EXTERNAL: CSV Changes for Vulnerability Variance Reports

On September 19, 2023, there will be a production release to improve the report download experience in the Alert Logic console. As part of this release, CSV generation for the Vulnerability Variance reports will be decoupled from data processing resulting in the following changes to Full and Summary Data CSV report options:

- Full and Summary Data CSV reports will no longer include columns/fields that are duplicates, have been deprecated, and/or are used exclusively for internal purposes.
- Summary Data CSV reports will be updated to focus primarily on the data values presented in filters, visualizations, and tables of interactive reports in the Alert Logic console.
- The order of columns/fields in the CSV reports may be modified as a result of adding and/or removing fields.
- CSV filenames and column/field names will be updated to be consistent across reports.

Daily Vulnerability Variance Report

The table below captures the specific changes to the Full Data and Summary Data CSV files for the Daily Vulnerability Variance report.

Report Option	Current Columns and Order	New Columns and Order (Sept 12)	Summary of Changes
Full Data (CSV)	1. Day of Vuln Date 2. Variance 3. New 4. Vulnerability Name 5. IP Address 6. Host Name 7. Operating System 8. Protocol 9. Environment Id 10. Port 11. Service Type 12. CVE 13. Vulnerability Span ID 14. CVSS Score 15. Severity 16. PCI Severity 17. CVSS Vector 18. Category 19. Customer Account 20. Deployment Name 21. ~~Relative Day~~ 22. VPC/Network 23. ~~Customer Filter (T|F)~~ 24. Description 25. ~~environment_id (vulnerability_variance_details_daily)~~	1. Day of Vuln Date 2. Variance 3. New 4. Vulnerability Name 5. IP Address 6. Host Name 7. Operating System 8. Protocol 9. Deployment ID 10. Port 11. Service Type 12. CVE 13. Vulnerability Span ID 14. CVSS Score 15. Severity 16. PCI Severity 17. CVSS Vector 18. Category 19. Customer Account 20. Deployment Name 21. VPC/Network 22. Description	☑ Rename 1 column/field (highlighted in Blue) • “Environment Id” changed to “Deployment ID” ☑ Remove 23 columns/fields (highlighted in Red) ☑ Change “Day of Vuln Date” from Custom format (6-Aug-23) to Date format (8/6/23) ☑ Rename CSV file to “Daily_Vulnerability_Variance_Full_Data.csv”

	26. ~~Evidence~~ 27. ~~Fixed~~ 28. ~~Host IP Address~~ 29. ~~Managed Account Id~~ 30. ~~Managed Account Name~~ 31. ~~Managed By Account Id~~ 32. ~~Managed By Account Name~~ 33. ~~New(dw)~~ 34. ~~Relative Day (copy)~~ 35. ~~Vuln Date~~ 36. ~~Vuln Day~~ 37. ~~vulnerability_span_id (vulnerability_variance_details_daily)~~ 38. ~~Vulnerable Asset Key~~ 39. ~~vulnerable_asset_key (vulnerability_variance_details_daily)~~ 40. ~~#NAME?~~ 41. ~~AVG(1)~~ 42. ~~managed_account_id (vulnerability_variance_details_daily)~~ 43. ~~New Count~~ 44. ~~Number of Records~~ 45. ~~unresolved Count~~		
Summary Data (CSV)	1. Day of Vuln Date 2. Variance 3. New 4. Vulnerability Name 5. IP Address 6. Host Name 7. ~~Operating System~~ 8. Protocol 9. Environment Id 10. Port 11. ~~Service Type~~ 12. ~~CVE~~ 13. ~~Vulnerability Span ID~~ 14. CVSS Score 15. Severity 16. ~~PCI Severity~~ 17. ~~CVSS Vector~~ 18. ~~AVG(1)~~ 19. ~~CVSS rank~~	1. Day of Vuln Date 2. Variance 3. New 4. Vulnerability Name 5. IP Address 6. Host Name 7. Protocol 8. Deployment ID 9. Port 10. CVSS Score 11. Severity 12. Category 13. Customer Account 14. Deployment Name 15. VPC/Network	☑ Rename 1 column/field (highlighted in Blue) • “Environment Id” changed to “Deployment ID” ☑ Remove 8 columns/fields (highlighted in Red) ☑ Add 4 columns/fields (highlighted in Green) • Customer Account • Deployment Name • VPC/Network • Category ☑ Change “Day of Vuln Date” from Custom format (6-Aug-23) to Date format (8/6/23) ☑ Rename CSV file to “Daily_Vulnerability_Variance_Summary_D

			ata.csv”

Weekly Vulnerability Variance Report

The table below captures the specific changes to the Full Data and Summary Data CSV files for the Weekly Vulnerability Variance report.

Report Option	Current Columns and Order	New Columns and Order (Sept 12)	Summary of Changes
Full Data (CSV)	1. Day of Vuln Week 2. Variance 3. New 4. Vulnerability Name 5. IP Address 6. Host Name 7. Operating System 8. Protocol 9. Environment Id 10. Port 11. Service Type 12. CVE 13. Vulnerability Span ID 14. CVSS Score 15. Severity 16. PCI Severity 17. CVSS Vector 18. Category 19. Customer Account 20. Deployment Name 21. ~~Relative week~~ 22. VPC/Network 23. ~~Customer Filter (T|F)~~ 24. Description 25. ~~environment_id (vulnerability_variance_details_weekly)~~ 26. ~~Evidence~~ 27. ~~Fixed~~ 28. ~~Host Ip Address~~ 29. ~~Managed Account Id~~ 30. ~~Managed Account Name~~ 31. ~~Managed By Account Id~~ 32. ~~Managed By Account Name~~ 33. ~~New(dw)~~ 34. ~~Relative week (copy)~~ 35. ~~Severity bars~~	1. Day of Vuln Week 2. Variance 3. New 4. Vulnerability Name 5. IP Address 6. Host Name 7. Operating System 8. Protocol 9. Deployment ID 10. Port 11. Service Type 12. CVE 13. Vulnerability Span ID 14. CVSS Score 15. Severity 16. PCI Severity 17. CVSS Vector 18. Category 19. Customer Account 20. Deployment Name 21. VPC/Network 22. Description	☑ Rename 1 column/field (highlighted in Blue) • “Environment Id” changed to “Deployment ID” ☑ Remove 25 columns/fields (highlighted in Red) ☑ Change “Day of Vuln Week” from Custom format (6-Aug-23) to Date format (8/6/23) ☑ Rename CSV file to “Weekly_Vulnerability_Variance_Full_Data.csv”

	36. ~~Vuln Date~~ 37. ~~Vuln Week~~ 38. ~~vulnerability_span_id (vulnerability_variance_keys_weekly)~~ 39. ~~Vulnerable Asset Key~~ 40. ~~vulnerable_asset_key (vulnerability_variance_details_weekly)~~ 41. ~~#NAME?~~ 42. ~~AVG(1)~~ 43. ~~managed_account_id (vulnerability_variance_details_weekly)~~ 44. ~~New Count~~ 45. ~~Number of Records~~ 46. ~~Unresolved~~ 47. ~~Count~~		
Summary Data (CSV)	1. Day of Vuln Week 2. Variance 3. New 4. Vulnerability Name 5. IP Address 6. Host Name 7. ~~Operating System~~ 8. Protocol 9. Environment Id 10. Port 11. ~~Service Type~~ 12. ~~CVE~~ 13. ~~Vulnerability Span ID~~ 14. CVSS Score 15. Severity 16. ~~PCI Severity~~ 17. ~~CVSS Vector~~ 18. ~~AVG(1)~~ 19. ~~CVSS rank~~	1. Day of Vuln Week 2. Variance 3. New 4. Vulnerability Name 5. IP Address 6. Host Name 7. Protocol 8. Deployment ID 9. Port 10. CVSS Score 11. Severity 12. Category 13. Customer Account 14. Deployment Name 15. VPC/Network	☑ Rename 1 column/field (highlighted in Blue) • Environment Id (change to Deployment ID) ☑ Remove 8 columns/fields (highlighted in Red) ☑ Add 4 columns/fields (highlighted in Green) • Customer Account • Deployment Name • VPC/Network • Category ☑ Change “Day of Vuln Week” from Custom format (6-Aug-23) to Date format (8/6/23) ☑ Rename CSV file to “Weekly_Vulnerability_Variance_Summary_Data.csv”

Monthly Vulnerability Variance Report

The table below captures the specific changes to the Full Data and Summary Data CSV files for the Monthly Vulnerability Variance report.

Report Option	Current Columns and Order	New Columns and Order (Sept 12)	Summary of Changes
Full Data (CSV)	1. Day of Vuln Month 2. Variance 3. New 4. Vulnerability Name 5. IP Address 6. Host Name 7. Operating System 8. Protocol 9. Environment Id 10. Port 11. Service Type 12. CVE 13. Vulnerability Span ID 14. CVSS Score 15. Severity 16. PCI Severity 17. CVSS Vector 18. Category 19. Customer Account 20. Deployment Name 21. Relative month 22. VPC/Network 23. Customer Filter (T|F) 24. Description 25. environment_id (vulnerability_variance_details_monthly) 26. Evidence 27. Fixed 28. Host IP Address 29. Managed Account Id 30. Managed Account Name 31. Managed By Account Id 32. Managed By Account Name 33. New(dw) 34. Relative month (copy) 35. Vuln Date 36. Vuln Month 37. vulnerability_span_id (vulnerability_variance_keys_monthly) 38. Vulnerable Asset Key 39. vulnerable_asset_key (vulnerability_variance_details_m	1. Day of Vuln Month 2. Variance 3. New 4. Vulnerability Name 5. IP Address 6. Host Name 7. Operating System 8. Protocol 9. Deployment ID 10. Port 11. Service Type 12. CVE 13. Vulnerability Span ID 14. CVSS Score 15. Severity 16. PCI Severity 17. CVSS Vector 18. Category 19. Customer Account 20. Deployment Name 21. VPC/Network 22. Description	☑ Rename 1 column/field (highlighted in Blue) • “Environment Id” changed to “Deployment ID” ☑ Remove 23 columns/fields (highlighted in Red) ☑ Change “Day of Vuln Month” from Custom format (31-May-23) to Date format (5/31/23) ☑ Rename CSV file to “Monthly_Vulnerability_Variance_Full_Data.csv”

	onthly) 40. #NAME? 41. AVG(1) 42. managed_account_id (vulnerability_variance_details_monthly) 43. New Count 44. Number of Records 45. Unresolved Count		
Summary Data (CSV)	1. Day of Vuln Month 2. Variance 3. New 4. Vulnerability Name 5. IP Address 6. Host Name 7. ~~Operating System~~ 8. Protocol 9. Environment Id 10. Port 11. ~~Service Type~~ 12. ~~CVE~~ 13. ~~Vulnerability Span ID~~ 14. CVSS Score 15. Severity 16. ~~PCI Severity~~ 17. ~~CVSS Vector~~ 18. ~~AVG(1)~~ 19. ~~CVSS rank~~	1. Day of Vuln Month 2. Variance 3. New 4. Vulnerability Name 5. IP Address 6. Host Name 7. Protocol 8. Deployment ID 9. Port 10. CVSS Score 11. Severity 12. Category 13. Customer Account 14. Deployment Name 15. VPC/Network	☑ Rename 8 columns/fields (highlighted in Blue) • Environment Id (change to Deployment ID) ☑ Remove 8 columns/fields (highlighted in Red) ☑ Add 4 columns/fields (highlighted in Green) • Customer Account • Deployment Name • VPC/Network • Category ☑ Change “Day of Vuln Month” from Custom format (31-May-23) to Date format (5/31/23) ☑ Rename CSV file to “Monthly_Vulnerability_Variance_Summary_Data.csv”