# THIRD PARTY CYBER SECURITY METRICS

**Prepared By: - Cyber Security and Technology Risk**

**Version: - 1.0**

**Effective Date: - June 01, 2024**

**INTRODUCTION:**

The Arabelle Solutions (ARS) Third-Party Cyber Security Metrics document outlines the cyber security metric requirements applicable to Critical Arabelle Solutions Third Parties, including suppliers and joint ventures. These metrics are to be provided to Arabelle Solutions 3rd Party Security (3PS) team at the noted frequency for each metric below. The metrics should be submitted to the following email address:

**itrisk3ps@arabellesolutions.com**

Arabelle Solutions reserves the right to update this document from time to time.

**1. Asset Management**

Frequency – Monthly

| Metric Title | Metric Explanation | Calculation Method | Scope | Target |
|---|---|---|---|---|
| Asset visibility | Visibility to the assets used by Third-Party supporting ARS engagement(s) | Total # of Third-Party assets (laptops or workstations) assigned to employees in ARS engagement(s) as per the details registered in Third Party asset management solution / Total # of Third-Party employees working for ARS engagement(s) excluding employees having ARS assets (for the period in scope) | Third-Party laptops/workstations, Third-Party personnel | 85% |
| | Visibility to the assets provided by GE to the Third-party supporting ARS engagement(s) | Informational, capture the total # of ARS assets (For the period in scope) | ARS laptops/workstations | N.A. |
| | Visibility to the assets provided by ARS to the Third-Party and returned back to ARS | Informational, capture the total # of ARS assets returned to ARS by the Third Party (for the period in scope) | ARS laptops/workstations | N.A. |

**2. Cyber Incident Response**

Frequency – Monthly

| Metric Title | Metric Explanation | Calculation Method | Scope | Target |
|---|---|---|---|---|
| Cyber incident reporting | Visibility on to the cyber events or cyber incidents which could potentially have an impact to ARS information, data or systems | Total # of cyber events or cyber incidents reported to ARS Cyber Incident Response Team at Raiseaconcern@arabellesolutions.com through mail / Total # of cyber events or cyber incidents recorded in Third-Party's cyber incident management solution (for the period in scope) | All cyber related incidents pertaining to ARS engagement(s), ARS information, data or systems | 100% |

**3. Vulnerability Management**

Frequency – Monthly

| Metric Title | Metric Explanation | Calculation Method | Scope | Target |
|---|---|---|---|---|
| Vulnerability visibility | Measurement of vulnerability scan coverage based on percentage of successful authenticated/agent scans | Total # of successful authenticated/agent scans. (Unique assets or IP addresses from scan) / total # of active assets as per Third-Party asset management solution (for the period in scope) | All assets (endpoints, servers, compute devices, storage devices, network devices) in scope for ARS engagement(s) | 90% |
| Vulnerability mitigation timelines | Measurement of critical vulnerabilities actioned by the target remediation timelines (typically 30 days) for a specific reporting month | (# of actioned (fixed, remediated, fixed by decom) critical vulnerabilities or risk accepted within remediation timeline reported minus any unverified vulnerability) / (Total critical vulnerabilities with a target remediation date in the current month minus any unverified vulnerability) | All assets (endpoints, servers, compute devices, storage devices, network devices) in scope for ARS engagement(s) | 90% |

**4.Identity & Access Management**

Frequency – Monthly

| Metric Title | Metric Explanation | Calculation Method | Scope | Target |
|---|---|---|---|---|
| Access provisioning | Visibility to the ARS SSO accounts provisioned for the period in scope | Total # of ARS SSO creation email or request / Total # of Third-Party resources onboarded during the period in scope | All Third-Party resources having a ARS SSO | 100% |
| Access de-provisioning | Visibility to the ARS SSO accounts de-provisioned for the period in scope | Total # of ARS SSO revocation email or request / Total # of Third-Party resources offboarded during the period in scope | All Third-Party resources having a ARS SSO | 100% |
| Remote access | Visibility to the ARS VPN accounts provisioned for the period in scope | Informational - Total # of Third-Party resources having ARS VPN account AND Total # of Third-Party resources having ARS SSO | All Third-Party resources having a ARS VPN account | N.A. |

**5. Software Security**

Frequency – Monthly

| Metric Title | Metric Explanation | Calculation Method | Scope | Target |
|---|---|---|---|---|
| Critical & high-risk vulnerability mitigation | Measurement of aged critical and high vulnerabilities remediated within timelines (30 days) | Total # of critical and high vulnerabilities remediated / Total # of critical and high discovered during the month | All applications developed by Third Party for ARS | 100% |

| | | | | |
|---|---|---|---|---|
| Application risk classification | Visibility into the count of applications/development projects without risk classification | Informational – Total # of applications/development projects without application risk classification AND Total # of applications/development projects initiated during the month | All applications developed by Third Party for ARS | N.A. |

**6. Data Protection & Endpoint Protection**

Frequency – Monthly

| Metric Title | Metric Explanation | Calculation Method | Scope | Target |
|---|---|---|---|---|
| Antivirus (AV) solution deployment | Validate installation & operation of antivirus solution on all endpoints & servers | Total # of servers and endpoints (laptops & desktops) reflecting in AV console / Total # of servers and endpoints (laptops & desktops) as per Third-Party asset management solution Data as it reflects in console of AV solution for the period in scope | All endpoints (laptops and desktops), servers and compute devices in scope for ARS engagement(s) | 97% |
| Antivirus (AV) signature definitions | Validate installation & operating effectiveness of antivirus signatures on all endpoints & servers | Total # of servers and endpoints (laptops & desktops) reflecting in AV console with virus definitions less than or equal to N-1 (N=current day) / Total # of servers and endpoints (laptops & desktops) as per Third-Party asset management solution Data as it reflects in console of AV solution for the period in scope | All endpoints (laptops and desktops), servers and compute devices in scope for ARS engagement(s) | 97% |
| Data Loss Prevention (DLP) solution deployment | Validate installation & operation of DLP solution on all endpoints | Total # of endpoints (laptops & desktops) reflecting in DLP console / Total # of endpoints (laptops & desktops) as per Third-Party asset management solution Data as it reflects in console of DLP solution for the period in scope | All endpoints (laptops and desktops) in scope for ARS engagement(s) | 97% |
| Encryption solution deployment | Validate installation & operation of data encryption solution on all endpoints & servers | Total # of servers and endpoints (laptops & desktops) reflecting in encryption tool console with drive or volume encryption equal to 100% / Total # of servers and endpoints (laptops & desktops) as per Third-Party asset management solution Data as it reflects in console of encryption solution for the period in scope | All endpoints (laptops and desktops), servers and compute devices in scope for ARS engagement(s) | 97% |

| | | | | |
|---|---|---|---|---|
| Endpoint detection and Response (EDR) solution deployment | Validate installation & operation of EDR solution on all endpoints | Total # of endpoints (laptops & desktops) reflecting in EDR console / Total # of endpoints (laptops & desktops) as per Third-Party asset management solution<br>Data as it reflects in console of EDR solution for the period in scope | All endpoints (laptops and desktops) in scope for ARS engagement(s) | 97% |
| Host based Intrusion Prevention System (HIPS) solution deployment | Validate installation & operation of HIPS solution on all endpoints | Total # of endpoints (laptops & desktops) reflecting in HIPS solution console / Total # of endpoints (laptops & desktops) as per Third-Party asset management solution<br>Data as it reflects in console of HIPS solution for the period in scope | All endpoints (laptops and desktops) in scope for ARS engagement(s) | 97% |
| Remote URL Filtering solution deployment | Validate installation & operation of URL filtering solution/ agent on all laptops | Total # of endpoints (laptops only) reflecting in remote URL filtering solution console / Total # of endpoints (laptops only) as per Third-Party asset management solution<br>Data as it reflects in console of remote URL solution for the period in scope | All endpoint laptops in scope for ARS engagement(s) | 97% |
| Data Loss - USB/Storage media block solution deployment | Validate installation & operation of security solutions deployed on all endpoints to prevent USB/Storage media access | Total # of endpoints (laptops & desktops) reflecting in the console of the solution (e.g.: DLP, EDR, Active Directory group policies etc.) used to block USB/Storage media access / Total # of endpoints (laptops & desktops) as per Third-Party asset management solution<br>Data as it reflects in console of solution used for blocking USB/Storage media access for the period in scope | All endpoints (laptops and desktops) in scope for ARS engagement(s) | 97% |

**7. Quarterly submission of Security Control Logs**

ARS requires that the following logs from the security control tools be submitted to the 3PS team on a quarterly basis. The logs should be specific to the ARS environment or assets that support ARS

a. Data Loss Prevention (DLP) Log (Log from implemented DLP solution)
b. Anti-virus (AV) logs
c. Endpoint Detection & Response (EDR) logs

**DEFINITIONS**

*ARS Confidential* Information is information created, collected, or modified by ARS that would pose a risk of causing harm to ARS if disclosed or used improperly, and is provided and identified as such to the Supplier under the Contract Document. ARS Confidential Information includes Highly Confidential, Personal, Controlled, or Sensitive Personal Data.

*ARS Data* includes Highly Confidential, Confidential, Personal, Controlled, or Sensitive Personal Data.

*ARS Highly Confidential Information* is ARS Confidential Information that ARS identifies as "highly confidential" in the Contract Document, or that ARS identifies as "Restricted," "Highly Confidential," or similar at the time of disclosure.

*Third-Party or Supplier* is the entity that is providing goods or services to ARS pursuant to the Contract Document. It also refers to ARS joint ventures.

*Third-Party Information System(s)* means any Third-Party system(s) and/or computer(s) used to Process, Store, Transmit and/or Access ARS Confidential Information pursuant to the Contract Document, which includes laptops and network devices.

*Third-Party Workers/Resources/Employees* means all persons or entities providing services and/or deliverables under the Contract Document, including Third-Party/Supplier's employees, permitted affiliates, suppliers, contractors, subcontractors and agents, as well as anyone directly or indirectly employed or retained by any of them.