CYSIV
A FORESCOUT COMPANY

Data Source Questionnaire

Instructions

Please **complete, save and return** this questionnaire to your Cysiv contact. Your responses help ensure:

1. Cysiv can provide a more accurate scoping of 24/7 SOC-as-a-Service costs
2. Cysiv onboards the right data sources, as efficiently as possible, and optimizes the ingestion and storage of this data
3. Cysiv creates threat detection use cases that fully align with your priorities and requirements.

If any questions do not apply to your organization, please put “NA” (not applicable).

Organization Name:

Part 1: Approximately how many

1. **Knowledge workers** do you have? Include all employees and contractors that have a company-issued laptop or desktop computer.

2. **Servers** are to be monitored? Include cloud workloads, virtual and on-premise servers.

3. **Events per second (EPS) or GB/day** of logs do you generate?

4. **Internet-facing applications** do you run?

5. **Containers** do you run?

6. **Network segments** do you have?

7. **Active directory forests** do you have?

8. **Domain controllers** do you have?

9. What **% of your servers** are Windows, Linux and serverless, Other?

10. What **% of your endpoint devices** are Windows, Mac, Linux or Mobile (Apple/Android)?

Part 2: What are the key vendors/products you use for

1. **Cloud services** (e.g., AWS, Azure, GCP, etc.)?

2. **SaaS applications (**e.g., Salesforce, Adobe, Microsoft, Slack, etc.)?

3. **SIEM** (e.g., Splunk, Exabeam, IBM QRadar, etc.)?

4. **Containers** (e.g., Docker, AWS Lambda, etc.)?

5. **Security** for endpoint protection, EDR, firewall, IPS, network proxy, email security, authentication, and CASB?

6. **Endpoint security** on your VMs or cloud compute instances?

7. **Identity and access management** (IAM) for your DevOps, and for your CloudOps teams?

8. **Security case management** (e.g., ServiceNow, RSA Archer, ManageEngine, Jira, etc.)?

9. **WAF** (e.g., Fortinet, Imperva, Barracuda, etc.)?

Part 3: Other

1. Regarding your **cloud applications**, please describe the nature, function, complexity or data volumes associated with them (e.g., music streaming service; data-intensive SaaS apps for F500 customers; internal apps migrated to cloud, etc.).

2. If you have a SIEM, do your network, endpoints, email or cloud assets **forward logs to it**?

3. Describe your **Bring Your Own Device (BYOD)** policy?

4. What are your **major IT environments** for running server and business workloads (e.g., Vmware, AWS, Azure, Google Cloud, mainframe, IoT, IoMT, etc.)?

5. Are any of your **security tools** covering a highly, internet-facing environment (e.g., web application firewall, firewall, etc.)?