IT Partnership Dashboard for April 2023 to July 2025 – Part One

IT Infrastructure Uptime and P1 Incidents.

T infrastructure comprises the fundamental components and resources that underpin IT services and operations. It serves as the backbone, facilitating the functionality of technology. These elements are crucial for operating various systems, including websites, email services, complex business applications, and data storage. Uptime for IT infrastructure denotes the percentage of time during which the IT infrastructure is accessible for use. This metric is essential in assessing reliability, as it reflects how consistently IT services are available without interruption. High uptime indicates minimal downtime.

This provides a comprehensive review of the performance of the IT infrastructure for the period spanning April 2023 through July 2025. The principal focus of this document is the analysis of system uptime and the management of Priority 1 (P1) incidents. The established operational objective is the maintenance of a minimum 99% uptime across all core services.

Performance Analysis: 2023 – 2024

Throughout the fiscal year of 2023-2024, the overall performance of the IT infrastructure was robust. An uptime of 100% was realised at the East Herts site, while the Stevenage site achieved 99% uptime, thereby fulfilling the departmental objective.

Uptime and P1's for IT infrastructure			
2023 / 2024			
	East Herts	Stevenage	
Apr-23	**100%**	**100%**	
May-23	**100%**	**92.30%**	17 hours downtime for Widows 7 issue for Housing (150 staff)
Jun-23	**100%**	**100%**	
Jul-23	**100%**	**100%**	
Aug-23	**100%**	**100%**	
Sep-23	**100%**	**100%**	
Oct-23	**100%**	**100%**	
Nov-23	**100%**	**100%**	
Dec-23	**100%**	**100%**	
Jan-24	**100%**	**100%**	
Feb-24	**100%**	**100%**	
Mar-24	**100%**	**100%**	
Total	**100%**	**99%**	The target is 99%

A significant P1 incident occurred in May 2023 at the Stevenage site, resulting in 17 hours of system downtime for 150 personnel within the Housing department. The causation was attributed to a legacy Windows 7 vulnerability. Following this event, corrective measures were implemented by the IT department, culminating in 100% uptime for both sites for the remaining period of the year. The effectiveness of this recovery serves to underscore the competence of the personnel in the resolution of critical system failures.

Performance Analysis: 2024 – 2025

The subsequent fiscal year was characterized by an exceptional degree of operational stability. A consistent 100% uptime was maintained at the East Herts site throughout the year, while the Stevenage site achieved an uptime of 99.83%. The sole reported P1 incident, which occurred in March 2025, involved a minor SBC Pool VDI issue that was resolved in less than 20 minutes. This outcome serves as a clear demonstration of the department's capacity for proactive monitoring and expeditious incident response.

Uptime and P1's for IT infrastructure.			
2024 / 2025			
	East Herts	Stevenage	
Apr-24	**100%**	**100%**	
May-24	**100%**	**100%**	
Jun-24	**100%**	**100%**	
Jul-24	**100%**	**100%**	
Aug-24	**100%**	**100%**	
Sep-24	**100%**	**100%**	
Oct-24	**100%**	**100%**	
Nov-24	**100%**	**100%**	
Dec-24	**100%**	**100%**	
Jan-25	**100%**	**100%**	
Feb-25	**100%**	**100%**	
Mar-25	**100%**	**99.83%**	20 mins SBC Pool VDI Issue
Total	**100%**	**100%**	The target is 99%

Current Performance Challenges: 2025 - 2026
The present reporting period has been marked by a series of operational challenges.

Uptime and P1's for IT infrastructure.			
2025 / 2026			
	East Herts	Stevenage	
Apr-25	**99.73%**	**100%**	EHC Only - Desk phones and ZC offline
May-25	**95.85%**	**95.85%**	Applications unavailable - printing unavailable - some users cannot reauthenticate once disconnected from Hosted Desktop
Jun-25	**91.19%**	**91.19%**	Users unable to login - FSLogix Error
Jul-25	**97.17%**	**97.17%**	Users unable to login - FSLogix Error
Aug-25			
Sep-25			
Oct-25			
Nov-25			
Dec-25			
Jan-26			
Feb-26			
Mar-26			
Total	**94.74%**	**96.05%**	The target is 99%

May 1, 2025: Applications Unavailable
Incident Description: A P1 incident was recorded on May 1, 2025, impacting both East Herts and Stevenage. This event precipitated the unavailability of applications and precluded users from reauthenticating from their Hosted Desktops, leading to a significant reduction in uptime to 95.85% at both locations. The incident further extended to encompass issues with printing services and user reauthentication for certain Hosted Desktop users.

Root Cause: To help explain what happened, a blade servers are housed together in a single chassis and work as the backbone for running many of our online services and virtual desktops.

These blade servers rely on accurate timekeeping, which they get by regularly synchronising their internal clocks with a central reference called the domain controller. The domain controller not only manages secure access but also acts as the official time source for all connected computers on our network. If a server's clock is out of sync with the domain controller, it can cause major problems—especially for logging in and verifying user identities.

In this case, one of our blade servers lost its time synchronisation with the domain controller. This meant that the affected blade's internal clock gradually drifted away from the official network time. As a result, some users had trouble reauthenticating or accessing services because their computers could no longer reliably prove to the system who they were. This is similar to trying to enter a building with a badge that's set to the wrong time—if the system can't verify the time, it might not let you in, even if you have the right credentials.

Remedial Actions: After identifying the root cause, the blade servers' time was resynchronized, and normal service was restored. The investigation revealed the importance of having a resilient external time synchronization system. Although there are no current issues with the setup, it has been identified as a potential cyber risk since many IT environments in the UK rely on the same external time source. Steps are being taken to ensure an alternative time source is available in case the primary one becomes compromised.

June 25 and July 2, 2025: FSLogix Errors
Incident Description: On June 25 and July 2, 2025, difficulties were encountered by a subset of VDI desktop users who were unable to access their profiles. This issue randomly impacted less than 50% of VDI users on the first date and less than 25% on the second, affecting both East Herts and Stevenage sites. It is to be noted that all other systems, including the network, laptops, and Microsoft 365 services, remained fully operational during these events.

Root Cause: We identified the root cause: permissions had unexpectedly been removed from user profile folders on some of our servers that store VDI user data. These folders are essentially individual digital workspaces, and without the correct permissions, users could not access their personalised settings and files. This issue occurred on two of our four servers on Tuesday 24th June, and the other two of the four servers on Tuesday 1st July
Crucially, we immediately conducted a full scan of our network as soon as the issue first appeared to determine if it had been a cyberattack. This was definitively ruled out.

Remedial Actions: The technical team collaborated with Microsoft to investigate the issue. Initially, Microsoft did not identify any problems in the log files. Over two weeks, several hotfixes and updates were installed as part of the investigation. The source of the problem was eventually traced to a new version of FSLogix, which included updated Group Policy templates that were not fully compatible with the existing configuration. This update, released by Microsoft, resulted in conflicts that caused the initial issue and subsequent issues affecting approximately 40 users:

- Daily sign-in prompts for Microsoft applications such as OneDrive, Teams, and Outlook
- TPM (Trusted Platform Module) errors

Such issues can occur when new features or updates are deployed by Microsoft without advance notice or documentation, as seen with the FSLogix case. Additionally, the restore and recovery process was reviewed and improved; while the initial restoration took around six hours, it can now be completed in less than an hour.

IT Network Infrastructure Uptime and P1 Incidents

IT Network infrastructure consists of the hardware, software, and services that enable computers and devices to connect and communicate. This includes components such as routers (to direct traffic between networks), switches (to connect devices within a network), firewalls (for security), cables (such as Ethernet and fiber optic), and wireless access points. Uptime for IT Network infrastructure refers to the percentage of time that the network and its components – including routers, switches, and firewalls – are fully operational and available for devices to connect and communicate. It is a measure of the reliability and accessibility of the network, which impacts productivity and the ability to access IT resources.

This provides a detailed review of the IT network infrastructure performance for the period of April 2023 through July 2025, with a particular focus on network uptime and the management of Priority 1 (P1) incidents. The IT department's operational objective is to maintain a minimum of 99% uptime across all core network services.

Performance Analysis: 2023 – 2024

For the fiscal year 2023-2024, the IT network infrastructure demonstrated a robust level of performance, achieving a total uptime of 99.8% for both East Herts and Stevenage sites, thus exceeding the 99% target.

Uptime and P1’s for IT Network infrastructure.			
2023 / 2024			
	East Herts	Stevenage	
Apr-23	**100%**	**100%**	
May-23	**100%**	**100%**	
Jun-23	**100%**	**100%**	
Jul-23	**100%**	**100%**	
Aug-23	**100%**	**100%**	
Sep-23	**100%**	**100%**	
Oct-23	**100%**	**100%**	
Nov-23	**97.50%**	**97.50%**	5 ½ hours downtime due to the dark fibre being Cut
Dec-23	**100%**	**100%**	
Jan-24	**100%**	**100%**	
Feb-24	**100%**	**100%**	
Mar-24	**100%**	**100%**	
Total	**99.8%**	**99.8%**	The target is 99%

A significant P1 incident occurred in November 2023, which impacted both sites, resulting in 5.5 hours of downtime. This was attributed to a fiber cut. Despite this incident, the department's quick response and subsequent remediation efforts ensured that the annual uptime target was met.

Performance Analysis: 2024 - 2025

Uptime and P1’s for IT Network infrastructure.			
2024 / 2025			
	East Herts	Stevenage	
Apr-24	**100%**	**100%**	Reports of intermittent Wi-Fi issues were resolved by connecting the majority of staff to public Wi-Fi for the most stable connection.
May-24	**100%**	**100%**	
Jun-24	**100%**	**100%**	
Jul-24	**100%**	**100%**	
Aug-24	**100%**	**100%**	
Sep-24	**98.6 %**	**98.6 %**	The server storage (pure array) could not make copies of the data due to problems with the network connection
Oct-24	**99.46%**	**99.46%**	
Nov-24	**100%**	**100%**	
Dec-24	**100%**	**100%**	
Jan-25	**99.7%**	**99.7%**	CAV Wifi Internet connection down / Virgin outage nationally - circuits down - resolution Failover to DHH internet connection
Feb-25	**99.9%**	**100%**	10 mins Network Lost on ZC/Desk Phones (Wallfields Only)
Mar-25	**99.98%**	**99.03%**	
Total	**99.81%**	**99.73%**	The target is 99%

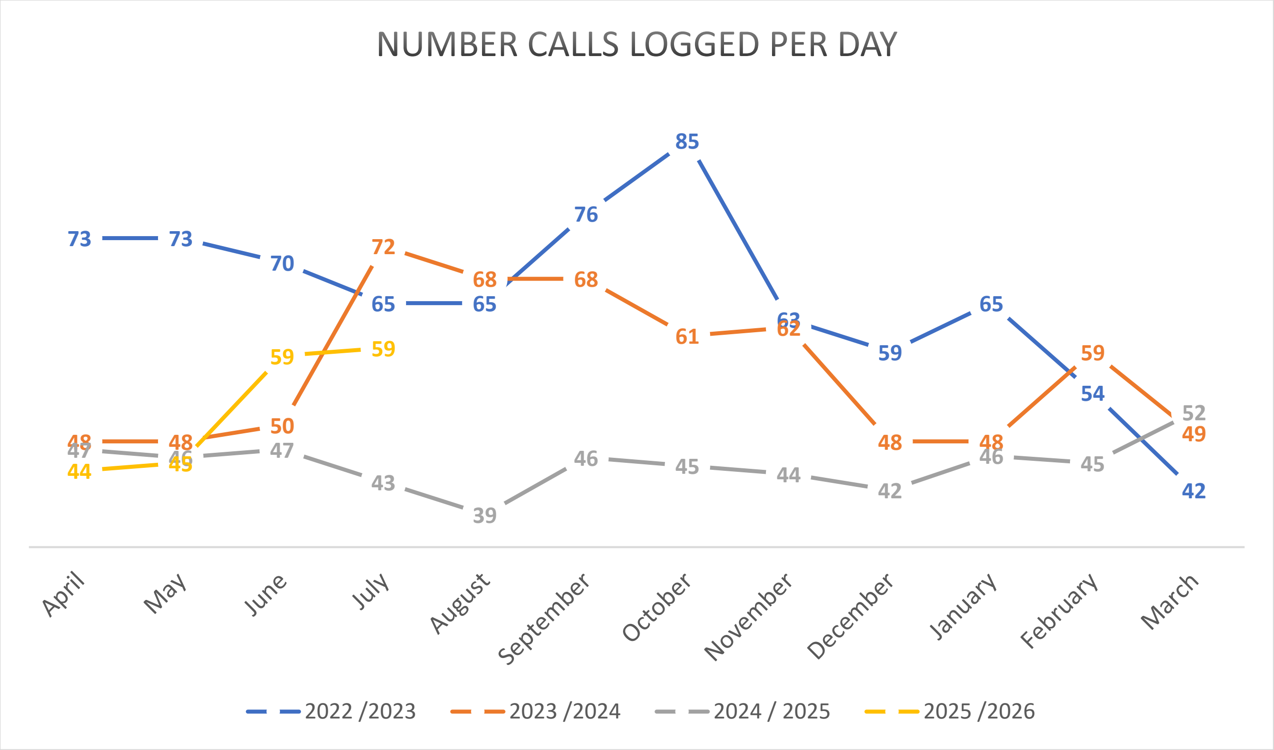
The fiscal year 2024-2025 was characterized by a few notable incidents that impacted overall network stability. The East Herts site concluded the year with an uptime of 99.81%, and the Stevenage site with 99.73%, both of which are just shy of the 99% target.

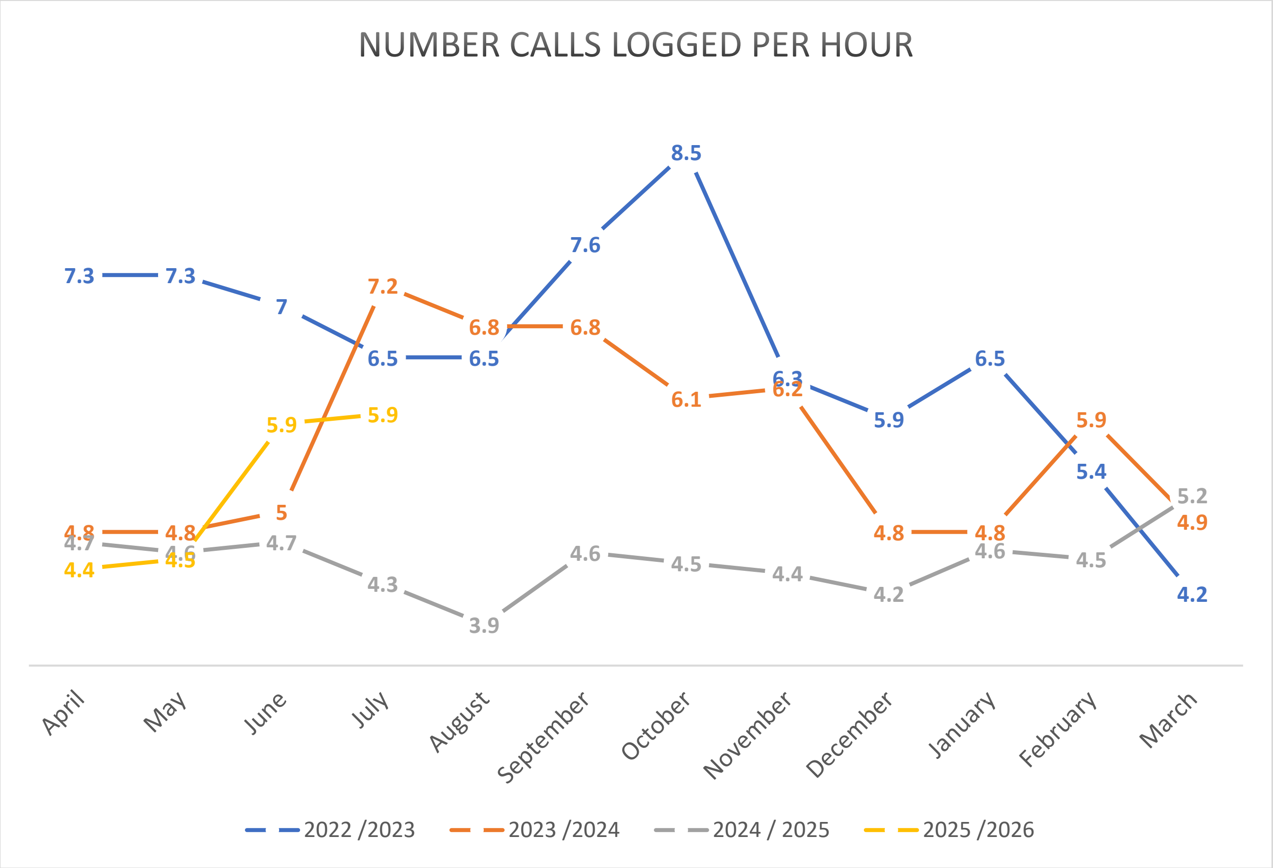
- In April 2024, reports of intermittent Wi-Fi issues were addressed by connecting the majority of staff to public Wi-Fi for a more stable connection, a temporary workaround that was put in place.
- A server storage issue (pure array) in September 2024 prevented the creation of data copies due to network connectivity problems, which resulted in a dip in uptime to 98.6% for East Herts and 98.6% for Stevenage.
- In January 2025, a CAV Wi-Fi internet connection outage, stemming from a national Virgin circuit issue, caused a brief period of downtime before a failover to the DHH internet connection was successful.
- In February 2025, a 10-minute network loss on ZC/Desk Phones at the Wallfields site was recorded, impacting the uptime for East Herts and Stevenage at 99.9% and 99.03% respectively**.**

Current Performance: 2025 – 2026

For the current reporting period, from April to July 2025, the network infrastructure has demonstrated a strong return to stability. Both the East Herts and Stevenage sites have maintained a perfect 100% uptime, with no reported P1 incidents to date. This marks a positive and encouraging start to the fiscal year.

Uptime and P1’s for IT Network infrastructure.			
2025 / 2026			
	East Herts	Stevenage	
Apr-25	**100%**	**100%**	
May-25	**100%**	**100%**	
Jun-25	**100%**	**100%**	
Jul-25	**100%**	**100%**	
Aug-25			
Sep-25			
Oct-25			
Nov-25			
Dec-25			
Jan-26			
Feb-26			
Mar-26			
Total	**100%**	**100%**	The target is 99%


NUMBER CALLS LOGGED PER DAY
73
73
70
65
65
76
85
63
59
65
54
42
48
48
50
72
68
68
61
62
48
48
59
49
47
46
47
43
39
46
45
44
42
46
45
52
44
45
59
59
April
May
June
July
August
September
October
November
December
January
February
March
2022 /2023
2023 /2024
2024 / 2025
2025 /2026


NUMBER CALLS LOGGED PER HOUR
7.3
7.3
7
6.5
6.5
7.6
8.5
6.3
5.9
6.5
5.4
4.2
4.8
4.8
5
7.2
6.8
6.8
6.1
6.2
4.8
4.8
5.9
4.9
4.7
4.6
4.7
4.3
3.9
4.6
4.5
4.4
4.2
4.6
4.5
5.2
4.4
4.5
5.9
5.9
April
May
June
July
August
September
October
November
December
January
February
March
2022 /2023
2023 /2024
2024 / 2025
2025 /2026

The number of calls logged per day and the number of calls logged per hour. The data covers the period from April 2022 to July 2025. These metrics are crucial for assessing the efficiency and workload of the Service Desk and for ensuring that support services are aligned with the organisation's needs.

Performance Analysis: 2022 - 2023
During the 2022-2023 period, the Service Desk recorded an average of 63 calls logged per day, with a corresponding average of 6.3 calls logged per hour. The peak months for call volume were October, with 85 calls per day, and September, with 76 calls per day. The lowest volume was recorded in March, with 42 calls per day. This data suggests a consistent, albeit fluctuating, level of demand for Service Desk support throughout the year.

Performance Analysis: 2023 - 2024
The 2023-2024 period showed a notable decrease in call volume compared to the previous year. The average number of calls logged per day dropped to approximately 55, while the average number of calls logged per hour decreased to 5.5. The highest volume was observed in July, with 72 calls per day, and September and August, both with 68 calls per day. This reduction in call volume may indicate improved system stability or increased efficiency in user self-service.

Performance Analysis: 2024 - 2025
The trend of decreasing call volume continued into the 2024-2025 period. The average number of calls logged per day was approximately 46, and the average number of calls logged per hour was 4.6. The highest volume occurred in March, with 52 calls per day. The consistent reduction in calls over a three-year period is a positive indicator of an overall more stable IT environment.

Current Performance: 2025 - 2026
For the current reporting period from April to July 2025, the call volume shows a mixed trend. In April and May, the number of calls logged per day was 44 and 45, respectively, which is consistent with the lower volumes seen in the previous year. However, in June and July, the volume increased to 59 calls per day, with a corresponding average of 5.9 calls per hour. This represents an increase in demand and will be monitored closely.

In summary, the IT Service Desk has demonstrated a general trend of decreasing call volumes over the past three years, due to a more stable IT environment.

Incidents that are resolved within four hours

Over the entire period of April 2022 to July 2025, the East Herts has demonstrated a slightly higher average incident resolution rate within four hours compared to the Stevenage. The East Herts average is approximately 91.4%, while the Stevenage average is approximately 88.4%. Both sites showed a similar pattern of performance improvement in the 2023-2024 fiscal year, followed by a decline in 2024-2025.

Year on Year	East Herts	Stevenage
April 2022 to March 2023	90.60%	87.53%
April 2023to March 2024	94.25%	93.12%
April 2024to March 2025	88.63%	83.23%
April 2025 to March 2026	92.62%	86.04%

Year-by-Year Performance

A year-by-year comparison reveals the following trends:

- 2022-2023: The East Herts site averaged a resolution rate of approximately 90.60%, which was higher than the Stevenage average of 87.53%.

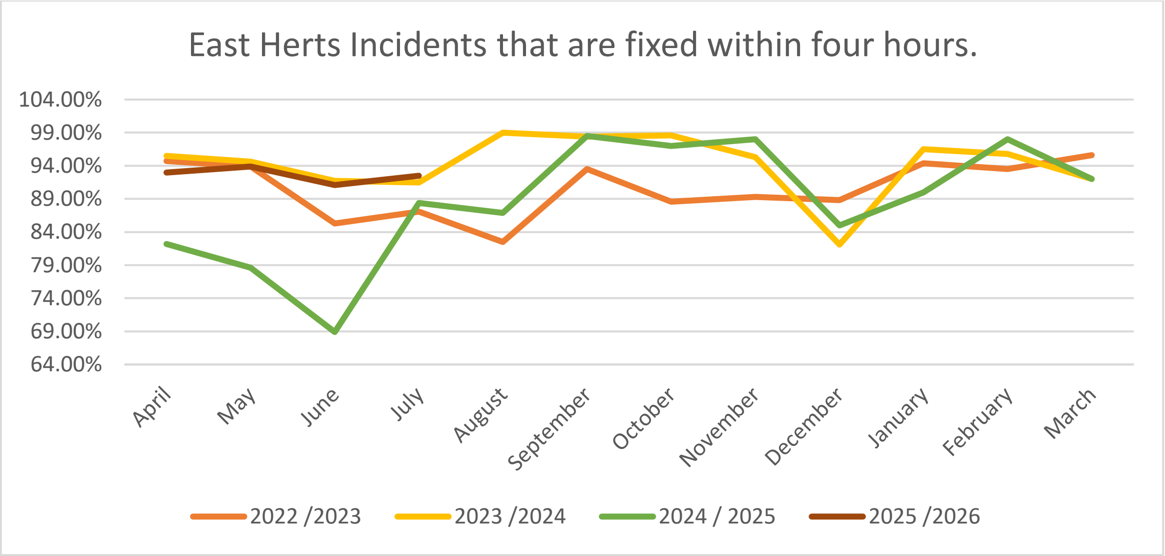
- 2023-2024: Both sites experienced a significant improvement in performance. The East Herts achieved an average of 94.25%, while the Stevenage improved to 93.12%.

- 2024-2025: A decline in performance was observed at both council. East Herts' average resolution rate fell to approximately 88.63%, and Stevenage's average experienced a more significant drop to approximately 83.23%.

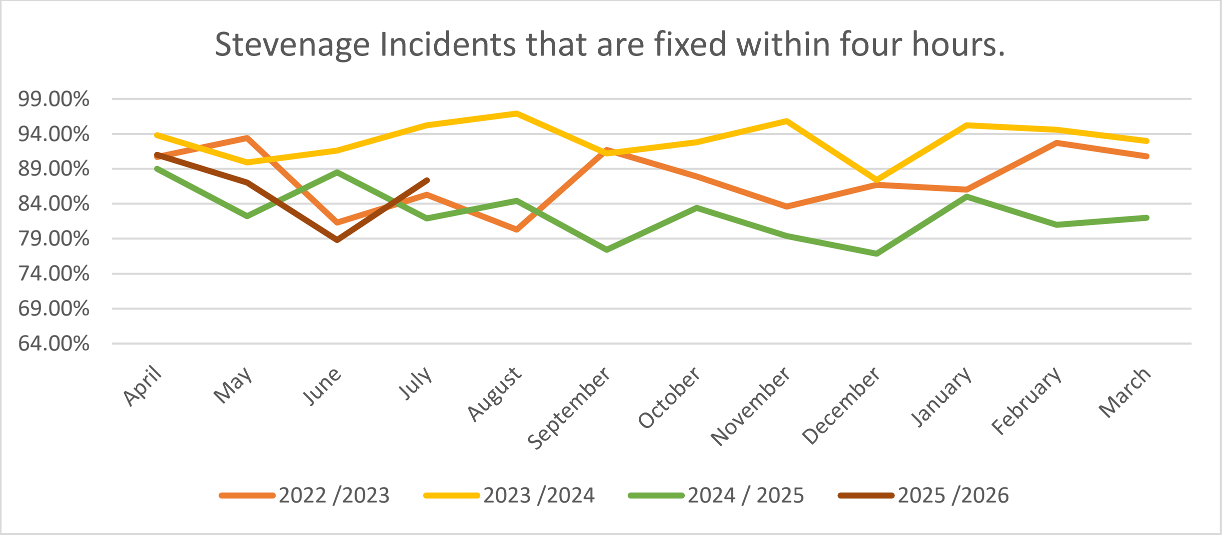
- 2025-2026 (Partial Year): The East Herts is currently averaging 92.62%, while the Stevenage is averaging 86.04%.

The year-on-year data shows an initial improvement followed by a recent decrease in performance. During the fiscal year 2023-2024, East Herts reported a resolution rate of 94.25%, while Stevenage reached 93.12%. The decline observed in 2024-2025 is linked to an organisational restructure and challenges in filling new Service Desk positions due to employment market conditions. Staffing levels were not met until January, resulting in limited resources and affecting resolution times.

The improved performance observed in the current partial year of 2025-2026 is a direct result of the new structure becoming fully operational. The team is now fully staffed and is demonstrating an improved capability to meet the demands of the service.



The resolution of incidents within four hours at the East Herts has shown fluctuations over the reporting period. In the 2022-2023 fiscal year, the average resolution rate was approximately 90.7%. This figure improved to an average of 95% in 2023-2024, demonstrating enhanced efficiency. However, in the 2024-2025 fiscal year, the average rate declined to approximately 88.5%. The performance in the current quarter of 2025-2026 shows a mixed trend, with April and May at 93% and 93.89% respectively, while June shows a slight decrease to 91.09%. and July has recovered to 92.48%.



The Stevenage site's performance has followed a similar, though more pronounced, pattern. The average resolution rate for 2022-2023 was approximately 88.3%, which saw a significant improvement to 93.4% in 2023-2024. In the 2024-2025 fiscal year, the average resolution rate experienced a decline to approximately 83.5%. The current quarter for 2025-2026 reflects a steady start, with rates of 91% in April and 87.02% in May, followed by a decrease to 78.81% in June, and a strong recovery to 87.33% in July.

Service Requests meeting Service Level Agreements (SLAs)

Over the entire period of April 2022 to July 2025 for both the East Herts and Stevenage. Meeting SLAs is a critical metric for assessing the efficiency and effectiveness of the IT support function and for ensuring that user needs are addressed in a timely and consistent manner.

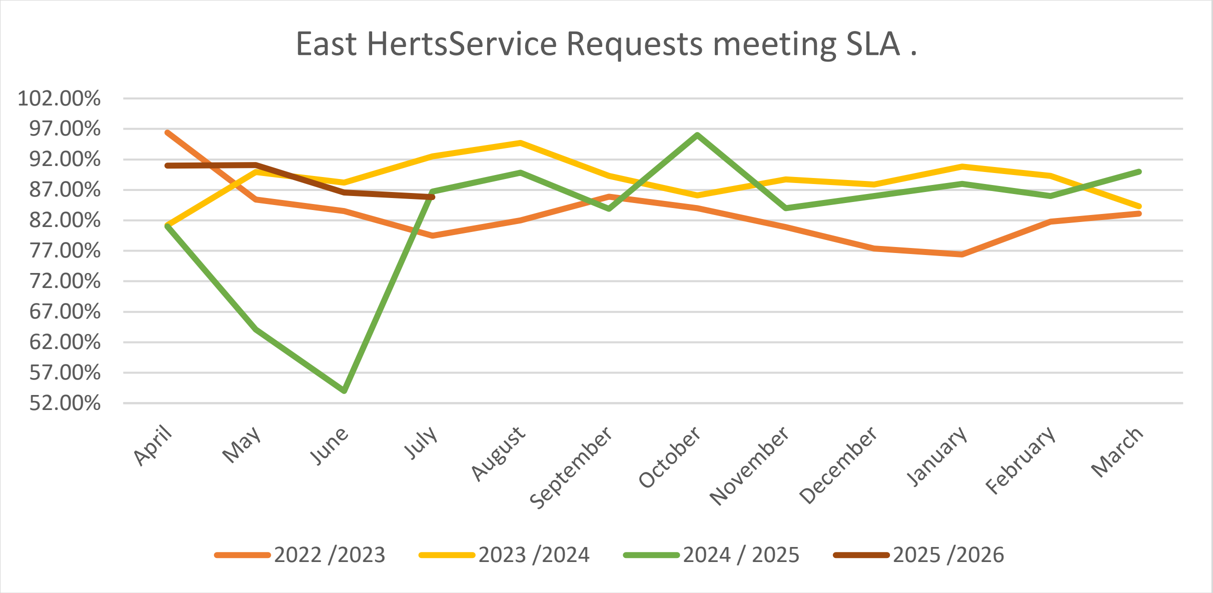
Year on Year	East Herts	Stevenage
April 2022 to March 2023	83.03%	79.19%
April 2023 to March 2024	88.58%	89.21%
April 2024 to March 2025	82.46%	82.89%
April 2025 to March 2026	88.61%	87.50%

Year-on-Year Performance Comparison

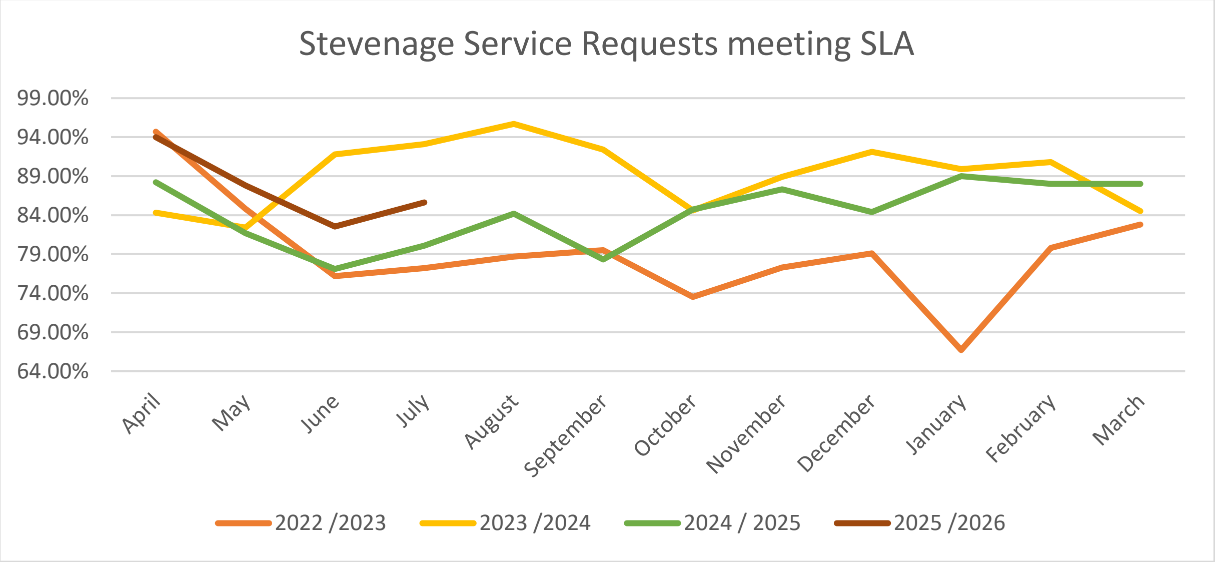
A year-on-year comparison of service request performance reveals the following trends:

- 2022-2023: The East Herts achieved an average SLA compliance rate of 83.03%, which was slightly higher than the Stevenage site's average of 79.19%.
- 2023-2024: Both sites experienced significant improvement. The East Herts average rose to 88.58%, while the Stevenage site's average increased to 89.21%, surpassing East Herts.
- 2024-2025: A decline in performance was observed at both councils. The East Herts average fell to 82.46%, and the Stevenage average decreased to 82.89%.
- 2025-2026 (Partial Year): Both councils are showing a strong recovery. East Herts is currently averaging 88.61% and Stevenage is averaging 87.50%.

The data indicates a cyclical performance pattern over the reporting period. Both East Herts and Stevenage demonstrated a notable improvement in SLA compliance from the 2022-2023 fiscal year to 2023-2024. This was followed by a corresponding decline in performance during the 2024-2025 period. This decline can be directly attributed to a combination of factors, including the two elections, a departmental restructure, and challenges in filling new service desk positions due to employment market conditions. These staffing challenges were not resolved until January, which impacted the team's capacity to meet service level agreements. The current data for 2025-2026 shows a positive turnaround, with both sites on a trajectory to regain the high performance levels seen in 2023-2024. With the new structure now fully staffed, have been effective in restoring stability and improving performance.



The performance of the East Herts in meeting service request SLAs has shown variability over the past three fiscal years. In the 2022-2023 fiscal year, the average SLA compliance rate was approximately 84.4%. This performance saw an improvement in 2023-2024, with the average rate increasing to approximately 88.5%. However, in the 2024-2025 fiscal year, the average compliance rate declined to approximately 78.4%. The current quarter for 2025-2026 shows a positive trend, with an April rate of 91.00%, May at 91.07%, and June at 85.81%.



The Stevenage performance has followed a similar pattern. The average SLA compliance rate for 2022-2023 was approximately 81.3%. This rate saw a notable improvement in 2023-2024, reaching an average of 89.9%. Similar to East Herts, the 2024-2025 fiscal year was characterised by a decline, with the average compliance rate dropping to approximately 84.7%. The current quarter for 2025-2026 shows a promising start, with rates of 84.30% in April, 87.81% in May, and 82.54% in June at 82.54%, and July at 85.64%.

Service Desk First-Line Fix Rate

This detailed analysis of the IT Service Desk's performance in resolving incidents at the first point of contact, known as the "first-line fix rate." This metric is a key indicator of the efficiency and capability of the frontline support team. The data covers the period from April 2022 to July 2025 for both the East Herts and Stevenage.

Year on Year	East Herts	Stevenage
April 2022 to March 2023	87.31%	77.85%
April 2023to March 2024	84.62%	77.44%
April 2024to March 2025	78.18%	82.05%
April 2025 to March 2026	96.50%	96.24%

Year-by-Year Performance Comparison

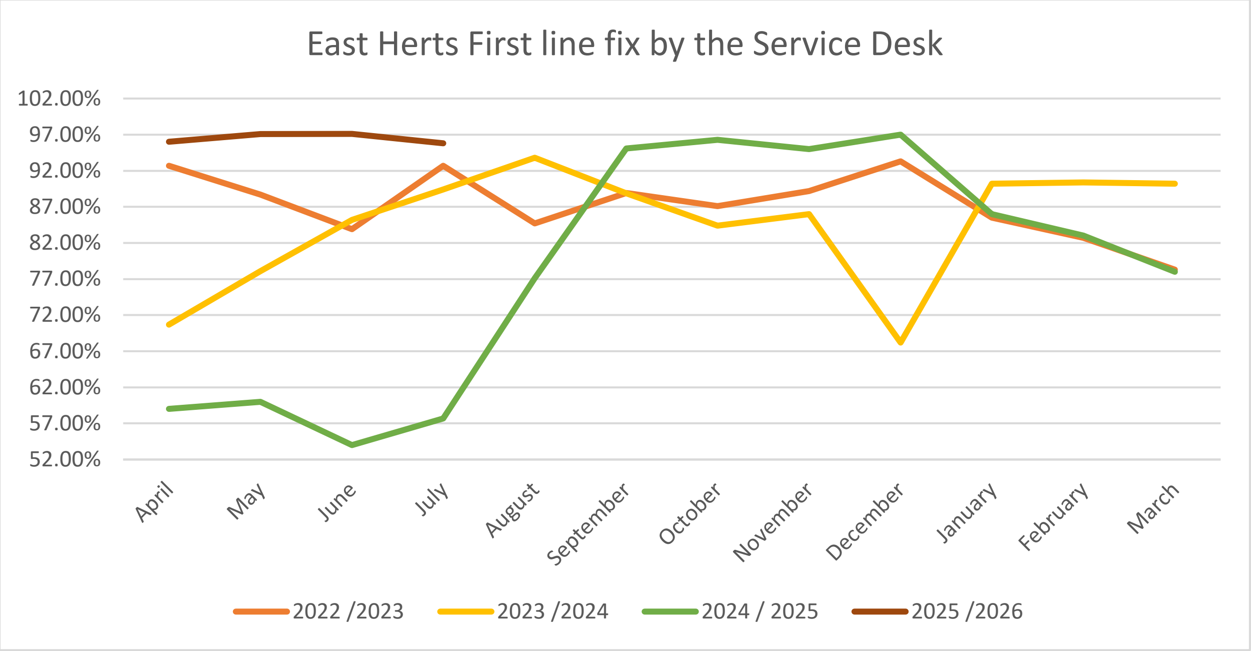
A year-on-year comparison of the first-line fix rates reveals the following trends:

- April 2022 to March 2023: The East Herts site's average resolution rate was 87.31%, which was notably higher than the Stevenage site's average of 77.85%.
- April 2023 to March 2024: The East Herts site experienced a decline to 84.62%, while Stevenage also saw a slight decrease to 77.44%.
- April 2024 to March 2025: A significant shift occurred in this period. The East Herts site's performance declined to 78.18%, while the Stevenage site's performance improved to 82.05%.
- April 2025 to March 2026 (Partial Year): Both sites have shown a remarkable recovery, with East Herts achieving an average of 96.50% and Stevenage at 96.24%.

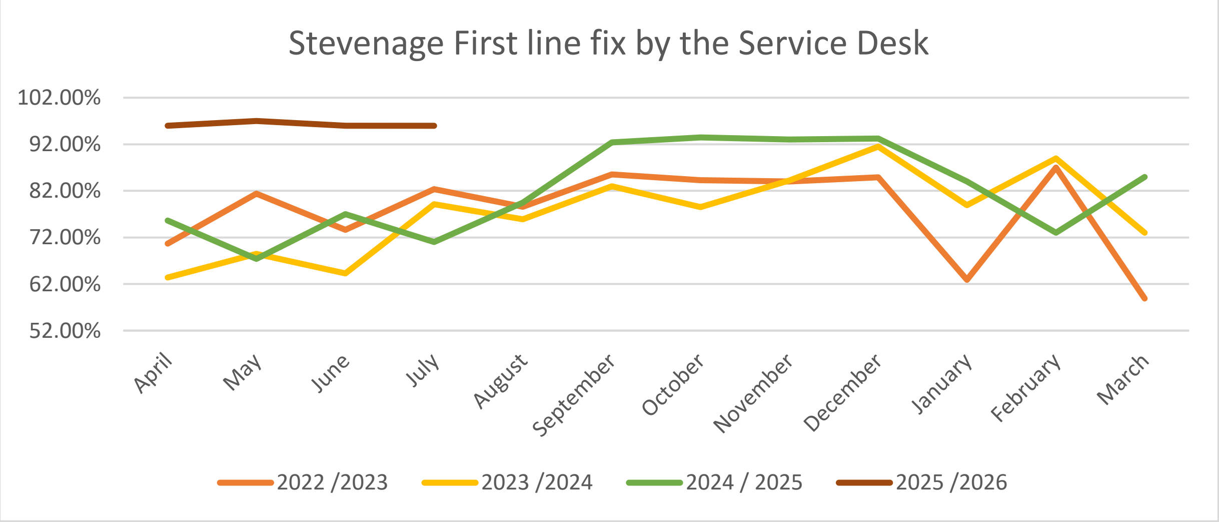
Summary of Year-on-Year Performance

The data show a fluctuating performance trend over the three-year period, with a clear decline in the first-line fix rate for both councils during the 2024-2025 fiscal year. This decline can be attributed to a combination of factors, including the two elections, a departmental restructure, and challenges in filling new Service Desk positions due to employment market conditions. These staffing challenges were not fully resolved until January.

The data for the current fiscal year (2025-2026), however, shows a significant and positive reversal of this trend. The substantial increase in performance observed from April 2025 onwards is a direct result of the new organisational structure being fully implemented. The new End User Compute team, positioned above the Service Desk team, has enhanced the overall efficiency and frontline resolution capabilities, allowing the Service Desk to focus on first-line fixes. The average first-line fix rates for East Herts and Stevenage have not only recovered but have surpassed the performance levels of all previous years.



The first-line fix rate for the East Herts has shown significant fluctuations over the reporting period. In the 2022-2023 fiscal year, the average rate was a robust 87.31%. This performance saw a decline in the 2023-2024 fiscal year, with the average rate dropping to 84.62%. The trend of decline continued into 2024-2025, where the average rate fell to 78.18%. However, the current quarter of 2025-2026 shows a remarkable recovery, with an average rate of 96.50%. Specifically, the data shows rates of 96.00% in April, 97.09% in May, 97.10% in June, and 95.80% in July, indicating a significant improvement in the team's ability to resolve issues on the first call.



The Stevenage performance has followed a similar, albeit more complex, pattern. The average first-line fix rate for 2022-2023 was 77.85%. This rate saw a notable improvement in 2023-2024, reaching an average of 82.05%. However, a decline was observed in 2024-2025, with the average rate falling to 78.18%. The current quarter for 2025-2026 reflects a strong recovery, with a current average of 96.24%. The data shows rates of 96.00% in April, 97.00% in May, 95.99% in June, and 95.97% in July, which represents a significant improvement over previous years.

Email and Web Security Performance

The data show a detailed analysis of the council's email traffic and security performance for the period of April 2023 through July 2025. The data presented covers the total volume of inbound email, the number of inbound malware and unsafe attachments detected and stopped, and the number of malware incidents from unsafe website clicks. These metrics are critical for assessing the scale of our digital communication and the effectiveness of our security protocols in an environment of consistently high traffic and evolving threats.

Email volumes across both councils

	Total Inbound Email	Total Outbound Email	
Apr-23	358,308.00	233,767.00	592,075.00
May-23	503,630.00	116,497.00	620,127.00
Jun-23	452,303.00	118,210.00	570,513.00
Jul-23	266,901.00	112,914.00	379,815.00
Aug-23	495,394.00	116,217.00	611,611.00
Sep-23	1,108,173.00	119,947.00	1,228,120.00
Oct-23	347,094.00	121,378.00	468,472.00
Nov-23	284,369.00	136,565.00	420,934.00
Dec-23	212,251.00	99,785.00	312,036.00
Jan-24	274,767.00	131,409.00	406,176.00
Feb-24	403,864.00	127,343.00	531,207.00
Mar-24	363,438.00	153,871.00	517,309.00
Apr-24	280,794.00	135,806.00	416,600.00
May-24	281,837.00	137,223.00	419,060.00
Jun-24	263,622.00	131,539.00	395,161.00
Jul-24	295,412.00	142,374.00	437,786.00
Aug-24	286,738.00	132,572.00	419,310.00
Sep-24	286,996.00	137,445.00	424,441.00
Oct-24	300,385.00	146,200.00	446,585.00
Nov-24	287,996.00	137,982.00	425,978.00
Dec-24	255,751.00	110,633.00	366,384.00
Jan-25	313,652.00	190,906.00	504,558.00
Feb-25	439,309.00	149,476.00	588,785.00
Mar-25	460,054.00	229,608.00	689,662.00
Apr-25	415,525.00	132,333.00	547,858.00
May-25	281,059.00	127,858.00	408,917.00
Jun-25	340,394.00	131,829.00	472,223.00
Jul-25	300,401.00	144,724.00	445,125.00

Inbound Malware Detected and Stopped	
Apr-23	24
May-23	61
Jun-23	6
Jul-23	16
Aug-23	29
Sep-23	12
Oct-23	22
Nov-23	31
Dec-23	34
Jan-24	13
Feb-24	20
Mar-24	12
Apr-24	16
May-24	11
Jun-24	11
Jul-24	16
Aug-24	14
Sep-24	20
Oct-24	20
Nov-24	25
Dec-24	10
Jan-25	10
Feb-25	12
Mar-25	22
Apr-25	18
May-25	4
Jun-25	1
Jul-25	4

	Attachment Sandboxed	Unsafe Attachment
Mar-24	46,269.00	7
Apr-24	45,311.00	6
May-24	46,631.00	3
Jun-24	45,511.00	2
Jul-24	50,275.00	7
Aug-24	43,729.00	0
Sep-24	44,532.00	14
Oct-24	47,282.00	17
Nov-24	43,913.00	8
Dec-24	38,348.00	1
Jan-25	47,701.00	7
Feb-25	43,104.00	2
Mar-25	49,730.00	5
Apr-25	41,656.00	5
May-25	41,447.00	11
Jun-25	40,839.00	3
Jul-25	43,812.00	3

Analysis of Email Volumes and Malware

The data reveals a consistently high volume of email traffic, which necessitates a robust security infrastructure. The relationship between email volume and the number of detected threats is a key area of analysis.

- 2023-2024: The average monthly inbound email volume was approximately 537,000, with a significant peak in September 2023 of over 1.1 million emails, which has been identified as a Denial of Service (DOS) email attack. This high volume of traffic was met with a total of 269 detected inbound malware incidents and 133 unsafe attachments. This demonstrates the scale of threats our systems must manage daily.

- 2024-2025: While the average monthly email volume was slightly lower at approximately 508,000, the security team successfully detected and stopped a total of 176 malware incidents and 122 unsafe attachments, a notable decrease from the previous year. This reduction indicates a clear improvement in the effectiveness and proactive nature of our security measures, despite a continued high volume of email traffic.

- 2025-2026 (Partial Year):_ The data for the current quarter from April to July 2025 shows a further reduction in detected threats. The total number of malware incidents was only 25, and unsafe attachments totalled 11, even with a recent monthly average of approximately 444,000 emails. This positive trend continues, with June and July recording extremely low numbers of incidents.

	Safe Click	Unsafe Click
Mar-24	4,031.00	3
Apr-24	11,318.00	21
May-24	13,343.00	10
Jun-24	13,877.00	34
Jul-24	16,180.00	28
Aug-24	16,390.00	46
Sep-24	17,994.00	36
Oct-24	20,049.00	26
Nov-24	18,320.00	21
Dec-24	15,306.00	19
Jan-25	17,122.00	15
Feb-25	15,461.00	53
Mar-25	15,938.00	20
Apr-25	60,953.00	60
May-25	77,461.00	273
Jun-25	22,324.00	17
Jul-25	24,401.00	30

Analysis of Unsafe Website Clicks

The number of malware incidents resulting from unsafe website clicks is a critical measure of user security awareness and the effectiveness of our web filtering.

- 2023-2024: A total of 231 incidents from unsafe website clicks were recorded. The highest number of incidents occurred in July 2023, with 46 cases.
- 2024-2025: A total of 329 incidents from unsafe website clicks were recorded. The highest number of incidents for this period was in August 2024 with 46 cases.
- 2025-2026 (Partial Year): The data for the current quarter shows a significant and concerning spike in these types of incidents. A total of 380 cases were recorded from April to July 2025, with a particularly high volume of 273 incidents in May alone.

Combined Security Incident Analysis

It is important to note that the tracking for both unsafe attachments and unsafe website clicks began in March 2024. A year-on-year analysis of all security incidents—inbound malware, unsafe attachments, and unsafe website clicks—reveals a shift in the nature of our primary security threats.

- 2023-2024: A total of 633 security incidents were recorded, with the majority being email-based threats (402 incidents, or 63.5%).
- 2024-2025: The total number of security incidents remained relatively consistent at 627. However, the proportion of email-based threats decreased significantly, while incidents from unsafe website clicks increased to become the dominant threat vector (329 incidents, or 52.5%).
- 2025-2026 (Partial Year): The total number of incidents for the current period is 416, with the overwhelming majority coming from unsafe website clicks (380 incidents, or 91.3%). This trend highlights a fundamental change in the threat landscape, with user behaviour and web browsing now representing the most significant security risk.

Analysis of Inbound Malware Detections

This report provides a detailed breakdown of the 296 total inbound malware instances detected and stopped by our security systems from April 2023 to April 2024. The analysis identifies the types of threats, their prevalence, and a brief description of their functionality.

Summary of Malware Detections by Type

The following table lists the number of times each type of malware was detected across the entire reporting period, sorted by total count.

Malware Type	Description	Total Count
CXmail/Phish-AC	A Mimecast-specific detection for a sophisticated phishing campaign.	17
MC-Html.Phishing.AF-1	A specific variant of HTML-based phishing attacks designed to trick users into providing sensitive information.	15
MC-Html.Phishing.ATO-1	A type of phishing attack designed for "account takeover."	14
MC-Html.Malware.Agent-2	A malware agent often delivered via HTML or JavaScript attachments, designed to install a Trojan and provide an attacker with control over the system.	13
Exploit.MathType-Obfs.Gen	An exploit targeting a known vulnerability in the MathType equation editor to deliver malware.	12
MC-Html.Phishing.JSAtob	Phishing attack using obfuscated JavaScript within an HTML attachment to create a fake login page and steal credentials.	9
MC-Html.Obfus.WTP-1/2	Malware using obfuscation techniques to hide its malicious intent from security scanners.	9
Other	A category for less common or unclassified threats.	9
JS:Trojan.Cryxos	A Trojan, typically delivered through JavaScript, used to install malicious software on a user's system.	7
CXmail/MalHtm-L	A malicious HTML file delivered via email, often a phishing attempt that exploits vulnerabilities in email clients.	7
MC-Html.Phishing.Script0x-1	A phishing attack using an HTML file with obfuscated script, similar to JSAtob, to evade detection.	6
AdvancedPhishing	A highly sophisticated phishing campaign that uses advanced techniques to evade detection.	6
UrlReputationScan	A detection of a malicious URL that has been flagged by a URL reputation scan, indicating it's a known threat.	6
Html.Phishing.Bank-1014	A phishing attack specifically designed to impersonate a banking institution.	4

Detailed Breakdown by Month

This section provides a month-by-month analysis of the detected malware, showing the specific types and their frequency for that period.

April 2023

- Total Detections: 24
- Key Threats: MC-Html.Phishing.JSAtob-1 (7 instances, 29%), GT:JS.Email.Phishing.1... (3 instances, 12%). This suggests a focus on HTML and JavaScript-based phishing.

May 2023

- Total Detections: 61
- Key Threats: MC-Html.Malware.Agent-2, Trojan.Phishing.ANQ (15 instances, 25%), JS:Trojan.Cryxos.12832... (10 instances, 16%). This month saw a high volume of trojan and malware agent attacks.

June 2023

- Total Detections: 6
- Key Threats: A diverse mix of single-instance threats, including GT:JS.Email.Phishing.1... and MC-Html.Phishing.JSRedir-13.

July 2023

- Total Detections: 16
- Key Threats: CXmail/MalHtm-L (4 instances, 25%), MC-Html.Phishing.JSRedir-7 (2 instances, 12%). This month had a recurrence of malicious HTML emails.

August 2023

- Total Detections: 29
- Key Threats: CXmail/MalHtm-L, MC-Html.Phishing.FormUnescape-1 (7 instances, 24%), MC-Trojan.Gen.ZE (4 instances, 14%). A mix of phishing and trojan attacks were prevalent.

September 2023

- Total Detections: 12
- Key Threats: MC-Html.Phishing.JBU-4 (3 instances, 25%), MC-Html.Phishing.Script0x-1 (3 instances, 25%). This period saw a focused campaign using HTML phishing attacks.

October 2023

- Total Detections: 22
- Key Threats: MC-Html.Phishing.AF-1 (9 instances, 41%), MC-Html.Obfus.WTP-2 (4 instances, 18%). A high concentration on a specific phishing variant was observed.

November 2023

- Total Detections: 31
- Key Threats: CXmail/Phish-AC, Generic.JS.Office.ScamPage... (16 instances, 52%). This was a highly successful and large-scale phishing campaign impersonating office services.

December 2023

- Total Detections: 34
- Key Threats: CXmail/OlEdI-BI, Exploit.MathType... (11 instances, 32%), MC-HTML.Phishing.ATO-1 (11 instances, 32%). This month saw the emergence of a new exploit-based threat alongside persistent phishing.

January 2024

- Total Detections: 13
- Key Threats: CXmail/MalHtm-L, CXmail/Phish-AI... (5 instances, 38%).

February 2024

- Total Detections: 20
- Key Threats: MC-Html.Malware.Agent-2 (3 instances, 15%), AdvancedPhishing, AvScanning... (3 instances, 15%). This suggests more sophisticated, multi-faceted attacks were being deployed.

March 2024

- Total Detections: 12
- Key Threats: MC-Trojan.Gen.RE... (2 instances, 17%), MC-Html.Obfus.WTP-2 (2 instances, 17%).

April 2024

- Total Detections: 16
- Key Threats: CXmail/Phish-Z (4 instances, 25%), MC-Html.Obfus.WTP-2 (5 instances, 38%).

Conclusion

The analysis demonstrates that phishing attacks remain the most consistent and dominant threat, often utilising HTML and JavaScript attachments to bypass defences. The data also highlights an evolving threat landscape, with periods of high-volume campaigns and the emergence of more sophisticated attacks like exploits and trojans. This information is crucial for developing a targeted security strategy that combines robust technical controls with ongoing user education.