however, leverage a combination of solutions to aid them in their CTEM journey. We believe that the WithSecure Exposure Management platform is an ideal example of this, combining the key technologies to aid CTEM implementation in a single platform.

Earlier this year, WithSecure announced its new Exposure Management solution as part of its Elements portfolio. This latest offering combines and enhances its Vulnerability Management and Cloud Security Posture Management products, adding AI-powered attack path analysis.

This solution maps well to the CTEM methodology, providing the tooling to aid organisations in integrating it into their vulnerability management programs.

- **Continuous**
  A continuous and proactive solution that regularly assesses your company's assets based on scan schedules you define.

- **Scoping**
  This tool helps you see your complete attack surface, covering Network equipment, Cloud Services (Azure, AWS), Managed Devices (workstations & servers), external-facing assets, and Identities (Entra ID). Once the scope has been defined, you can use the built-in business context to identify critical assets, which will be used in prioritising findings.

- **Discovery**
  It is built on a 360˚discovery platform that combines traditional vulnerability scanning with cloud misconfiguration analysis and identity protection to give complete visibility of vulnerabilities and risks across the aforementioned asset types.

- **Prioritise & Validate**
  Utilising its AI-powered prioritisation capability, Exposure Management combines the discovered findings with its unique Threat intelligence and the asset-based business context you define. Attack paths to these findings are validated, simulating the path an attacker could take to compromise your estate.

- **Mobilise**
  Exposure Management enriches findings with clear remediation advice, allowing you to mobilise your teams quicker and arm them with the information they need to act. Asset contacts can be set to provide you with an instant single-click escalation to notify the relevant teams. Benchmarking your organisation's exposure risk helps you measure the effectiveness of your actions.

  Exposure Management is part of the modular WithSecure Elements solution, which incorporates Extended Detection and Response (EDR), Endpoint Security, Identity Security and Collaboration Protection (M365 protection).

Summary and Next Steps: Building a Stronger Security Posture

As cyber threats evolve, taking a proactive approach to vulnerability management is essential. WithSecure's Exposure Management platform offers a comprehensive solution that aligns with the CTEM methodology, helping organisations stay ahead of risks.

Your team can address critical vulnerabilities more effectively and efficiently by leveraging continuous monitoring, AI-driven prioritisation, and validated attack paths.

Now is the time to act. Strengthen your organisation's security by integrating a holistic exposure management process that provides complete visibility across your assets, ensuring rapid detection and response to emerging threats.

Next Steps:

- Assess your current security posture and identify areas of improvement.
- Explore the tools and services within WithSecure's portfolio to enhance vulnerability management.
- Contact our team to discuss how WithSecure can support your organisation's journey to a stronger, more secure future.

Reach out to us today to explore how we can help strengthen your security. Whether you're looking for more information or ready to schedule a consultation, let's collaborate to protect your business against evolving threats.

Flowtransform.com
info@flowtransform.com
+44 (0) 1442 927 996