Questions answered: 360

Anzahl Tables: 93

**1. Demographics**

|  |  |  |
| --- | --- | --- |
| **1.1 Basic Data** | | |
|  | **Question** | **Answer** |
| **1.1.1** | Firm Name | CECONOMY AG |
| **1.1.2** | Address | Kaistr. 3, 40221 Düsseldorf, Germany |
| **1.1.3** | Country | Germany |
| **1.1.4** | Primary Website(s) | https://www.ceconomy.de/ |

|  |  |  |
| --- | --- | --- |
| **1.2 Contact Information** | | |
|  | **Question** | **Answer** |
| **1.2.1** | Primary Contact Name | Günther Groo |
| **1.2.2** | Primary Contact Title | Head of Group Insurance |
| **1.2.3** | Primary Contact Role | Head of Group Insurance |
| **1.2.4** | Primary Contact Email | groo@mediamarktsaturn.com |
| **1.2.5** | Primary Contact Phone | +49 (841) 634 1067 |
|  | Comment | ??tbv |

|  |  |  |
| --- | --- | --- |
| **1.3 ID Numbers** | | |
|  | **Question** | **Answer** |
| **1.3.1** | Ticker Symbol | - |
| **1.3.2** | DUNS Number | 341291102 |

|  |  |  |
| --- | --- | --- |
| **1.4 Basic Demographics** | | |
|  | **Question** | **Answer** |
| **1.4.1** | Currency for monetary responses. The selection applies throughout the Cyber Self-Assessment unless otherwise noted. | Euro - EUR |
| **1.4.2** | Revenue - Most Recent FY | 21,800,000,000 |
|  | Comment | 2022 |
| **1.4.3** | Employee Count (approx.) | 53,000 |
|  | Comment | 2022 |
| **1.4.4** | Primary Industry (NAICS Code Look up | 4492 Electronics and Appliance Retailers |
| **1.4.5** | Secondary Industry (NAICS Code Look up | 4492 Electronics and Appliance Retailers |
| **1.4.6** | Tertiary Industry (NAICS Code Look up | 4492 Electronics and Appliance Retailers |
| **1.4.7** | Please select geographies and indicate your organization's revenue allocation. | |
|  | Sum Of Revenue | 0 |
|  | Comment | ??tbv |

**2. Governance**

|  |  |  |
| --- | --- | --- |
| **2.1 Security Organization** | | |
|  | **Question** | **Answer** |
| **2.1.1** | Please provide an overview of the organization's information/cybersecurity structure: | IT:MMS technology subsidiary of retail group: captive provider for all group companiesorganized in 100 - 120 product teams, e.g &quot;technology foundation&quot;: server, client, networking, asset management, cloud management etc.Some countries have separate IT units, e.g. for running special applications-&gt; harmonization activities are on the way (Italy is currently somewhat independent, one AD, but separate O365 tenant, is being migrated to the standard stack, O365 in 2Q23)group-wide governance:CFO of country org is responsible for IT, report in this function to the central CTOCentral IT: ca. 1000 FTE, decentralized country IT: ca 10-25 FTEInfoSec:Group CISO reports solid to CTO; group CISO org ca. 35 FTE (plus 15 open positions)each country has a country CISO who reports dotted to the group CISO and solid to local CFODefines group-wide InfoSec policies, release of cyber security level 3 policies by CTOregular meetings with CTO biweekly, SvB bi-monthlya standardized reporting template is used: roadmap topics, threat intelligence , KPIs (Progress Asset Management Initiative, # Cyber Security Events (incidents), Cyber Security Risk Exposure (Risk Vectors &amp; Trends), progress of recruitment of IT specialists, training completion, # vulnerabilites)Responsibities of CISO org:- Cyber defense (scanning, SIEM, EDR, SOC)- Cyber Sec engineering (technical advisory, reviews)- ISMS &amp; risk management (product risk assessments, central cyber risk management and third party risk management)- ISO (coordination of local country ISOs)Risk management process: - case-by-case, based on technical reviews - ad-hoc based on threats (e.g. Ukraine conflict, vulnerabilities) - RM manages exceptions to established compliance (need to be reviewed annually at minimum) - regular risk assessment process \* Quarterly Corporate Risk Management Process \* interview with VP technology - product risk process \* regular \* form-based, filled out by product owner risks are evaluated within the risk management org Internal audit dept audit compliance wrt InfoSec policiesCybersecurity Organizational structure will be provided as part of slide deck. |
| **2.1.2** | Overall Information Technology Budget (most recent FY) |  |
|  | Comment | can be provided on request |
| **2.1.3** | Percentage of your IT budget allocated to information/cybersecurity (approx.). |  |
|  | Comment | can be provided on request |
| **2.1.4** | Overall Information/Cybersecurity Budget (most recent FY) |  |
|  | Comment | can be provided on request |
| **2.1.5** | Our information/cybersecurity organization is: | |
|  | Centralized (e.g. There is a centralized information/cybersecurity function which oversees all business units) | X |
|  | Decentralized (e.g. Business units are individually responsible for information/cybersecurity functions) |  |
|  | Federated/Hybrid (e.g. Business units have day-to-day management control, but there are centralized information/cybersecurity policies and standards) |  |

|  |  |  |
| --- | --- | --- |
| **2.2 Security Officers** | | |
|  | **Question** | **Answer** |
| **2.2.1** | The organization has a Chief Information Security Officer (CISO), Chief Security Officer (CSO) or functional equivalent. (If yes, please provide name in additional commentary) | Yes |
| **2.2.2** | If you answered Yes to statement 3.2.1, please indicate to whom the individual reports. | CTO - Chief Technology Officer |
| **2.2.3** | If you answered Yes to statement 3.2.1, does that individual periodically, but not less than annually, brief the board of directors or an equivalent if a non-public organization? | Yes |
| **2.2.4** | The organization manages cyber/information security risks by: (check all that apply). | |
|  | Performing a cybersecurity risk assessment at least annually to identify risks, analyze risks, assess likelihood, assess impact, prioritize risks, plan response strategies, and monitor, evaluate, and adjust. | X |
|  | Documenting the results of the annual cybersecurity risk assessment/management in a report that includes prioritized risk response actions including accept, transfer, mitigate, or avoid. | X |
|  | Presenting the Cybersecurity Risk Assessment Report to the Board, or equivalent at least annually. | X |
| **2.2.5** | The organization has a Chief Privacy Officer (CPO) or a functional equivalent. (if yes, please provide name in additional commentary) | Yes |
|  | Comment | DP belongs to Compliance, CPO (Dr. Kai Schumacher also leads Compliance) responsible for German entities and group-wide11 persons are responsible for privacy centrally (mostly legal professionals)Country DPOs are responsible for their own country companies. Central DP provides advice and templates but need to be adapted by country DPOs for their countryThere is a monthly meeting among all country DPOs plus Group Privacy team to discuss relevant topics. |

|  |  |  |
| --- | --- | --- |
| **2.3 Security Policies and Standards** | | |
|  | **Question** | **Answer** |
| **2.3.1** | The organization documents and implements enterprise or company-wide policies/programs (select all that apply): | |
|  | Cyber / Information Security Policy. | X |
|  | Acceptable Use Policy (AUP) that defines for all parties the ranges of permitted use of organizationally-provided technologies; contains consequences for noncompliance/violation of the AUP. | X |
|  | Users are disallowed from surfing social media platforms from organizational assets except where this is a defined business need. |  |
|  | Insider Threat Program coordinated capabilities to deter, detect, and mitigate insider threats. |  |
| **2.3.2** | The following cybersecurity standards, frameworks, or best practices are leveraged by the organization: | |
|  | ISO/IEC 27001 'Information Security Management System (ISMS)' | X |
|  | NIST Special Publications aimed at computer/cyber/information security | X |
|  | Center for Internet Security 'Critical Security Controls' | X |
|  | ISACA 'COBIT' |  |
|  | FFIEC 'Cybersecurity Assessment Tools' |  |
|  | NIST Cybersecurity Framework (NIST CSF) | X |
|  | PCI-DSS | X |
|  | HIPAA Security |  |
|  | Information Security Forum (ISF), Standard of Good Practice for Information Security |  |
|  | Others (please describe below): |  |
|  | Comment | ISMS based on ISO Leveraging of best-practices from these standards, but not certified |
| **2.3.3** | The organization has documented enterprise or company-wide Privacy Policies (please note policy titles, the version, and date released) | Yes |
| **2.3.4** | The organization implements a physical security program with risk-based protections (e.g., CCTV, visitor access controls, badge access, and alarms for the perimeter) to secure offices and data center facilities. | Yes |
| **2.3.5** | Our screening and background check requires background verification checks including criminal records, credit history, education and reference checks, and employment history as permitted by law. (please check all that apply). | |
|  | Employees |  |
|  | Contractors/ Consultants |  |
|  | Comment | Not part of a regulated industry that requires background checks. Valid drivers license is usually requested as indicator for potential alcohol or drug abuse |

|  |  |  |
| --- | --- | --- |
| **2.4 Independent Audit / Assessment** | | |
|  | **Question** | **Answer** |
| **2.4.1** | The organization engages with an independent service provider to:   a) conduct an assessment of our information/cybersecurity program and associated controls.   b) prepare and deliver a report that documents the results of the assessment and recommendations for improvement. | Yes |
|  | Comment | 2020 Secunet 2022 Alix Partners |
| **2.4.2** | Our internal Audit department conducts risk-based audits or assessments of the information/cybersecurity program and associated controls on an annual or more frequent basis. | Yes |
|  | Comment | varying scope depending on priorities and business requirements (??tbv) |

**3. Data Protection**

|  |  |  |
| --- | --- | --- |
| **3.1 Records** | | |
|  | **Question** | **Answer** |
| **3.1.1** | Number of records in the custody of the organization by PCI (Payment Card Industry/Information). | 0 |
|  | Comment | PCI / PII fully outsourced to payment processor |
| **3.1.2** | The PCI Information provided above is an estimation? | No |
| **3.1.3** | Number of records in the custody of the organization by PHI (Protected Health Information) / Sensitive Personal Data. | 53000 |
|  | Comment | Work or contract relevant information on health or disabilities of individual employees can be included in HR files. Very low number (equal to employee count). |
| **3.1.4** | The PHI Information provided above is an estimation? | Yes |
| **3.1.5** | Number of records in the custody of the organization by PII (Personally Identifiable Information) / Personal Data. |  |
|  | Comment | 98,7 Million total customer records, of that 45,7 million active customers (numbers from 28.02.2023) + 53.000 employees (rounded from 2022)Additionally bank data is stored especially for subscription services (IBAN, BIC &amp; Name) ca. 1 million entries (??tbv) |
| **3.1.6** | The PII Information provided above is an estimation? | No |
| **3.1.7** | Number of records processed and/or transacted by the organization annually by PCI (Payment Card Industry/Information). | 0 |
|  | Comment | ??tbv |
| **3.1.8** | The PCI Information provided above is an estimation? | No |
| **3.1.9** | Number of records processed and/or transacted by the organization annually by PHI (Protected Health Information) / Sensitive Personal Data. |  |
|  | Comment | Processing only in few individual cases through HR. No transaction to 3rd parties |
| **3.1.10** | The PHI Information provided above is an estimation? | Yes |
| **3.1.11** | Number of records processed and/or transacted by the organization annually by PII (Personally Identifiable Information) / Personal Data. |  |
|  | Comment | 2 billion annual customer interaction as reference (??tbv) |
| **3.1.12** | The PII Information provided above is an estimation? | Yes |

|  |  |  |
| --- | --- | --- |
| **3.2 Information Control** | | |
|  | **Question** | **Answer** |
| **3.2.1** | The organization regularly handles or processes information owned by other organizations, unrelated companies, or external customers (please check all that apply). | |
|  | Personally Identifiable Information (PII) | X |
|  | Protected Health Information (PHI) |  |
|  | Intellectual Property/Trade Secrets/Marked Confidential Information | X |
|  | Sales/Business Projections | X |
|  | Merger & Acquisition/Business Development | X |
|  | Insider Financial Information (e.g., non-public information related to a publically traded company's earnings, forecasts, and acquisition and divestiture plans) |  |
|  | Product Development / Research & Development |  |
|  | Advertising / Marketing / Product Roadmaps | X |
|  | Government Classified Data |  |
|  | Other (please describe below): |  |
|  | Comment | PII : only in rare cases (consumer financing), ID card copies are transmitted (but never stored) to financial institutions |
| **3.2.2** | We encrypt account usernames and authentication credentials during transmission over an IT network (i.e., we do not permit clear text usernames and authentication credentials across networks). | Yes |
|  | Comment | only internally: there is a small number of documented exceptions, these are monitored, roadmap in place to replace these (??tbv systems replaced) |
| **3.2.3** | The organization utilizes mandatory encryption to protect critical information and other sensitive information (e.g., PII, PHI, etc.) as defined by information classification and protection policies. | |
|  | Data at Rest |  |
|  | Data in Transit | X |
|  | Corporate laptops and desktops | X |
|  | Data on Removable media |  |
|  | Mobile Devices (e.g., Mobile phones and tablets) | X |
|  | Backups |  |
|  | Comment | Policy defines requirements depending on data classificationEncryption for removable media is currently being established |

|  |  |  |
| --- | --- | --- |
| **3.3 Media Disposal** | | |
|  | **Question** | **Answer** |
| **3.3.1** | Our organization maintains data disposal/ sanitization policies that define media (e.g., hard drives, CDs, USB storage devices, etc.) sanitization requirements and techniques. | Yes |
| **3.3.2** | We have procedures or contracts with service providers to sanitize items or media with sensitive/confidential information prior to reuse or to disposal. | Yes |
| **3.3.3** | Our procedure or service provider retains an audit trail - chain of custody process and proof of media destruction/disposal (i.e., certificate of disposal or destruction). | Yes |

**4. Inventory and Control of Enterprise Assets**

|  |  |  |
| --- | --- | --- |
| **4.1 Inventory all hardware devices** | | |
|  | **Question** | **Answer** |
| **4.1.1** | The following percentage of hardware connected to the organization's network is inventoried: | 75-100% |
|  | Comment | ca. 165k total devicesca. 46k clients (win/mac, workstation)ca. 10k mobile devicesca. 20k printersca. 35k network devicesca. 13k serversca. 11k cash registersca. 30k other devices not in above categoriesOf the above 97% are inventorized |
| **4.1.2** | The organization’s hardware asset inventory is updated: | Other |
|  | Comment | continuously via scanners |

|  |  |  |
| --- | --- | --- |
| **4.2 Track all hardware devices** | | |
|  | **Question** | **Answer** |
| **4.2.1** | The organization's hardware inventory is documented: | Auto |
| **4.2.2** | An automated asset inventory and discovery tool provides visibility to the following percentage of hardware across the enterprise? | 75-100% |
|  | Comment | 100% via network scanners |
| **4.2.3** | We leverage our automated asset inventory tool's discovery capabilities to help detect unknown or unauthorized devices, and to improve the accuracy of our inventory. | Yes |
| **4.2.4** | Our active discovery tool is configured to execute at least: | Daily |

|  |  |  |
| --- | --- | --- |
| **4.3 End of Life (EOL) Technology** | | |
|  | **Question** | **Answer** |
| **4.3.1** | Our organization relies on operating systems, software, or hardware that is no longer supported or is considered “end-of-life” (EOL) by the manufacturers. (If yes, summarize EOL cases) | No |
|  | Comment | EoL policy is in place, task force installed specifically for handling legacy systemsOngoing process to lifecycle windows 2012 servers &amp; mobile devices before EoLExceptions are archived systems in an isolated environment that are retained for legal requirements but are not active, connected to the network or relied on in any way |
| **4.3.2** | End-of-life technologies in use by the organization: (select all that apply) | |
|  | Are segregated from the rest of the network |  |
|  | Have additionally purchased extended support for the software, where available. | X |
|  | Other (please add comments describing compensating controls, or summarize milestone dates or target dates to upgrade to a supported platform) | X |
|  | Comment | increased monitoring, end point protection |

**5. Inventory and Control of Software Assets**

|  |  |  |
| --- | --- | --- |
| **5.1 Inventory all Software** | | |
|  | **Question** | **Answer** |
| **5.1.1** | We maintain an inventory of software in use across the organization. | Yes |
| **5.1.2** | If yes to statement 5.1.1, the inventory captures what percentage of software, including version, that is in use throughout the enterprise. | 50-74% |
|  | Comment | Ongoing project to improve software asset inventory |
| **5.1.3** | Our inventory of software installed on enterprise assets is updated at least: | Other |
|  | Comment | updated continuously, reviewed annually |

|  |  |  |
| --- | --- | --- |
| **5.2 Software and Hardware Inventory Tools** | | |
|  | **Question** | **Answer** |
| **5.2.1** | The organization's software inventory is documented: | No |
|  | Comment | cherwell, leanIX is being introduced for core business apps, ??tbv |
| **5.2.2** | An automated software inventory tool provides visibility to the following percentage of information systems across the enterprise: | 50-74% |
| **5.2.3** | Our inventory of software is: | |
|  | All supported. |  |
|  | All supported, other than those with documented exception with mitigating controls. |  |
|  | Updated with a process repeated at least monthly. |  |
|  | Comment | See patch management process ??tbv |

|  |  |  |
| --- | --- | --- |
| **5.3 File Integrity Tools (Allowlisting)** | | |
|  | **Question** | **Answer** |
| **5.3.1** | In concert with the software inventory, our file integrity checking tools validate software has not been modified prior to execution on a system. | Yes |
|  | Comment | MS Application guard checks secure score of applications Users can override, but this pops up at the SOC |
| **5.3.2** | Our application allowlisting technology is configured to allow critical systems to run software only if it is included on our allowlist. (Describe the allowlisting solution and indicate the name of the solution provider below). | No |
|  | Comment | on Domain Controllers and systems with access to these, there is white listing enabled |

**6. Secure Configuration of Enterprise Assets and Software**

|  |  |  |
| --- | --- | --- |
| **6.1 Standard Secure Baseline Configurations** | | |
|  | **Question** | **Answer** |
| **6.1.1** | We implement standard secure configuration images for operating systems and software applications. | Yes |
| **6.1.2** | Our standard secure configurations for operating systems and software applications incorporate industry recognized security hardening techniques (e.g., Center for Internet Security (CIS) Security Configuration Benchmarks or NIST security configuration checklists, etc.). | Yes |
|  | Comment | For selected CIS controls. |
| **6.1.3** | We implement secure configurations (incorporating industry recognized security hardening techniques) for the following percentage of our operating systems and software applications: | 50-74% |
|  | Comment | partially, standard vendor images (e.g. Google) need to be employed at the moment.There is a project in place to bring this metric up to 80% (by 2Q23) ??tbv |

|  |  |  |
| --- | --- | --- |
| **6.2 System Configuration Management Tools** | | |
|  | **Question** | **Answer** |
| **6.2.1** | Our system configuration management tools (e.g., Active Directory Group Policy, etc.) enforce and redeploy configuration settings to systems. | Yes |

|  |  |  |
| --- | --- | --- |
| **6.3 Information System Change Tools** | | |
|  | **Question** | **Answer** |
| **6.3.1** | In our organization, the development, testing, and production IT environments are separated. | Yes |
|  | Comment | Separate projects, separate interconnects |
| **6.3.2** | Our formal system/application change control policy requires risk assessment, security testing, authorization, and establishment of roll-back procedures prior to deployment into our production environment. | No |
|  | Comment | Each product team is authorized to employ their own change management processes. A central policy is planned for major releases in May 2023Goal is to standardize this across the group |

|  |  |  |
| --- | --- | --- |
| **6.4 Screen Lockout / Inactivity Logout** | | |
|  | **Question** | **Answer** |
| **6.4.1** | Our system configuration automatically engages screensaver lockout after a set period of inactivity to limit access to unattended computers. | Yes |
|  | Comment | after 15 minutes of inactivity but employees are instructed to lock workstation upon leaving it |
| **6.4.2** | In our organization, user accounts are automatically logged off after a standard period of inactivity. | No |

|  |  |  |
| --- | --- | --- |
| **6.5 Unsuccessful Logon Attempts / Automatic Account Lock** | | |
|  | **Question** | **Answer** |
| **6.5.1** | In our organization, accounts are locked out after a set number of failed login attempts and accounts either automatically unlock after a standard period of time or end-users contact the helpdesk to unlock accounts. | Yes |
|  | Comment | external access: 5 attempts: 5 minutes lockedinternal: 10 attempts 5 minutesadmin users are locked permanentlyPassword reset:user contacts service desk -&gt; authenticates via security questions -&gt; new initial password is generated via randomized tool, then eithera) manager gets issued new initial passwordb) user ets issued new initial password via phone-&gt; user logs in and needs to change password (enforced technically)SSPR is planned (Azure AD) for 2023 |

**7. Audit Log Management**

|  |  |  |
| --- | --- | --- |
| **7.1 Audit Logs and Records** | | |
|  | **Question** | **Answer** |
| **7.1.1** | We implement standard audit logging policies for hardware devices and software. | Yes |
| **7.1.2** | Our audit logging policies require a timestamp, source addresses, destination addresses, and other useful data elements. | Yes |
| **7.1.3** | Whenever possible, our system logs are kept in a standardized format, such as syslog entries or the Common Event Expression. | Yes |
| **7.1.4** | We utilize at least two synchronized time sources to provide uniform timestamps. | Yes |
| **7.1.5** | We maintain audit logs for a period of no less than (select from list): | 30 days |
|  | Comment | For most systems 180+ days |
| **7.1.6** | The organization enforces detailed audit logging of access or changes to sensitive data. | No |

|  |  |  |
| --- | --- | --- |
| **7.2 Audit Storage Capacity** | | |
|  | **Question** | **Answer** |
| **7.2.1** | We configure our network boundary devices including: firewalls, network-based Intrusion Prevention System (IPS), and inbound and outbound proxies to "verbosely log" traffic both allowed and blocked. | Yes |
|  | Comment | Combination out of EDR (MDE) and Firewalls logging all connections (attempts & successful) |
| **7.2.2** | Select all of the Audit Policies enabled on Domain Controllers: | |
|  | Audit Credential Validation (Failure) | X |
|  | Audit Process Creation (Success) | X |
|  | Audit Security Group Management (Success and Failure) | X |
|  | Audit User Account Management (Success and Failure) | X |
|  | Audit Other Account Management Events (Success and Failure) | X |
|  | Audit Sensitive Privilege Use (Success and Failure) | X |
|  | Audit Logon (Success and Failure) | X |
|  | Audit Special Logon (Success) | X |
|  | None of the above |  |
|  | Not applicable (not using Active Directory) |  |

|  |  |  |
| --- | --- | --- |
| **7.3 Audit Anomaly Reviews** | | |
|  | **Question** | **Answer** |
| **7.3.1** | Our organization analyzes audit logs/reports/alerts on a regular basis to identify anomalies or unusual activities. | SIEM |
| **7.3.2** | Our security personnel and/or system administrators actively review anomalies to identify unauthorized activities and resolve incidents via our incident response and management processes. | Yes |

**8. Network Monitoring and Defense**

|  |  |  |
| --- | --- | --- |
| **8.1 Security Operations Center / SIEUM** | | |
|  | **Question** | **Answer** |
| **8.1.1** | The organization operates its own Security Operations Center (SOC) and/or has an outsourced Managed Security Service Provider (MSSP) with the following capabilities at a minimum:  a) Established incident alert thresholds  b) Security Incident and Event Management (SIEM) monitoring and alerting for unauthorized access connections, devices, and software. | Own |
|  | Comment | hybrid, night-time or weekend operations are outsourced |
| **8.1.2** | The SOC/MSSP capabilities include, but are not limited to, the following:   a) 24x7 operations  b) mix of signature and heuristic-based detection   c) incident response, containment, and remediation capabilities   d) active threat intelligence and analytics delivering rapid alerts/notification and/or countermeasures  e) processes are continuously improved. | Yes |
| **8.1.3** | We implement a SIEM (Security Information and Event Management) or log analytic tool for unified aggregation, consolidation, correlation, analysis, and alerting. | Yes |
| **8.1.4** | We continuously refine and tune our SIEM (e.g., profiling common system events to tune detection towards unusual activity) to minimize false positives and insignificant alerts. | Yes |
|  | Comment | Use case development continuously done in alignment to MITRE Att&ck framework and incident/risk review |
| **8.1.5** | Our Security Operations Center / Managed Security Service Provider (SOC/MSSP) obtains relevant indicators of compromise (IOCs) combined with leveraging threat intelligence feeds to rapidly discover and respond to threats. (e.g., correlate IOC and identify and alert on threat actors targeting the organization). | Yes |
|  | Comment | MDE alerts are monitored 24/7 by MSSP, ability to isolate threats, combined with on-call duty for internal SOC |

|  |  |  |
| --- | --- | --- |
| **8.2 Intrusion Detection and Prevention Systems** | | |
|  | **Question** | **Answer** |
| **8.2.1** | Our organization deploys intrusion detection and prevention security devices at network egress points to detect and prevent attacks through the use of signatures, network behavior analysis, and other mechanisms. | Yes |
|  | Comment | dedicated IDS: Cisco Stealthwatch Prem & Cloud |
| **8.2.2** | Our intrusion prevention systems (IPS) are deployed in an active block mode - to block known bad signatures, malicious activities/ code, and sophisticated attack behaviors. | Yes |
| **8.2.3** | Our organization routes all outbound web requests through a web proxy which monitors for and blocks potentially malicious content. | Yes |
|  | Comment | Web-proxy: cisco with SSL meta data analysis, no traffic splittingreverse proxies: F5 WAFs (until end of 2023), cloudflare (for all cloud-hosted services, incl. DDoS protection) |

**9. Account Management**

|  |  |  |
| --- | --- | --- |
| **9.1 Identity and Access Management** | | |
|  | **Question** | **Answer** |
| **9.1.1** | Please describe the organization’s remote access protocols (e.g., Remote Desktop Protocol RDP, VPN, Telnet, etc.) to the corporate network and how the organization secures remote access for each protocol. | VPN, Azure virtual windows desktops; internally: RDP disabled on clients |
| **9.1.2** | The organization uses the following tools for directory services, identity providers (IdP), federation and/or rights management: (select all that apply). | |
|  | Microsoft Active Directory (Active Directory) | X |
|  | Azure Active Directory (Azure AD) | X |
|  | Okta |  |
|  | Ping |  |
|  | Active Directory Federation Services |  |
|  | Google Workspaces |  |
|  | Other (please describe in commentary) |  |
|  | None |  |
| **9.1.3** | The organization’s authoritative source of identity for the majority of users is: | Active Directory and Azure AD (Active Directory is authoritative) |
| **9.1.4** | The organization implements the following controls to protect Privileged Service Accounts: (please select all that apply) | |
|  | There is an inventory of all Privileged Service Accounts, and it is updated at least quarterly. | X |
|  | Privileged Service Accounts have password lengths of at least 25 characters. |  |
|  | Privileged Service Accounts have their passwords rotated at least annually. | X |
|  | Privileged Service Accounts have their passwords rotated at least quarterly. |  |
|  | (New) Privileged Service Accounts are configured using the principle of least privilege. | X |
|  | (New) Privileged Service Accounts are configured to deny interactive logins. | X |
|  | (New) Specific monitoring rules are in place for Privileged Service Accounts to alert your Security Operations Center (SOC) of any abnormal behavior. | X |
|  | Service Accounts are tiered such that different accounts are used to interact with workstations, servers, and authentication servers, even for the same service. |  |
|  | Processes drive a review of the requirements of each service associated with a "Privileged" "Service Account" at least annually to verify the service still requires the permissions the service account has (and de-privilege if not). |  |
|  | Not Applicable: there are no Privileged Service Accounts. |  |
|  | Comment | There is a tier 0 for services, tier 1/2 separation for services is not complete yet.Tier 0 accounts are evaluated in their permissions annually, for other tiers there are plans for an implementation |
| **9.1.5** | Indicate the number of active accounts the organization has for Domain Administrator Accounts. Accounts should not include inactive accounts, but should include all nested accounts aggregated across all domains/forests. |  |
|  | Comment | MMSRG.net : 10-15, exact data can be provided upon request or discussed during risk dialogue Inside.Media-Saturn.net: Data can be provided upon request or discussed during risk dialogue (tbv??)Redcoon.Local: 5 Domain Admin Accounts |
| **9.1.6** | Indicate the number of active accounts the organization has for Privileged Services Accounts. Accounts should not include inactive accounts, but should include all nested accounts aggregated across all domains/forests. |  |
|  | Comment | MMSRG.net : Data can be provided upon request or discussed during risk dialogueInside.Media-Saturn.net: Data can be provided upon request or discussed during risk dialogueRedcoon.Local: 15 Service Accounts Previously filled value: see comment??tbv tier 0 priviliged |
| **9.1.7** | Indicate the number of users who have persistent administrative access to servers and/or workstations other than their own. |  |
|  | Comment | MMSRG.net : Data can be provided upon request or discussed during risk dialogueInside.Media-Saturn.net: 0Redcoon.Local: 8 Persistent Accounts |

|  |  |  |
| --- | --- | --- |
| **9.2 Account Management and Review** | | |
|  | **Question** | **Answer** |
| **9.2.1** | We review user accounts at least annually to confirm all accounts are associated with a valid end-user. | Yes |
|  | Comment | joiner/leaver/mover: integrated IDM via SAP HR -> AD, syncs every 6h |
| **9.2.2** | We review service/system accounts at least annually and disable any account that cannot be associated with a valid business process and owner. | No |
|  | Comment | There is a process in place, but coverage not 100%Roadmap in place to implement control to 100%!! ??tbv |
| **9.2.3** | We review user, administrative, and privileged accounts at least (select from list) to confirm all accounts are associated with a valid user. | Quarterly |
|  | Comment | via integrated identity management. Annual audit (for a sample) |
| **9.2.4** | We monitor user accounts and flag dormant accounts (e.g., accounts with no activity for over 60 calendar days) and consult with the corresponding manager prior to disabling the account. | Yes |
|  | Comment | There is such a monitoring in place, however, it is common for some (store) employees to not log in over extended periods of time |

|  |  |  |
| --- | --- | --- |
| **9.3 Password Policies** | | |
|  | **Question** | **Answer** |
| **9.3.1** | Our organization's technical controls enforce the following password requirements (select all that apply): | |
|  | Minimum number of characters | X |
|  | Complexity (e.g., lowercase, uppercase, numbers, or symbols) requirements | X |
|  | Prohibit reuse | X |
|  | Blocking known weak passwords (e.g., "1q2w3e4r5t" and "Passw0rd!") |  |
|  | Detects known compromised/breached passwords from dark web and other sources, and enforces a password reset |  |
|  | Passwords expiration (change is required) at least annually | X |
|  | Comment | minimum length is 8 tbv?? roadmap evtl?passwords have to be changed every 90 days for office users, for admin users 60 daystbv?? |
| **9.3.2** | If there are technological limitations preventing multi-factor authentication, then we enforce complex long passwords (i.e., longer than 14 characters). | Yes |
|  | Comment | For service accounts tbv?? minimum length |

**10. Access Control Management**

|  |  |  |
| --- | --- | --- |
| **10.1 Identity and Access Management** | | |
|  | **Question** | **Answer** |
| **10.1.1** | The organization implements the following controls to protect user accounts with domain administrative privileges: (please select all that apply) | |
|  | System administrators have a unique, privileged credential for administrative tasks (separate from their user credentials for everyday access, email, etc.). | X |
|  | Domain Administrator Accounts require multifactor authentication. | X |
|  | Domain Administrator Accounts are managed and monitored through just-in-time access, are time bound, and require approvals to provide privileged access. |  |
|  | Domain Administrator Accounts are kept in a password safe that requires the user to "check out" the credential (which is rotated afterwards). |  |
|  | In addition to being kept in a password safe, Domain Administrator Accounts are not exposed to the administrative user when "checked out", and access is recorded through a session manager. |  |
|  | Domain Administrator Accounts can only be used from Privileged Access Workstations (workstations that do not have access to internet or email). | X |
|  | There is a log of all actions by "Domain Administrator Accounts" for at least the last thirty days. | X |
|  | None |  |
|  | Comment | MFA: Microsoft account on premise tier 0 concept with privileged access work stations, authenticate via Azure Tenent to access tier 0 systems .For Azure AD Microsoft multi factor authentication with Code or Push.For Azure AD access is time bound admin access.Logs are kept for 180 days in SIEM |
| **10.1.2** | The organization’s posture with respect to access controls for member servers is best described as:    Note: This question is regarding employees' everyday user accounts; where the Applicant provisions employees with separate credentials for administrative access, those accounts should not be considered for the purposes of this question. | No employees are in the Administrator's group or have local admin access to member servers. |
|  | Comment | Users can request temporary admin access to their workstation via separat admin account needs to be released by the manager. |

|  |  |  |
| --- | --- | --- |
| **10.2 Account Monitoring** | | |
|  | **Question** | **Answer** |
| **10.2.1** | In our organization, user accounts have an expiration date which is monitored and enforced. |  |
|  | Comment | for externals: yes for internals, not applicable, as synced with SAP HR |
| **10.2.2** | In our organization, system accounts have an expiration date which is monitored and enforced. | No |

|  |  |  |
| --- | --- | --- |
| **10.3 Account Revocation** | | |
|  | **Question** | **Answer** |
| **10.3.1** | We follow a process to disable user accounts upon termination of an employee, contractor/consultant, or third party user. | Yes |
| **10.3.2** | We follow a process to disable system accounts upon termination of an employee, contractor/consultant, or third party user. | Yes |

|  |  |  |
| --- | --- | --- |
| **10.4 Privileged Access Management** | | |
|  | **Question** | **Answer** |
| **10.4.1** | We limit the use and distribution of administrator or privileged accounts (select all that apply): | |
|  | Via an account authorization process requiring senior management approval. | X |
|  | Administrative/Privileged credentials are separate from credentials used to perform day-to-day tasks. | X |
|  | Administrators are explicitly disallowed from surfing the internet or accessing personal email from their privileged accounts. | X |
|  | Comment | there is a documented process regarding admin approval, enforced technically |
| **10.4.2** | The organization manages Desktop / Local Administrator privileges via: Please check all that apply and indicate the name of the solution(s) below: | |
|  | Endpoint Privilege Management (EPM) |  |
|  | Local Administrator Password Solution (LAPS) or an equivalent solution that sets a different, random password for the common local administrator account across all domain-attached computers. | X |
|  | Privileged Access or Account Management (PAM) | X |
|  | Other (please describe below): |  |
|  | Comment | PAM for Tier-0: PAWs and OTP are required for access to any Tier-0 admin activity |
| **10.4.3** | The organization implements a Privileged Account Management (PAM) solution that, (select all that apply, and add a comment with the name of your PAM solution) | |
|  | Controls access to administrative/privileged accounts | X |
|  | Monitor, record, audit and analyze administrative/privileged access, sessions, and actions | X |
|  | Automated credential management (i.e., credentials automatically rotate after each use or the use of temporary one-time use passwords) | X |
|  | Comment | OTP is used as secondary factor, primary admin password is persistent (but needs to be rotated every 60 days) |

|  |  |  |
| --- | --- | --- |
| **10.5 Multi-Factor Authentication** | | |
|  | **Question** | **Answer** |
| **10.5.1** | The scope of our PAM implementation includes, (check all that apply): | |
|  | Application Accounts |  |
|  | Break glass (emergency or firecall) accounts | X |
|  | Domain administrative accounts | X |
|  | Service accounts |  |
|  | Windows local accounts |  |
|  | Windows server local accounts |  |
|  | Comment | not OTP for breakglass accounts, but there passwords are physically distributed in halves, requiring 4-eye principle for log ons |
| **10.5.2** | Our organization uses the following secondary factor methods for MFA: | |
|  | SMS |  |
|  | Biometric authentication |  |
|  | Authenticator application | X |
|  | Secondary email |  |
|  | Endpoint certificate | X |
|  | Physical security keys | X |
|  | Comment | authenticator most commonVPN uses a device certificate &amp; AD credentials some physical keys are in use |
| **10.5.3** | Irrespective of a user's location, we require multi-factor authentication for access to our most critical or sensitive data or systems. | Yes |
| **10.5.4** | We require multi-factor authentication for all remote login access to the corporate network (e.g., Virtual Private Network (VPN), Remote Desktop Protocol (RDP), or other secure remote access, etc.). | Yes |
|  | Comment | incl. O365 and Wifi |
| **10.5.5** | Irrespective of a user's location, we require multi-factor authentication and encrypted channels for all administrative account access. | No |
|  | Comment | Tier-0 yes, see abovethe rest via device certificate |

**11. Network Infrastructure Management**

|  |  |  |
| --- | --- | --- |
| **11.1 Firewall** | | |
|  | **Question** | **Answer** |
| **11.1.1** | The organization configures firewalls to prevent unauthorized access, and the firewall configurations are reviewed at least annually. | Yes |
|  | Comment | Cisco Firepower perimeter (central DC) stores: Palo Alto |
| **11.1.2** | Our formal firewall policy is to deny-all by default, permit-by-exception to ensure only explicitly approved incoming/outgoing traffic is permitted. | Yes |

|  |  |  |
| --- | --- | --- |
| **11.2 Wireless Network Security** | | |
|  | **Question** | **Answer** |
| **11.2.1** | We implement wireless security policies and protocols that require strong encryption standards. | Yes |
| **11.2.2** | Our organization maintains a completely separate (logically or physically) wireless network for guests, Bring Your Own Device (BYOD) users, and other untrusted devices. | Yes |
|  | Comment | traffic joined with corporate traffic at uplink only |

|  |  |  |
| --- | --- | --- |
| **11.3 Network Segmentation** | | |
|  | **Question** | **Answer** |
| **11.3.1** | In our organization, the network is segmented based on: (select the answer(s) that best reflects your network segmentation approach): | |
|  | Business unit |  |
|  | Geographic/regional | X |
|  | Classification level of the information stored on the servers |  |
|  | Data processing and storage based on the sensitivity of the data |  |
|  | Isolating critical systems, functions, or resources | X |
|  | Role and functionality |  |
|  | Comment | Countries, DCs,PKI, Tier-0Servers, clients, printers, phonesStores (incl micro segments within stores)Cloud projects are segemented by role and functionality |
| **11.3.2** | To mitigate risks/threats and increase our operational resilience, we implement enhanced security controls/protections (select all that apply): | |
|  | Perform traffic filtering between network segments. | X |
|  | Use network appliances to filter ingress or egress traffic and perform protocol filtering. | X |
|  | Deploy a network intrusion prevention solution to block known malicious traffic at network boundaries. | X |
|  | Implement port-level access control utilizing 802.1x or similar Network Access Control (NAC) protocols for authenticating and authorizing device. |  |
|  | Configure software on user workstations, with a default-deny rule to drops all traffic except those services and ports that are explicitly allowed. | X |
|  | Comment | NAC is implemented for Wifi,Port configuration is in place |

**12. Malware Defenses**

|  |  |  |
| --- | --- | --- |
| **12.1 Malware Protection** | | |
|  | **Question** | **Answer** |
| **12.1.1** | The organization implements the following malware protections: | |
|  | Incoming emails are filtered/scanned for known malicious attachments and suspicious file types, including executable | X |
|  | Macro-enabled files cannot be run by default. | X |
|  | A quarantine service is provided. | X |
|  | Email attachments are evaluated in a sandbox to determine if malicious prior to delivery. | X |
|  | Emails are filtered to block suspicious messages based on their content or attributes of the sender. | X |
|  | Comment | User cannot enable macros  Cisco Email security appliance (cloud service) |
| **12.1.2** | The organization installs and regularly updates anti-malware solutions (e.g., anti-virus, anti-spyware, advanced endpoint security) to the following percentage of assets, and exceptions are documented. |  |
|  | Comment | Mobile devices covered by MDM (Intune). A dedicated malware solution for mobile devices is currently in evaluation. ??tbv |
| **12.1.3** | Specify the endpoint security tool(s) used. If multiple, please add in commentary area. |  |
|  | Comment | Defender for Office is planned currently in negotiation |
| **12.1.4** | The endpoint security tool(s) are configured to:(select all that apply) | |
|  | For those tools which require updated definitions, such tools are updating at least daily. | X |
|  | Block (as opposed to solely notify of) suspected malicious processes and files. | X |
|  | Find unmanaged assets, which are addressed at least weekly. |  |
|  | Enable anti-tamper features. | X |
|  | Comment | MDE discovery is scanning unmanaged assets on the network |

**13. Continuous Vulnerability Management**

|  |  |  |
| --- | --- | --- |
| **13.1 Vulnerability and Patch Management** | | |
|  | **Question** | **Answer** |
| **13.1.1** | Vulnerability scans are performed at least (select from dropdown list) | Monthly |
|  | Comment | Internet-facing: weeklyInternal infrastructure scans: monthlyTenable over all internal and external serverExternal domains are monitored by Nimbusec quarterlyplus cloud-specific solutions |
| **13.1.2** | Our organization deploys automated patch management processes/tools to update operating systems, software/applications, and other application software or firmware. | No |
|  | Comment | Automated process for windows/mac clients and 80% of windows servers (remainder cannot be rebooted at any time for automated patching, restart and patching of these has to be coordinated)Not automated are linux servers but is currently being automated (Rollout at 50% using ansible)patch process (partially manual):Clients: MS software: via SCCM / InTune Patch tuesday -&gt; Patches are rolled out to all clients within 2 weeks. Postponing not possible, reboot is forced at EOB. Mac and other (e.g. mobile devices): managed by individual product team, processes and timelines varyServers: see above for MS and non-MS. Test Process for each application. Security patches are rolled out over 5 days.- Central Ansible Job: forced once a month. Process done for GCP and in the Global data centerFor MS: Ansible uses a WSUS server which provides the cleared patches, transfers them to the servers and installs them.Ansible uses a JFrog Artifact Repository which provides the cleared packages for Ubuntu (20.04) and SLES 12/15, transfers them from a repo-server to the managed client and starts the installation.- Store server are patched once a month via WSUS according to a predefined schedule.- Capgemini Server landscape: patched by CG, MSH informed by CG about rollout of patches. Windows server patched once a month, Linux patched once in a quarter.- PlusServer: Windows patched via WSUS once a month; Linux patched based on need. (Contract ends on 30th of September 2023) |
| **13.1.3** | Our organization deploys vulnerability patches: | Monthly |
|  | Comment | Vulnerability Patches are patched according to their risk evaluation, patching procedure above applies for the both vulnerability and functional patches |
| **13.1.4** | The organization's target timeframe to patch Common Vulnerability Scoring System (CVSS) v3 Critical Severity 9.0-10.0 vulnerabilities across your enterprise is: | Within 7 calendar days of release |
|  | Comment | Policy states for CVSS scores 8-10: 1 week empirically, this is done faster |
| **13.1.5** | In the most recent full quarter, the organization was successful at achieving the target timeframe selected above in statement 13.1.4 to patch (select from list) CVSS Critical Severity vulnerabilities across the enterprise. | Not tracked/Don’t know |
|  | Comment | A task force has been set up to define the necessary KPIs and collect the respective informationData can be provided upon request |
| **13.1.6** | The organization's target timeframe to patch Common Vulnerability Scoring System (CVSS) v3 High Severity 7.0-8.9 vulnerabilities across your enterprise is: | Within 15 calendar days of release |

|  |  |  |
| --- | --- | --- |
| **13.2 Penetration Testing** | | |
|  | **Question** | **Answer** |
| **13.2.1** | In our organization, annual or more frequent penetration testing (i.e., testing that emulates adversary actions and hostile cyber attacks) is conducted on the network and critical systems. | Yes |
|  | Comment | regular audit of productive systems before rollout of significant software |
| **13.2.2** | Our processes require penetration testing activities that include, but are not limited to, the following:  a) annual assessment(s) b) independent penetration agents simulate adversary actions c) testing scope includes the network and business critical systems/ applications d) penetration test results and recommendations are risk-rated and/or prioritized to mitigate or remediate vulnerabilities and weaknesses identified. | Yes |
|  | Comment | b) internal and external agents perform penetration testing. Further penetration testing: Post Go-Live by Audit, Pre Go-Live by Cyber Security  c) yes, risk and change-based testing of critical applications & network d) vulnerability management & risk management |

**14. Security Awareness and Skills Training**

|  |  |  |
| --- | --- | --- |
| **14.1 Security Training** | | |
|  | **Question** | **Answer** |
| **14.1.1** | In our organization, cybersecurity training is mandatory for all employees (select period from list). | Annually |
|  | Comment | Monthly phishing campaigns including mandatory training for clickers, annual cybersec training for all employees and special trainings for focus groups (admins, devs, finance&amp;HR) |
| **14.1.2** | Cybersecurity training is mandatory for vendors/contractors and third party partners with access to the corporate network (select period from list). | Annually |
|  | Comment | Same process as for 'normal' employees, see above |
| **14.1.3** | We perform an annual analysis to identify gaps in our cybersecurity skillset, and develop and implement training roadmaps and/or project plans to close identified gaps. | Yes |
|  | Comment | Individual development plan for security employees |

|  |  |  |
| --- | --- | --- |
| **14.2 Security Awareness Program** | | |
|  | **Question** | **Answer** |
| **14.2.1** | Our cybersecurity awareness program materials train users to avoid common cyber-risks and threats, such as social engineering and phishing. | Yes |
|  | Comment | KnowBe4 platform is used to train all employees at least annually |
| **14.2.2** | We update cybersecurity awareness training and communications content frequently (at least annually) to embody the latest attack and social engineering techniques. | Yes |
|  | Comment | monthly phishing campaigns, focus groups for CXO fraud (including all executives) |
| **14.2.3** | Our organization tags external emails to alert employees that the email originated from outside the organization. | Yes |
|  | Comment | There is a special warning for specific &quot;VIP senders&quot; (executives) |
| **14.2.4** | The organization conducts internal phishing campaigns at least annually. | Yes |
|  | Comment | monthly |
| **14.2.5** | Our organization has a documented process to report suspicious emails to an internal security team to investigate. | Yes |
|  | Comment | via automated phishing button |

**15. Data Recovery**

|  |  |  |
| --- | --- | --- |
| **15.1 Recovery Processes and Procedures** | | |
|  | **Question** | **Answer** |
| **15.1.1** | Our organization conducts backups for Applications | Daily |
|  | Comment | AVAMAR: daily incrementell foreverBackup retention: Retention as requested by Application Owner, no standard retentionLocation and DR copy: two physical systems in two location per country HQphysical Accesscontrol to Datacenter: only a limited number and named employees have access to the data centerlogical Access control to Backup: only named accounts not connected to AD or LDAP ServiceGDC Ingolstadt: daily (incremental)/weekly (full)/no snapshot backup as requested by ApplicationownerBackup retention: 30 daysLocation and DR copy: the latest three snaps are stored two physical systems (NetApp Metrocluster) one in Wankelstrae and one in Westparkone additional system for storing all backupsphysical Accesscontrol to Datacenter: only a limited number and named employees have access to the data centerlogical Access control to Backup: only named accounts not connected to AD or LDAP ServicePPDM@GCP: daily FS Backup Backup retention: 30 daysLocation and DR copy: two primary DDVE systems in Region Europe West 4 (Amsterdam)one additional DDVE system for replication in Region Europe West 3 (Frankfurt)physical Accesscontrol to Datacenter: employees who have physical access to the components do not have access to the virtual systems running on themlogical Access control to Backup: only named accounts not connected to AD or LDAP ServiceCapgemini: weekly fulldaily incrementalBackup retention: 15/30 daysLocation and DR copy: two physical DataDomain Systens (one in DC FR2 and one in DC FR4) in vise versa replications modephysical Accesscontrol to Datacenter: only a limited number and named employees have access to the data centerlogical Access control to Backup: only named accounts not connected to AD or LDAP ServicePlusserver (contract ends on 30.09.2023): weekly full (on Sunday)Monday to Saturday incrementalBackup retention: 2 weeksLocation and DR copy: 2 datacenter locations in Hamburg (kgham, noham)Backup of systems cross-wise to other DC locationBackup type &quot;disk-2-tape&quot;physical Accesscontrol to Datacenter: only a limited number of named employees have access to DCs.For externals a physical access policy is implemented.logical Access control to Backup: only named accounts |
| **15.1.2** | Our organization conducts backups for Databases | Continuously |
| **15.1.3** | Our organization conducts backups for Servers | Daily |
| **15.1.4** | Our organization conducts backups for Workstations/laptops and endpoints | Other (please describe) |
|  | Comment | no backup, no critical data to be stored on devices |
| **15.1.5** | Our organization conducts backups for Critical Information (Critical Information means critical information as defined by the organization’s information classification or business continuity / disaster recovery plans/policies) | Other (please describe) |
|  | Comment | as above |
| **15.1.6** | We test system restoration capabilities by performing a full restoration from a sample set of backup data at least. | Annually |
|  | Comment | at least annually |
| **15.1.7** | To strengthen recovery from malicious encryption (e.g., crypto-ransomware attack), we isolate backup files from the network (i.e., backup files are not continuously accessible from the network). | |
|  | Isolate backup files from the network (i.e., backup files are not continuously accessible from the network). | X |
|  | Store offline (archive) backups onsite. |  |
|  | Store offline (archive) backups offsite. | X |
|  | Backups are immutable (i.e., cannot be altered or deleted) | X |
|  | Comment | via Dell backup appliance Datacenter / Operators: AVAMAR, GDC Ingolstadt, PPDM@GCP, Capgemini, Plusserver Isolate backup files from the network (i.e., backup files are not continuously accessible from the network).: No, Backup has its own network, but is continuously connected Store offline (archive) backups onsite: Only for Plusserver Backups are immutable (i.e., cannot be altered or deleted): Can not be altered, but with sufficient privileges deleted |
| **15.1.8** | After an incident is contained, the organization implements procedures/processes to remediate affected systems and restore systems to our normal or fully operational state. | Yes |
|  | Comment | DRP in place |

|  |  |  |
| --- | --- | --- |
| **15.2 Business Continuity** | | |
|  | **Question** | **Answer** |
| **15.2.1** | The organization maintains a business continuity/disaster recovery plan, and the plan is tested: | Biennially (once every 2 years) |
|  | Comment | BDP/DR plans are tested at least every two years |
| **15.2.2** | The organization's Recovery Time Objective (RTO), defined as the maximum target period IT functionality may be lost due to an incident, is the following for critical systems: | Less than 5 hours |
|  | Comment | Most critical systems with customer facing business impact (e.g. webshop) can be restored within few minutes through cloud recovery &amp; failover functionalities and have RTOs less than 1 hour.Overall RTO for critical systems is defined within maximum 24hCriticality is proportional to turnover in a given time period |
| **15.2.3** | Our organization reviews and updates IT disaster recovery plans quarterly to address system/organizational changes, lessons learned, or problems encountered during the most recent restoration. | No |
|  | Comment | Is being done annually |
| **15.2.4** | The organization maintains an alternate backup IT facility which would be categorized as: | A hot site |
| **15.2.5** | The organization has the capability to immediately failover to redundant or standby information systems. | Yes |
|  | Comment | Multi-region cloud architecture is being employed |
| **15.2.6** | We review and revise IT disaster recovery plans on an annual basis; revisions incorporate lessons learned from IT disaster recovery plan tests and previous restoration activities. | Yes |

**16. Service Provider Management**

|  |  |  |
| --- | --- | --- |
| **16.1 Outsourced Services** | | |
|  | **Question** | **Answer** |
| **16.1.1** | The organization conducts security assessments and periodic re-assessments on third party partners and other service providers with access to information assets. | Yes |
|  | Comment | But only on initial onboarding or re-onboarding of a vendor; no regular audits for existing \*unchanged\* relationships (tbv??)using standardized questionnaire |
| **16.1.2** | The organization reviews independent audit reports (e.g., SSAE 18 SOC 2, HITRUST certification, or Standardized Information Gathering (SIG), Agreed Upon Procedures (AUP)\*) from third party partners and other service providers with access to information assets at least annually. \* The most recent version of the standards listed. | No |
| **16.1.3** | Our organization requires confirmation from our cloud vendors that they are compliant with any applicable laws related to data storage and data transfer. | Yes |
| **16.1.4** | Our cloud provider utilizes DDoS mitigation solutions. | Yes |
|  | Comment | via Cloudflare &amp; akamai until September 2023 |

|  |  |  |
| --- | --- | --- |
| **16.2 Third Party Risk Management Oversight** | | |
|  | **Question** | **Answer** |
| **16.2.1** | Our organization requires vendors to maintain insurance or another means of indemnification for losses caused by the provider, including from a privacy breach. | No |
| **16.2.2** | The organization requires interconnection agreements for connections between the organization's network and external networks (e.g., third-parties, vendors, etc.). |  |
|  | Comment | N/A |
| **16.2.3** | If interconnection security agreements are required, the organization's agreements contain information/cybersecurity requirements including risk-based monitoring for anomalous activities. |  |
|  | Comment | N/A |
| **16.2.4** | The organization has a process or technical solution to identify, assess, manage, monitor, and reduce the risks from third party partners and other service providers. | No |
|  | Comment | There is an ongoing BCM project that addresses questions on risks due to dependencies from critical 3rd parties (tbv?? third party risk assessment providers) |
| **16.2.5** | We maintain an inventory of what percentage of third party or vendor managed information systems (residing outside of the organization's boundaries and not under the organization's direct control) that have access to or process our information assets (e.g., cloud, SaaS, etc.). | 75-100% |
|  | Comment | All services with a cost above 25k are inventarized during sourcing and are maintained |

**17. Incident Response Management**

|  |  |  |
| --- | --- | --- |
| **17.1 Incident or Breach Response Plan(s)** | | |
|  | **Question** | **Answer** |
| **17.1.1** | Our incident response or breach response plan is (select all that apply): | |
|  | Formally documented. | X |
|  | Aligned with the National Institute of Standards and Technology (NIST) Special Publication 800-61. |  |
|  | Aligned with ISO/IEC 27035 guidance |  |
|  | Aligned with an other governmental authority (e.g. US-CERT or ANSSI) – please describe in comments. |  |
|  | Comment | ??tbv |
| **17.1.2** | Our incident response program requires incident response and reporting instructions within contracts for third party partners or service providers that manage or have access to corporate/organizational data via contract riders or agreed-upon terms and conditions. | Yes |
|  | Comment | ??tbv |
| **17.1.3** | We have internal resources and/or an active contract with incident response service providers to accomplish incident containment, eradication (e.g., eliminate malware and return systems to normal operations), and orchestrate recovery. | Yes |
|  | Comment | InfoGuard |
| **17.1.4** | Our incident response program encompasses the following core capabilities: | |
|  | Processes/procedures for performing incident classification, prioritization, handling, reporting, and recovery. | X |
|  | Ransomware response playbook. | X |
|  | Playbook for a ransomware incident of 3rd parties/MSPs. |  |
|  | A defined response team structure. | X |
|  | Plan testing or exercise requirements. | X |
|  | Plan review and update schedule. | X |
|  | Process to resume business operations by restoration of known clean backups |  |
|  | Process/procedures for recovery, such as activating the IT disaster recovery plan |  |
|  | Names and contact information for relevant authorities, including law enforcement |  |
|  | Comment | Document and corresponding process is currently being reviewed and updated thereafter ??tbvTesting requirement tbd?? |

|  |  |  |
| --- | --- | --- |
| **17.2 Incident Response Exercises** | | |
|  | **Question** | **Answer** |
| **17.2.1** | Our organization conducts incident/breach response scenario-based exercises that: (select all that apply) | |
|  | Include Cyber Incident response tabletop reviews. | X |
|  | Requires participation from cyber incident response and senior management personnel defined in our plan to refresh their responsibilities. | X |
|  | Reflect current threats and risks faced by our industry or similar organizations, including facing threats from ransomware actors. | X |
|  | Results in documentation of lessons learned and revisions/improvements required. | X |

|  |  |  |
| --- | --- | --- |
| **17.3 Incident Containment and Mitigation Activities** | | |
|  | **Question** | **Answer** |
| **17.3.1** | Our security operations center or third party provider monitors the US-CERT, industry-related Information Sharing and Analysis Center (ISAC), and other feeds for alert and threat information; this information is reviewed and actions taken to mitigate risks. | Yes |
|  | Comment | MS Defender for Endpoint includes threat intelligence integration. In addition, exchange through formal and informal groups (e.g. BSI, CERT Bund)Intel471 Periscope weekly report |
| **17.3.2** | Our incident response strategy is integrated with organization/corporate business continuity plans and IT disaster recovery capabilities. | No |
|  | Comment | Respective plans (crisis management, BCPs, IR & DRP) exists, but different units are responsible for this and they were developed independently |
| **17.3.3** | The average time to triage and contain security incidents of workstations for the most recent completed quarter is: |  |
|  | Comment | Depending on type of incident and channel, containment can be done within few minutes or within same day (for low priority incidents)??tbv |
| **17.3.4** | Our incident monitoring/ handling practices require incident documentation | Yes |
| **17.3.5** | We have qualified forensics personnel or an active contract with a forensics service provider to conduct investigations, determine the scope of a breach, and establish what data was compromised. | Yes |
|  | Comment | 4 internals, plus retainer/insurance provider |

|  |  |  |
| --- | --- | --- |
| **17.4 Forensics are performed** | | |
|  | **Question** | **Answer** |
| **17.4.1** | We review and revise incident/breach response plans to address system/organizational changes, lessons learned, or problems encountered during previous incident detection and response activities. | Yes |
| **17.4.2** | We have a documented crisis communication plan that addresses communications activities such as, but not limited to, the following: a) emergency contact information for senior personnel, such as senior executives, corporate communications, the general counsel, and the CIO/CISO, etc.  b) identification and contact information for key audiences, such as customer/ investor relations managers, employee unions, and state and federal regulators, etc. | Yes |
| **17.4.3** | Our crisis communication plan includes, but is not limited to:  a) cyber insurance policy documentation and contact information  b) guidelines and procedures for establishing a corporate spokesperson  c) approval and escalation procedures to clear information or press releases prior to external release  d) breach notification template and consultation process with external legal counsel to review and approve notices prior to release | Yes |

|  |  |  |
| --- | --- | --- |
| **17.5 Incident Response Plan Improvement** | | |
|  | **Question** | **Answer** |
| **17.5.1** | In concert with our incident/ breach response plans, we maintain pre-negotiated contracts with data breach response/ resolution providers (e.g., call centers, notices and communications, and credit monitoring services). | No |
| **17.5.2** | Our organization retains pre-approved reputational risk advisors to develop an action plan to improve public relations, enhance customer trust, and monitor the effectiveness of these plans. | No |

**18. Technology in Use**

|  |  |  |
| --- | --- | --- |
| **18.1 Microsoft 365 Protections** | | |
|  | **Question** | **Answer** |
| **18.1.1** | The organization uses Microsoft 365. | Yes |
| **18.1.2** | The organization uses the following protections with Microsoft 365. | |
|  | Microsoft 365 Advanced Threat Protection. | X |
|  | Multi-Factor Authentication is required at all times. | X |
|  | Other (please describe email security capabilities in commentary). | X |
|  | Not applicable. |  |
|  | Comment | Cisco ESA, is being replaced by MS Defender for Office |

|  |  |  |
| --- | --- | --- |
| **18.2 Cloud Utilization** | | |
|  | **Question** | **Answer** |
| **18.2.1** | The organization utilizes cloud computing in the following way(s): (please check all that apply) | |
|  | Public cloud | X |
|  | Private cloud |  |
|  | Hybrid of public/private cloud | X |
|  | The organization does not utilize cloud computing |  |
| **18.2.2** | Please describe the types of business processes, applications or functions which the organization relies on for cloud computing. | O365 SAP (SuccessFactors & Concur, etc.) Deployment of products in Azure and Google cloud Cloudflare MS Dynamics 365 Mirakl Shopify |

|  |  |  |
| --- | --- | --- |
| **18.3 Information / Cybersecurity Capabilities and Tools** | | |
|  | **Question** | **Answer** |
| **18.3.1** | The organization operates the following Information Technology (IT) and Information/Cybersecurity tools and capabilities (please check all that apply and indicate key vendors): | |
|  | Network Intrusion Detection/Prevention Systems (IDPS) | X |
|  | Unified Threat Management (UTM)/ Threat Prevention/ Protection Systems (TPS) |  |
|  | Network Data Loss Prevention (DLP) solution |  |
|  | Protective Domain Name Service (PDNS) | X |
|  | Security Information and Event Management (SIEM) | X |
|  | Email DLP solution |  |
|  | Enforce Sender Policy Framework (SPF) | X |
|  | DomainKeys Identified Mail (DKIM) | X |
|  | Domain-based Message Authentication, Reporting and Conformance (DMARC) |  |
|  | Block malicious and phishing URLs | X |
|  | Multi-Factor Authentication to on-premise backups |  |
|  | Multi-Factor Authentication to cloud-based backups | X |
|  | Host Intrusion Prevention Systems (HIPS) | X |
|  | File Integrity Tools (Whitelisting) | X |
|  | Endpoint DLP solution |  |
|  | Endpoint Detection and Response (EDR) solutions | X |
|  | Advanced Endpoint Security | X |
|  | Network Detection and Response (NDR) solutions | X |
|  | Identity and Access Management solutions | X |
|  | Bring Your Own Device (BYOD) security solutions |  |
|  | Password management software | X |
|  | Wireless Network Security solutions | X |
|  | Network Intrusion Detection Systems (NIDS) | X |
|  | DDoS mitigation solutions | X |
|  | Please describe other tools or capabilities that support the organization's cyber/information security program |  |
|  | Comment | File Integrity Tools (Whitelisting): Tier 0 only (covered through organizational process. Technical solution to be implemented)NDR: StealthwatchDMARC in implementation ??tbvMFA to onprem ??tbv |

**19. Event History**

|  |  |  |
| --- | --- | --- |
| **19.1 Event History** | | |
|  | **Question** | **Answer** |
| **19.1.1** | Within the past 5 years, has the organization sustained any network security incidents or data incidents that resulted in a material financial loss to the organization? If yes, please describe in detail below. | Yes |
|  | Comment | 08.11.2021 – Ransomware Further information was already provided |
| **19.1.2** | Within the past 5 year, has the organization received any demands or claims relating to allegations of theft of information or breach of information security? If yes, please describe in detail below. | No |
|  | Comment | Not with regard to data privacy claims |
| **19.1.3** | Within the past 5 years has the organization been required to notify any individuals or entities because of a breach of information security? If yes, please describe in detail below. | No |
| **19.1.4** | Within the past 5 years, has the organization been the subject of any government action, regulatory investigation or subpoena regarding any alleged violation of any privacy/data security law or regulation? If yes, please describe in detail below. | No |
| **19.1.5** | Within the past 5 years, has the organization experienced a network outage, or substantial loss of IT functionality for more than 6 hours? If yes, please describe in detail below. | No |
| **19.1.6** | Within the past 5 years has the organization sustained any network security incidents, or outages as the result of the actions of a 3rd party vendor (e.g. cloud vendors, IT consultants, payroll, data processing)? If yes, please describe in detail below. | Yes |
|  | Comment | see 19.1.1 |

**20. Biometric Information**

|  |  |  |
| --- | --- | --- |
| **20.1 Biometric Information** | | |
|  | **Question** | **Answer** |
| **20.1.1** | The organization uses or provides technology that scans biometric identifiers, e.g. fingerprints, fingers, hands, faces, eyes. | No |
|  | Comment | ??tbv |
| **20.1.2** | The organization manages and discloses use of biometric information: (select all that apply) | |
|  | Notice is provided and consent is obtained from individuals who use the technology. |  |
|  | Via a written policy addressing the storage, collection, and retention of the biometric information. |  |
|  | Biometric information is sold, leased, or traded with third parties. |  |
| **20.1.3** | The organization follows data retention and destruction procedures for biometric information: (select all that apply) | |
|  | Stored according to a written retention schedule in line with legal requirements. (If selected, please describe in commentary box if the data retention schedule is readily available to the public) |  |
|  | Biometric information is destroyed according to a written policy as soon as practicable and in line with legal requirements. (If selected, please describe in commentary box if the data destruction policy is readily available to the public) |  |
| **20.1.4** | Equipment or technology provided by a third-party vendor is used to collect, receive, or retain biometric data. (If Yes, please describe in commentary box if the notice and consent obtained from individuals who use the technology include notification that the biometric information is disclosed to the third-party) |  |
| **20.1.5** | The organization follows storage and protection procedures for biometric information: (select all that apply) | |
|  | Stored separately from other types of data. |  |
|  | Different protections are implemented for biometric information compared to other types of sensitive information. (If selected, please describe in commentary box) |  |
|  | Only defined parties are granted access to stored biometric information. |  |
| **20.1.6** | Any complaints have been received alleging the collection, receipt, retention, use, dissemination, or sale of biometric information. |  |

**21. HIPAA**

|  |  |  |
| --- | --- | --- |
| **21.1 HIPAA** | | |
|  | **Question** | **Answer** |
| **21.1.1** | Your organization is considered a Covered Entity under the Health Insurance Portability and Accountability (HIPAA) Act and the Health Information Technology for Economic and Clinical Health (HITECH) Act. | No |
| **21.1.2** | Your organization is considered a Business Associate under the HIPAA/HITECH Acts. |  |
| **21.1.3** | The organization is HIPAA compliant and conducts at least yearly compliance reviews. |  |
| **21.1.4** | All Business Associate agreements are reviewed to ensure they are HIPAA compliant. |  |

**22. PCI**

|  |  |  |
| --- | --- | --- |
| **22.1 PCI** | | |
|  | **Question** | **Answer** |
| **22.1.1** | Your organization is required to be compliant with Payment Card DSS Standards (PCI-DSS). |  |
|  | Comment | ??tbv |
| **22.1.2** | Revenue for credit card transactions that are processed annually through the organization’s system: |  |
| **22.1.3** | Percentage of these transactions completed online or other card not present transactions vs. Point of Sale (POS) transactions: |  |
| **22.1.4** | Percentage of revenue completed by online or other card not present transactions vs. Point of Sale (POS) transactions: |  |
| **22.1.5** | PCI Merchant Level (i.e., 1-4): |  |
| **22.1.6** | The organization is currently compliant with PCI-DSS Validation Requirements as required by your merchant level (i.e. Level 1 - 4). |  |
| **22.1.7** | Version of PCI-DSS against which the organization was assessed: |  |
| **22.1.8** | Percentage of the organization's POS System that is EMV compliant (100%, 75%, 50%, 25%, 0%): |  |
| **22.1.9** | The organization’s POS system was installed with the assistance of a system integrator, reseller or consultant qualified by the PCI Security Standards Council Qualified Integrators and Resellers (QIR) program. |  |
| **22.1.10** | The organization maintains a separate network for their POS system (e.g. through the use of jump servers). |  |
| **22.1.11** | The organization require third party providers, who operate or maintain your POS system, to maintain insurance or another means of indemnification for loss caused by the provider. |  |
| **22.1.12** | The organization utilizes a payment processor that provides regular evidence of PCI-DSS compliance. |  |
| **22.1.13** | Any PCI data that is stored is encrypted while at rest. |  |
| **22.1.14** | Any PCI data that is stored is in tokenized form while at rest. |  |
| **22.1.15** | The organization implements malware protection on their POS terminals. |  |
| **22.1.16** | The organization implements log monitoring around PCI and POS system activity. |  |
| **22.1.17** | Intrusion Detection Systems (IDS) and Data Loss Prevention (DLP) are implemented within the POS network and any other PCI systems. |  |
| **22.1.18** | Penetration testing and vulnerability scans are performed on the POS network and any other PCI systems at least annually. |  |
| **22.1.19** | IDS and DLP are monitored 24 hours a day. |  |
| **22.1.20** | PCI data is either encrypted or tokenized while transit. |  |
| **22.1.21** | The organization utilizes Point to Point Encryption (P2PE) that is PCI-DSS certified. |  |
| **22.1.22** | In addition to having P2PE that is PCI-DSS certified, the organization does not hold the decryption keys for the PCI data, and PCI data may only be decrypted in a third party provider's environment. |  |
| **22.1.23** | The organization utilizes PCI Validated P2PE, approved by the PCI Security Standard Council. |  |
| **22.1.24** | The organization is compliant with the Song Beverly Act and other similar laws/regulations. |  |
| **22.1.25** | The organization is compliant with the credit card display provisions of the Fair and Accurate Credit Transaction Act (FACTA). |  |

**23. Trending Topics**

|  |  |  |
| --- | --- | --- |
| **23.1 SolarWinds** | | |
|  | **Question** | **Answer** |
| **23.1.1** | The organization runs a version of SolarWinds Orion vulnerable to the SUNBURST or SUPERNOVA backdoors. | No |
| **23.1.2** | The organization at any time ran a version of SolarWinds Orion vulnerable to the SUNBURST or SUPERNOVA backdoors. | No |
| **23.1.3** | Please describe the measures undertaken to investigate any potential malicious activity in your organization's system. | N/A |
| **23.1.4** | Any evidence of malicious activity as a result of the SolarWinds vulnerability was found on your organization's system. | Not Applicable |

|  |  |  |
| --- | --- | --- |
| **23.2 Microsoft Exchange / Hafnium** | | |
|  | **Question** | **Answer** |
| **23.2.1** | The organization runs a version of Microsoft Exchange Server 2010 through to 2019 vulnerable to the zero-day exploits being targeted. | No |
| **23.2.2** | The organization at any time ran a version of Microsoft Exchange Server 2010 through to 2019 vulnerable to the zero-day exploits being targeted. | Yes |
| **23.2.3** | Please describe the measures undertaken to investigate any potential malicious activity in your organization's system. | exchange servers were not directly exposed to internet (WAF segregated) Patches applied within 24h, Microsoft scripts were run, no IoCs detected |
| **23.2.4** | Any evidence of malicious activity as a result of this Microsoft Exchange vulnerability was found on your organization's system. | No |
| **23.2.5** | The appropriate patch/upgrade has been applied to your organization's system as recommended by Microsoft. | Yes |

|  |  |  |
| --- | --- | --- |
| **23.3 Pulse Connect Secure VPN** | | |
|  | **Question** | **Answer** |
| **23.3.1** | The organization uses Pulse Connect Secure VPN products. | No |
| **23.3.2** | The organization has run the KB44755 Pulse Connect Secure (PCS) Integrity Assurance tool to check for the possibility of compromise. | Not Applicable |

|  |  |  |
| --- | --- | --- |
| **23.4 Accellion FTA** | | |
|  | **Question** | **Answer** |
| **23.4.1** | The organization uses the Accellion FTA product. | No |
| **23.4.2** | The organization at any time used the Accellion FTA product. | No |
| **23.4.3** | Your organization is not aware of your data being exposed as a result of the Accellion FTA incident. | Yes |

|  |  |  |
| --- | --- | --- |
| **23.5 Log4j** | | |
|  | **Question** | **Answer** |
| **23.5.1** | The organization identified vulnerable versions of Log4j in enterprise systems, including but not limited to: applications, on-premise software components, cloud software components, in-house software development, and third-party technology providers. | Yes |
| **23.5.2** | The organization developed software affected by the Log4j vulnerability. | Yes |
| **23.5.3** | Please describe the measures undertaken to investigate and remediate any potential malicious activity in your organization’s system. | ... |
|  | Comment | All affected systems and libraries were identified (including scan of all github projects), special vulnerability scan performed (tenable) to find them, patches applied, FWs configured with IoCs to detect attack patterns, internet-facing systems were temporarily isolated or taken offline until patch could be applied, |
| **23.5.4** | Please describe the timelines for remediation of impacted systems. | internet-facing systems were neutralized in a prioritized fashion over the course of 4 weeks, total time to mitigation: 4 months |
| **23.5.5** | Please describe the measures for detection implemented. | see above |
| **23.5.6** | The organization has contacted critical suppliers and vendors to determine if they have identified and remediated the Log4j vulnerability in their systems and services. | Yes |

**24. External Partner Accompaniments**

|  |  |  |
| --- | --- | --- |
| **24.1 AIG | Data Security & Business Continuity** | | |
|  | **Question** | **Answer** |
| **EPA.1.1** | Select one response:  How centralized is the Applicant’s information security program? | Other (indicate to the right and describe in comments section at end of Data Security & Business Continuity section). |
|  | Comment | tbv?? IT, Legal, Insurance |
| **EPA.1.2** | With regards to the Applicant's management of information technology assets (hardware and software): | |
|  | The Applicant has a process to update its hardware asset inventory at least weekly based on discovery tools or IP Address Management (IPAM) software. | X |
| **EPA.1.3** | Select all responses that are true: With regards to the Applicant's management of "Vital Assets": | |
|  | The Applicant has an inventory of all data stores - including data owner, the asset it's stored on, sensitivity, retention limits and disposal requirements - for at least all sensitive data and updates it at least annually. |  |
|  | The Applicant has defined and documented all "Vital Assets". |  |
|  | The Applicant has a process to actively identify "Vital Assets" and update the inventory of "Vital Assets" at least quarterly |  |
|  | The Applicant prioritizes "Vital Assets" by importance to business operations. | X |
|  | None of the above. |  |
|  | Comment | Hardware asset inventory is in place, software asset inventory is in inplementation, software asset scanning available, data asset inventory is planned, classification of vital assets ongoing as data asset inventory becomes available |
| **EPA.1.4** | With respect to the Applicant's disaster recovery capabilities: | |
|  | At least quarterly, Applicant tests its ability to restore different "Vital Assets" in accordance with the Recovery Time Objective (RTO). |  |
|  | Comment | Customer facing vital assets (e.g. webshop) are operated on kubernetes clusters ensuring high availability including self-healing capabilities, each day parts of the infrastructure are being discarded and replaced (e.g. node out of date/failure) |
| **EPA.1.5** | Select all responses that are true: With respect to the Applicant's backup capabilities: | |
|  | Applicant’s backup strategy includes onsite, regular backups. | X |
|  | Applicant’s backup strategy includes offsite, regular backups (Cloud or Continuity of Operations Site). | X |
| **EPA.1.6** | Select all responses that are true: With respect to the Applicant's monitoring of "Vital Assets": | |
|  | The Applicant has an internal function and/or has an outsourced Managed Security Service Provider (“MSSP”) charged with monitoring security event alerts, including alerts on "Vital Assets" (a "Security Operations Center" or "SOC"). | X |
|  | The Applicant's SOC/MSSP is provided an updated list of "Vital Assets" at least quarterly. |  |
|  | The Applicant's SOC/MSSP uses a Security Information and Event Monitoring (SIEM) solution to automate the collection of logs from "Vital Assets". | X |
|  | None of the above/Don’t know. |  |
|  | Comment | Updated list of vital assets is directly available to SOC, not all vital assets classified, see EPA 1.3SIEM/EDR connected to most systems (98% of all systems capable of installing MDE) including vital assets, as inventory is updated, finetuning of log collection will take place |

|  |  |  |
| --- | --- | --- |
| **24.2 AIG | Identity, Credential, and Access Management Security** | | |
|  | **Question** | **Answer** |
| **EPA.2.1** | With respect to the Applicant's account management: | |
|  | The Applicant's inventory of accounts includes the individual's name, username, start/stop dates, and department. | X |
| **EPA.2.2** | With respect to the Applicant's policies and technical controls on passwords: | |
|  | The Applicant educates users on the risks of password reuse and has a policy against it. | X |
|  | Comment | technically enforced, regular awareness trainings |
| **EPA.2.3** | Select one response: How do both employees and vendors of the Applicant authenticate to those Vital Assets which are SaaS/3rd party applications? | MFA is required by policy for all access to externally hosted Vital Assets, and all exceptions to the policy are documented. |
|  | Comment | ??tbv |
| **EPA.2.4** | Select one response: Authenticator Assurance Level (AAL) which best represents the Applicant's authentication solution(s). NIST Special Publication 800-63B defines the Authenticator Assurance Levels. |  |
|  | Comment | ??tbv |
| **EPA.2.5** | Use separate rows in the text box provided below for each “Privileged” “Service Account” (the number of active Privileged Service Accounts is provided in the Marsh Cyber Self-Assessment | Identity and Access Management section | question 1.6). Within each row indicate the following attributes for each “Privileged” “Service Account”:    a. The name of the account  b. The privileges it has,   c. The software product it supports,   d. What hosts the service account is authenticating to, and  e. Why those entitlements are required | This information is confidential |
| **EPA.2.6** | Select one response: Which description below best reflects the Applicant's posture with respect to access controls for each user's workstation? For the purposes of this question, where the Applicant is using an endpoint privilege manager or other similar technology to allow users to temporarily request administrative access for certain activities, that should not be considered "admin access". | Applicant's policy is that employees by default are not in the Administrators' group and do not have local admin access; all exceptions to the policy are documented. |

|  |  |  |
| --- | --- | --- |
| **24.3 AIG | Security Monitoring and Incident Response** | | |
|  | **Question** | **Answer** |
| **EPA.3.1** | With respect to the Applicant's security and network monitoring capabilities: | |
|  | Applicant has tools to monitor for data loss (DLP) and they are in blocking mode. |  |
| **EPA.3.2** | What percentage of the Applicant's "Vital Assets" are being logged and forwarded to a SIEM solution? | 98 |
|  | Comment | 98% of capable devices equipped with EDR, remainder: ??tbv |
| **EPA.3.3** | Select all responses that are true: With respect to how the Applicant validates the efficiency and effectiveness of security controls: | |
|  | Applicant uses Breach and Attack Simulation (BAS) software to verify the effectiveness of security controls. |  |
|  | Applicant has a "red team" on staff to test security controls, or at least annually engages experts to perform a penetration test focused on internal systems. | X |
| **EPA.3.4** | Does the Applicant have a documented process to respond to phishing incidents (whether targeted specifically at the Applicant or its employees, or not)? | Yes |

|  |  |  |
| --- | --- | --- |
| **24.4 AIG | Risk Management** | | |
|  | **Question** | **Answer** |
| **EPA.4.1** | Does the Applicant have a vulnerability scanning program which identifies and manages vulnerabilities across "Vital Assets"? | Yes |
| **EPA.4.2** | Select all responses that are true: With respect to the factors the Applicant uses to prioritize patching: | |
|  | Common Vulnerability Scoring System (CVSS) score. | X |
|  | Correlation with whether the vulnerability affects the Applicant's "Vital Assets". | X |
|  | Generic threat intelligence (e.g., that threat actors are exploiting a given vulnerability; this includes tools like CISA’s Known Exploited Vulnerability Catalog). | X |
|  | Threat intelligence specific to the Applicant (including intelligence that threat actors may be targeting the Applicant specifically via exploitation of a certain vulnerability, or data from the Applicant’s environment which indicates where threat actors are focused). |  |
|  | None of the above/Don't know. |  |
|  | Comment | Each discovered vulnerability is assessed according to CVSS score, exploitability and criticality of asset (&quot;Vital Asset&quot;) |
| **EPA.4.3** | Select all responses that are true: With respect to the Applicant's policies for the use of organizational IT assets: | |
|  | Users are disallowed from accessing personal email from organizational assets. |  |
|  | Users and administrators are required to report suspected violations. | X |
| **EPA.4.4** | Select all responses that are true: With respect to the Applicant's capabilities to monitor for risky behavior and malicious insiders: | |
|  | Applicant monitors for when a user or administrator account sets an insecure password. |  |
|  | Applicant monitors for when “Privileged” accounts access unauthorized websites and services. |  |
|  | Applicant monitors for unauthorized remote access to "Vital Assets". | X |
|  | Comment | Insecure passwords are prevented by password policy (technically enforced)Definition of &quot;Privileged Accounts&quot; applies only to Tier 0 accounts (except Azure Privileged Role Admin), which do not have internet access and are restricted to PAWsFor Azure AD PIM is active |

|  |  |  |
| --- | --- | --- |
| **24.5 AIG | Phishing Defense** | | |
|  | **Question** | **Answer** |
| **EPA.5.1** | With respect to the Applicant's capabilities for mitigating phishing incidents: | |
|  | Where the Applicant is conducting simulated phishing attacks, the success ratio was less than 15% on the last test (less than 15% of employees were successfully phished). | X |
|  | Comment | &lt; 7% |
| **EPA.5.2** | Select all responses that are true: With respect to the Applicant's capabilities to block potentially harmful websites and/or email: | |
|  | Applicant blocks uncategorized and newly registered domains using web proxies or DNS filters. |  |
|  | Applicant's web filtering capabilities are effective on all organization assets, even if the asset is not on the organization's network (e.g., assets are configured to utilize cloud-based web filters or require a VPN connection to browse the internet). |  |
|  | Comment | ??tbvweb content filtering on clients will be in place by October 2023 (not in VPN/on-prem, already in place for VPN/on-prem) |

|  |  |  |
| --- | --- | --- |
| **24.6 AIG | Malware Defense** | | |
|  | **Question** | **Answer** |
| **EPA.6.1** | Select all responses that are true: With respect to the Applicant's endpoint security tool's capabilities: | |
|  | Applicant uses endpoint security tools with behavioral-detection and exploit-mitigation capabilities. | X |
|  | Applicant uses an endpoint threat detection and response (ETDR or EDR) tool which does all the following: monitors for threat indicators; identifies patterns which match known threats; automatically responds by removing or containing threats; alerts security personnel of incidents; provides forensic and analysis capabilities to allow analysts to perform threat hunting activities. | X |
|  | Applicant implements application controls across workstations to only allow for execution of authorized applications. Unauthorized applications are blocked, and the list of authorized applications is reassessed at least bi-annually. |  |
|  | Comment | Application whitelisting is active for Tier 0, Blacklisting on all clients |
| **EPA.6.2** | Select all responses that are true: With respect to the Applicant's capabilities to limit lateral movement: | |
|  | Applicant has implemented host firewall rules that prevent the use of RDP to log into workstations. | X |
|  | Applicant has configured all service accounts to deny interactive logons. | X |
|  | Comment | There are documented exceptions where service accounts require interactive logon for technical reasons |

|  |  |  |
| --- | --- | --- |
| **24.7 AIG | Third Parties & Managed Service Providers Defense** | | |
|  | **Question** | **Answer** |
| **EPA.7.1** | Select all responses that are true: With respect to the roles of third parties or Managed Service Providers (MSPs) for the Applicant's network, including remote access to resources such as cloud and VPNs | |
|  | Applicant utilizes an MSP for administration of "Vital Assets". | X |
|  | Applicant utilizes an MSP for security operations. | X |
|  | Applicant utilizes an MSP for data backup and recovery. | X |
|  | Applicant utilizes an MSP for cloud transformation. | X |
|  | Applicant utilizes an MSP for software development. | X |
|  | Applicant provides third parties persistent ("always on") access to corporate resources (access does not require Applicant's authorization). | X |
|  | None of the above/Don’t know. |  |
|  | Comment | With a very complex IT landscape, we use MSPs in multiple locations, details can be provided upon request |

|  |  |  |
| --- | --- | --- |
| **24.8 AIG | Perimeter and Internet Defense** | | |
|  | **Question** | **Answer** |
| **EPA.8.1** | Select all responses that are true: With respect to the Applicant's capabilities to secure externally-exposed systems, including internet-facing systems: | |
|  | Applicant maintains an inventory of externally-exposed assets. | X |
|  | Applicant has a Web Application Firewall (WAF) in front of all externally-exposed applications, and it is in blocking mode. | X |
|  | Applicant uses an external service to monitor its attack surface (internet-facing systems). | X |
|  | Applicant disables or blocks on externally-exposed systems those ports, services, and protocols known to allow the spread of ransomware, including, but not limited to RDP, SMBv1, and SMBv2. | X |
|  | Applicant’s externally-exposed assets are segmented within a demilitarized zone (DMZ), and the DMZ is not directly routable to the corporate network. Users requiring access to DMZ services are routed to the internet for access. |  |
|  | Comment | NimbusSec for external attack surface monitoringDMZ is in place, however ??tbv |

**25. Media**

|  |  |  |
| --- | --- | --- |
| **25.1 Media** | | |
|  | **Question** | **Answer** |
| **ME.1.1** | The organization’s media activities include: (select all that apply) | |
|  | Television |  |
|  | Radio |  |
|  | Print |  |
|  | The organization’s website(s). (If selected, please list domain names in commentary box) |  |
|  | Internet advertising |  |
|  | Social media |  |
|  | Marketing materials |  |
|  | Audio or video streaming |  |
|  | Other (If selected, please describe in commentary box) |  |
| **ME.1.2** | The organization has a formal review process conducted with legal counsel to screen and clear material for intellectual property and compliance prior to any publication, broadcast, distribution, or use. |  |
| **ME.1.3** | The formal review process includes any published or broadcast material, including digital content, and titles, trademarks and/or service marks for all domain names, service names, designs, and logos. |  |
| **ME.1.4** | The organization allows third-party generated content to be displayed on its website(s). |  |
| **ME.1.5** | Protections with third-party content providers and contributors – including freelancers, independent contractors, and other talent – include: (select all that apply) | |
|  | Written permissions or releases are obtained. |  |
|  | Indemnification or hold harmless agreements in the organization’s favor are required. |  |
| **ME.1.6** | The organization has established an employee education program for issues relating to intellectual property, defamation, privacy, and information gathering. |  |
| **ME.1.7** | Please describe the policies and procedures for addressing controversial or potentially defamatory or infringing content on the organization’s website(s). |  |

**26. Tech Errors and Omissions**

|  |  |  |
| --- | --- | --- |
| **26.1 Technology Products and Services** | | |
|  | **Question** | **Answer** |
| **TE.1.1** | Indicate the products and services the organization offers, and the annual revenues (nominal or as a percentage) associated with each service. |  |

|  |  |  |
| --- | --- | --- |
| **26.2 Business Structure** | | |
|  | **Question** | **Answer** |
| **TE.2.1** | The organization has made significant changes in business activities/structure within the last 12 months, or anticipates significant changes in business activities/structure within the next 12 months. If yes, please provide detail in commentary. |  |

|  |  |  |
| --- | --- | --- |
| **26.3 Client Contracts** | | |
|  | **Question** | **Answer** |
| **TE.3.1** | The number of clients the organization currently has: |  |
| **TE.3.2** | The average contract size of the organization with current clients: |  |
| **TE.3.3** | The length of the organization's average contract: |  |
| **TE.3.4** | Indicate the contract value and duration of the organization's top 5 clients. |  |
| **TE.3.5** | The organization's percentage of professional services provided by written contract is: |  |
| **TE.3.6** | The following risk mitigation clauses are included in your standard terms and conditions: (select all that apply) | |
|  | Customer Acceptance/Final Sign Off |  |
|  | Force Majeure |  |
|  | Limitation of Liability |  |
|  | (New) Monetary Cap on Direct Damages |  |
|  | Exclusion of Consequential Damages |  |
|  | Hold Harmless Agreements |  |
|  | Payment Terms |  |
|  | Disclaimer of Warranties |  |
|  | Indemnification Clause |  |
|  | (New) Dispute Resolution or Escalation Procedure |  |
|  | Project Phases/Milestones |  |
| **TE.3.7** | The percentage of contracts that the organization enters into with standard terms and conditions and without modifications is: |  |
| **TE.3.8** | The organization's customer facing colleagues are able to modify standard contractual terms and conditions within certain parameters. |  |
| **TE.3.9** | Further modifications to standard contract agreements are approved by legal counsel. |  |
| **TE.3.10** | The organization’s policy is not to enter into contracts with uncapped liability. |  |

|  |  |  |
| --- | --- | --- |
| **26.4 Subcontracting** | | |
|  | **Question** | **Answer** |
| **TE.4.1** | The percentage of the organization's services involving subcontracting is: (e.g. independent contractors, temporary workers, or other non-employees) |  |
| **TE.4.2** | The percentage of subcontractors with whom the organization has written contracts is: |  |
| **TE.4.3** | Written contracts for agreements between subcontractors: | |
|  | Uses standardized contract language. |  |
|  | Contains indemnification or hold harmless agreements in favor of your organization. |  |
|  | Identifies work product as ‘work made for hire’ or includes other provisions for the ownership of intellectual property. |  |
|  | Includes requirements to follow the organization's standard cybersecurity control protocols. |  |
| **TE.4.4** | The organization requires subcontractors to carry: (select all that apply, and indicate standard insurance limit requirements in comments) | |
|  | Professional liability insurance |  |
|  | Cyber insurance |  |
| **TE.4.5** | Please describe the organization's formal vetting procedure for subcontractors. |  |

|  |  |  |
| --- | --- | --- |
| **26.5 Quality Control** | | |
|  | **Question** | **Answer** |
| **TE.5.1** | The organization has an escalation procedure for customer or product-support complaints. If yes, please describe your escalation procedure. |  |
| **TE.5.2** | The organization uses the following practices in quality control and customer support procedures. (select all that apply) | |
|  | Alpha and Beta Testing Procedures |  |
|  | Vendor or VAR Certification Process |  |
|  | Final Customer Sign off Requirements |  |
|  | User Acceptance Testing Measures |  |
|  | Documented Project Milestone Procedures |  |
|  | 24/7 Customer Support |  |
|  | Pre-Release Screening for Design Errors/Flaws |  |
|  | Documented Customer Complaint/Escalation Process |  |
|  | Written Functional Specification Requirements |  |
|  | Internal Post Project Review Procedures |  |
|  | (New) Written Product Recall Process |  |
|  | Other |  |

|  |  |  |
| --- | --- | --- |
| **26.6 Intellectual Property Rights** | | |
|  | **Question** | **Answer** |
| **TE.6.1** | The organization has written policies and procedures in place for: | |
|  | Auditing the organization's use of software licenses. |  |
|  | Avoiding copyright infringement with regard to software/computer code. |  |
|  | Responding to allegations of copyright infringement with regard to software/computer code. |  |
|  | Determining if open source code is used during the organization's software development efforts. |  |
|  | Other formal safeguard procedure against infringing on IP. (describe below) |  |
| **TE.6.2** | Those who provide software code to the organization, including developers and independent contractors, are required to: | |
|  | Assign or license the Applicant their rights to the use of the code. |  |
|  | Warrant that their work does not violate another party’s IP rights. |  |
|  | Indemnify the Applicant when an IP infringement claim is made against them based on the code provided. |  |

**27. Operational Technology**

|  |  |  |
| --- | --- | --- |
| **27.1 Access Control** | | |
|  | **Question** | **Answer** |
| **OT.1.1** | Does your organization have a policy to govern remote and third party access for employees, contractors and third parties? |  |
| **OT.1.2** | Your OT environment is segmented from your Information Technology (IT) environments in the following ways: (select all that apply) | |
|  | Unidirectional Security Gateways |  |
|  | VLANs |  |
|  | DMZs |  |
|  | Other |  |
| **OT.1.3** | Can employees remotely access the OT environment |  |
| **OT.1.4** | Do you permit employees remote access to your OT environment? |  |
| **OT.1.5** | Can third-parties remotely access the OT environment? |  |
| **OT.1.6** | Is MFA enforced for third-party remote access to the OT environment? |  |
| **OT.1.7** | Does your organization monitor and alert when ICS, SCADA, and OT administrative credentials are used for non-administrative functions? |  |
| **OT.1.8** | Does your organization scan all enterprise devices remotely logging into the organization's ICS, SCADA, and OT network prior to accessing the ICS, SCADA, and OT network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices? |  |
| **OT.1.9** | Where possible, does your organization configure access for all ICS, SCADA, and OT accounts through as few centralized points of authentication as possible, including network, security, and cloud systems? |  |
| **OT.1.10** | How do you manage domain controllers? |  |
| **OT.1.11** | Do you block internet access to domain controllers? |  |
| **OT.1.12** | Do you maintain a list of assets which are under the scope of Domain controller and which are not? |  |
| **OT.1.13** | Does your organization manage OT credentials separately from IT credentials? Ie. Are there separate credentials for IT versus OT users. |  |

|  |  |  |
| --- | --- | --- |
| **27.2 ICS Network / Endpoint Monitoring** | | |
|  | **Question** | **Answer** |
| **OT.2.1** | Does your organization utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur within your organizations ICS, SCADA, and OT environments? |  |
| **OT.2.2** | Does your organization configure monitoring systems to record network packets passing through the boundary at each of the organization's ICS, SCADA, and OT network boundaries? |  |
| **OT.2.3** | Does your organization deploy network-based Intrusion Detection Systems (IDS) sensors within ICS, SCADA and OT environments to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's ICS, SCADA and OT network boundaries? |  |
| **OT.2.4** | For your critical ICS, SCADA, and OT, does your organization enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring)? |  |
| **OT.2.5** | Does your organization ensure that all ICS, SCADA, and OT accounts have an expiration date that is monitored and enforced? |  |
| **OT.2.6** | Does your organization use a network based data loss prevention (DLP) solution to monitor and control the flow of data within the ICS, SCADA, and OT environment? |  |
| **OT.2.7** | Does your organization monitor attempts to use deactivated ICS, SCADA, and OT accounts through audit logging? |  |
| **OT.2.8** | For your critical ICS, SCADA, and OT assets, does your organization receive an alert when ICS, SCADA, and OT users deviate from normal login behavior (such as unusual login hours, login duration, login from unexpected regions, inconsistent login frequency, and simultaneous logins)? |  |
| **OT.2.9** | Does your organization employ an Endpoint detection and response on supported workstations, servers and endpoints? |  |
| **OT.2.10** | Does your OT security monitoring feed into a Security Operations Center? |  |

|  |  |  |
| --- | --- | --- |
| **27.3 Business Continuity & Incident Response Planning** | | |
|  | **Question** | **Answer** |
| **OT.3.1** | Do you have a documented Business continuity/Disaster recovery Plan? How frequently is it reviewed? Does your Business Continuity Plan account for plans to recover from an ICS\_SCADA\_OT cybersecurity event? |  |
| **OT.3.2** | Does your organization use any of the following techniques for ICS\_SCADA\_OT data recovery? (Please select all that apply) | |
|  | Where applicable, ensure that all system data is automatically backed up on a regular basis |  |
|  | Where applicable, ensure that configuration exports are conducted on a regular basis |  |
|  | On a regular basis, perform system restoration exercises to ensure that the backups are properly working |  |
|  | Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network |  |
|  | Ensure that system backups and recovery procedures are documented |  |
|  | In cases where devices are not capable of complete backups, all software, settings, and configurations are captured in order to perform a restoration process |  |
| **OT.3.3** | Does your organization ensure that all ICS, SCADA, and OT backups have at least one backup destination that is not continuously addressable through operating system calls? |  |
| **OT.3.4** | As related to ICS\_SCADA\_OT, does your organization use any of the following incident response and management techniques? (Please select all that apply) | |
|  | Written incident response plans define roles of personnel and phases of incident handing/management |  |
|  | Job titles and duties for handling incidents are assigned to certain individuals and ensure tracking and documentation occur throughout the incident |  |
|  | Designated management personnel, as well as backups, who will support the incident handling process |  |
|  | Assemble and maintain information on third-party contact information to be used for reporting an security incident |  |
|  | The Incident Response plan has been reviewed and approved by ICS Operational Leadership |  |
|  | Response team are familiar with escalation procedure for OT incidents |  |
|  | Response teams are thoroughly familiar with the risks inherent to the ICS environment |  |
|  | Response team are thoroughly familiar with the mitigations to prevent secondary damage that may impact operational safety and protection of personnel, equipment, information, and a myriad of other dependent and interdependent factors. |  |
|  | Create incident scoring and prioritization schema based on known or potential impact |  |
|  | At least once a year, the business conducts cybersecurity incident tabletop exercises that include threats to ICS\_SCADA\_OT |  |
|  | These tabletop exercises also include ransomware as a potential threat to ICS\_SCADA\_OT |  |
| **OT.3.5** | Who is authorized to respond to incidents? (select all that apply) | |
|  | MSSP |  |
|  | SOC |  |
|  | Other |  |

|  |  |  |
| --- | --- | --- |
| **27.4 Incident Response Planning** | | |
|  | **Question** | **Answer** |
| **OT.4.1** | Does the organization use uninterruptable power supplies? If yes, for how many sites/facilities? |  |

|  |  |  |
| --- | --- | --- |
| **27.5 Internet of Things** | | |
|  | **Question** | **Answer** |
| **OT.5.1** | Does your organization utilize IoT devices? (If responding yes to this question please fill out questions 2-11) |  |
| **OT.5.2** | Does your organization use any of the following techniques to control the use of Critical\_IoT administrative privileges? (Please select all that apply) | |
|  | Default passwords are changed to something unique |  |
|  | Administrative accounts or accounts controlling a device use unique accounts with dedicated administrative passwords. |  |
|  | Administrative accounts for management applications use unique passwords |  |
|  | If possible, unsuccessful administrative account login attempts are logged and alerted. |  |
| **OT.5.3** | Does your organization maintain documented security configurations for Critical\_IoT? |  |
| **OT.5.4** | Does you organization verify that updates are regularly applied to Critical\_IoT devices? |  |
| **OT.5.5** | As related to Critical\_IoT, does your organization log inbound and outbound traffic for the discovery of malware infections? |  |
| **OT.5.6** | Does your organization perform any of the following in regards to Critical\_IoT assets? (Please select all that apply.) | |
|  | Conduct at least monthly critical risk assessments to identify active ports, services, and protocols running on the critical assets |  |
|  | After each risk assessment ensure that only expected and approved network ports, protocols, and services are running on each device |  |
|  | Apply firewalls or port filtering tools on systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed |  |
|  | Place firewalls in front of any critical systems to verify and validate the traffic going to the server and any unauthorized traffic is blocked and logged |  |
|  | Prevent Critical\_IoT assets from being directly accessed via the internet |  |
| **OT.5.7** | Does your organization regularly back up Critical\_IoT data to approved backup locations? |  |
| **OT.5.8** | Does your organization regularly perform tests of restoring Critical\_IoT from backed up data? |  |
| **OT.5.9** | For your Critical\_IoT, does your organization require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication? |  |
| **OT.5.10** | For your Critical\_IoT, does your organization scan all enterprise devices remotely logging into the organization's network prior to accessing the network? |  |
| **OT.5.11** | Does your organization have process for monitoring and disabling accounts in regards to your Critical\_IoT? (Please select all that apply) | |
|  | An automated process for revoking system access by disabling accounts immediately upon termination or employee changes responsibilities |  |
|  | Disable any account that is not associated with a business process or business owner |  |
|  | Automatically disable dormant accounts after a set period of inactivity |  |
|  | Ensure all accounts have an expiration date that is enforced |  |
|  | Monitor attempts to access deactivated accounts |  |
|  | Alert when users deviate from normal login behavior |  |

|  |  |  |
| --- | --- | --- |
| **27.6 Inventory / Asset Visibility** | | |
|  | **Question** | **Answer** |
| **OT.6.1** | Does your organization use any of the following techniques to inventory and control ICS\_SCADA\_OT hardware assets ? (Please select all that apply.) | |
|  | Maintain an accurate and up-to-date inventory of new and old devices from multiple vendors, including up-to-date technical drawings |  |
|  | Ensure that all equipment acquisitions and system modifications follow an approval process and the technical drawings are updated |  |
|  | Immediate removal of unauthorized equipment |  |
| **OT.6.2** | Does your organization use any of the following techniques to inventory and control ICS\_SCADA\_OT software assets? (Please select all that apply) | |
|  | Maintain an up-to-date list of recommended and supported software and versions, from the ICS manufacturers and vendors, that are required for each system. |  |
|  | Forecast operating systems and application lifecycle cost in alignment with typical COTS (commercial off the shelf software) End of Life and End of Support (EoL/EoS) Notifications. |  |
|  | Ensure cybersecurity requirements and secure development lifecycle are a consideration within procurement/sourcing processes. |  |

|  |  |  |
| --- | --- | --- |
| **27.7 Network Architecture** | | |
|  | **Question** | **Answer** |
| **OT.7.1** | Does your organization physically or logically segregate ICS, SCADA, and OT assets from the rest of the organization? |  |
| **OT.7.2** | Are there any dual homed computers in the ICS architecture ( ie. Dual homed means having infrastructure such as servers in both IT and OT environments)? |  |
| **OT.7.3** | Are emergency shutdown systems segregated from control systems and sensing functions? |  |

|  |  |  |
| --- | --- | --- |
| **27.8 Network Security** | | |
|  | **Question** | **Answer** |
| **OT.8.1** | For your critical ICS\_SCADA\_OT assets does your organization enable anti-exploitation features, deploy appropriate toolkits that offer additional malware protection, and/or use ICS\_SCADA\_OT firewalls to block malicious activity? |  |
| **OT.8.2** | Does your organization leverage the use of wireless networks and technology within the ICS\_SCADA\_OT environment? (if yes, then please answering the Wireless Access Control questions below.) |  |
| **OT.8.3** | Does your organization use any of the following techniques to track, control, prevent, and correct the security use of wireless local area networks (WLANs), access points, and wireless client systems within your ICS\_SCADA\_OT environment? | |
|  | Perform regular risk assessments to understand how a wireless incident may impact personal and functional safety, lead to ICS disruption, damage, or destruction of digital and physical products and services |  |
|  | Ensure wireless ICS system utilizing Public Key Infrastructure (PKI), enforce expiration dates, non-repudiation and certificate chains validation, and revocation |  |
|  | Ensure wireless (including cellular, sat, etc.) based ICS systems do not fail open when jammed |  |
|  | Ensure wireless (including cellular, sat, etc.) based ICS networks are controlled/private networks |  |
|  | Ensure software security patches and product upgrades are applied throughout the wireless infrastructure and products are kept current throughout their lifecycle |  |
|  | If wired connection is more appropriate, then use that connection in place of wireless |  |
|  | Where possible, limit wireless signal strength and range to what is necessary for the application in order to reduce the potential for remote accessibility of the connection from outside a security perimeter |  |
|  | Ensure that rogue wireless discovery tools are set to alert only |  |
|  | Ensure that all wireless connections are persistent, encrypted, defined point-to-point or point-to-multipoint wireless configuration |  |
|  | Ad hoc or guest connections are not permitted |  |
| **OT.8.4** | Does your organization prevent ICS\_SCADA\_OT assets from being directly accessed via the internet? |  |
| **OT.8.5** | Does your organization apply host-based firewalls or port filtering tools on systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed? |  |
| **OT.8.6** | Does your organization place application firewalls in front of any critical systems to verify and validate the traffic going to the server and any unauthorized traffic is blocked and logged? |  |
| **OT.8.7** | Does your organization ensure that network firewalls, within the ICS\_SCADA\_OT environment, are configured to deny by default? |  |
| **OT.8.8** | Does your organization use any of the following techniques to track, control, prevent, and correct secure access to critical ICS\_SCADA\_OT assets according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification. (select all that apply) | |
|  | ICS systems are physically and logically network segmented |  |
|  | Enable firewall filtering between ICS and non-ICS networks to ensure that only authorized systems are able to communicate with ICS systems necessary to fulfill their specific responsibilities |  |
|  | Encrypt all sensitive information in transit between ICS and non-ICS networks |  |
|  | Enforce detailed audit logging for access to sensitive ICS data or changes to sensitive ICS data |  |
|  | Enable access control lists to restrict data and system access to only authorized individuals and systems |  |
| **OT.8.9** | For your ICS\_SCADA\_OT, does your organization deploy web application firewalls (WAFs) or application firewalls that inspect traffic flowing to the ICS\_SCADA\_OT web application? |  |
| **OT.8.10** | Does your organization configure the ICS, SCADA, and OT servers to automatically conduct an anti-malware scan of removable media when inserted or connected? |  |
| **OT.8.11** | Does your organization configure the assets hosting ICS, SCADA, and OT assets to not auto-run content from removable media? |  |
| **OT.8.12** | Does your organization configure systems not to write data to external removable media, if there is no business need for supporting such devices. |  |

|  |  |  |
| --- | --- | --- |
| **27.9 Patch Management** | | |
|  | **Question** | **Answer** |
| **OT.9.1** | How does your organization patch OT systems ? |  |
| **OT.9.2** | What is the frequency for installation patches? |  |
| **OT.9.3** | For your ICS\_SCADA\_OT, does your organization maintain separate environments for production and non-production systems? Developers should not have unmonitored access to production environments. |  |

|  |  |  |
| --- | --- | --- |
| **27.10 Penetration Testing** | | |
|  | **Question** | **Answer** |
| **OT.10.1** | Does your organization use any of the following techniques for ICS\_SCADA\_OT penetration testing?(select all that apply) | |
|  | Leveraging both the internal OT team and specialized third parties to conduct regular security assessments to identify a greater diversity of vulnerabilities and attack vectors that can be used to breach security of ICS systems |  |
|  | Ensuring that personnel conducting vulnerability assessments are skilled in working within ICS environments to reduce the possibility of inadvertent negative impact to operations |  |
|  | Including tests for the presence of unprotected system information, data leakage, and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, documents containing passwords, or other information critical to system operation |  |
|  | Using results from vulnerability scans and security assessments in concert |  |
|  | Ensuring personal and functional safety, as well as protecting digital and physical assets throughout the testing process |  |
| **OT.10.2** | Ensuring personal and functional safety, as well as protecting availability of operations, the organization conducts intrusive penetration testing on: (select all that apply) | |
|  | The whole OT environment |  |
|  | Specific systems only |  |
|  | Specific vulnerabilities only |  |
|  | Red team/blue team exercise |  |
| **OT.10.3** | Has your organization created a test bed that mimics a production environment for specific ICS, SCADA, and OT penetration tests and Red Team exercises to prevent from adversely impacting the production environment? |  |
| **OT.10.4** | Does your organization deploy automated software update tools in order to ensure that your ICS, SCADA, and OT are running the most recent security updates provided by the software vendor, and/or does your organization retroactively remediate all high severity vulnerabilities (and OWASP-ICS/SCADA top 10 vulnerabilities) after each vulnerability scan? |  |

|  |  |  |
| --- | --- | --- |
| **27.11 Physical Security** | | |
|  | **Question** | **Answer** |
| **OT.11.1** | How is physical access controlled to critical devices? |  |

|  |  |  |
| --- | --- | --- |
| **27.12 Policies, Standards and Procedures** | | |
|  | **Question** | **Answer** |
| **OT.12.1** | Does your organization have an ICS\_SCADA\_OT specific cybersecurity policy? |  |
| **OT.12.2** | Does your organization employ dedicated personnel whose primary responsibility is ICS\_SCADA\_OT cybersecurity? |  |
| **OT.12.3** | If yes to #2, are the dedicated ICS\_SCADA\_OT personnel part of the IT Security organization? |  |
| **OT.12.4** | If yes to #2, are they part of the Engineering/Operational Support organization? |  |
| **OT.12.5** | Is there a dedicated budget for ICS\_SCADA\_OT cybersecurity? |  |
| **OT.12.6** | Who is authorized to approve the budget for SCADA OT Cybersecurity every year? |  |
| **OT.12.7** | Does your organization maintain documented, standard security configuration standards for all authorized ICS\_SCADA\_OT systems? |  |
| **OT.12.8** | Does your organization keep inventory of secure images as related to ICS\_SCADA\_OT? (Please select all that apply) | |
|  | Maintain secure images or templates for all systems in the enterprise |  |
|  | Store and monitor master images and templates on secure servers |  |
| **OT.12.9** | Does your organization implement any of the following security awareness and training programs for employees and contractors that interface with the ICS\_SCADA\_OT environment? (Please select all that apply) | |
|  | A completion of a security awareness program is for all visitors (Including 3rd parties: contractors, subcontractors, vendors, etc.). |  |
|  | Baseline physical and cybersecurity security education is provided to standardize knowledge, skills, and abilities (KSAs) for ICS personnel, as well as others that interface with and support ICS (e.g. IT personnel, ITOT Hybrid personnel, third-party contractors, service/support personnel, and others as appropriate). |  |
|  | Advanced immersive cybersecurity security education and training is provided to personnel expected to perform higher-risk, more advanced processes, or those who are making decisions relating to design, build, operation, and maintenance factors. |  |
|  | Standardizing on baseline and periodic measures of security KSAs including personnel capabilities assessments, required industry security certifications, security skills building roadmaps to grow personnel capabilities over time to better safeguard systems, reinforce best practices, and evolve as new risks are identified and new threats emerge. |  |
| **OT.12.10** | Are the facilities under the scope of coverage designed with mechanical safety protection devices in accordance with relevant regulations and standards ( API,ISO, IEC etc.) |  |
| **OT.12.11** | Are the facilities under the scope of coverage compliant with international safety and security standards such as NERC? |  |
| **OT.12.12** | How do you evaluate and manage the spare part requirements to resume business operations within defined time period in case of system failure. |  |

|  |  |  |
| --- | --- | --- |
| **27.13 Vendor Management** | | |
|  | **Question** | **Answer** |
| **OT.13.1** | List Control systems and the Vendor which supports the systems |  |
| **OT.13.2** | Does your organization have in place the following? | |
|  | A maintenance and support contract with all vendors for the systems which is reviewed annually. |  |
|  | The contract with vendors captures the escalation matrix of vendors which is reviewed annually. |  |
|  | A documented Third party security policy to ensure the implementation security controls with respect to the services provided by the Third Party. |  |
|  | Monitoring the service provided by the third party for ICS, SCADA and OT peripherals and review the services on periodic basis. |  |
|  | Document the changes in the services provided by the third party in the maintenance and support contract. |  |
|  | Perform risk assessment whenever there is change in the service provided by the third party and appropriate actions are taken for the closure of identified risks. |  |
|  | Enforced appropriate risk-based multifactor authentication (MFA). |  |
|  | Engagement with the internal security operations center to develop specific use cases for monitoring third party accesses. |  |
|  | Code of Conduct |  |
|  | Access management (provision/modification/revocation). |  |
|  | Training |  |

|  |  |  |
| --- | --- | --- |
| **27.14 Vulnerability Assessment** | | |
|  | **Question** | **Answer** |
| **OT.14.1** | Does your ICS\_SCADA\_OT environment contain legacy systems that the original manufacturer considers ‘end of life’ or that are no longer supported with security patches and updates? |  |
| **OT.14.2** | How often does your organization conduct ICS, SCADA, and OT vulnerability assessments? |  |
| **OT.14.3** | Does the organization have a defined process for identifying ICS\_SCADA\_OT devices with critical vulnerabilities? |  |
| **OT.14.4** | Does your organization use any of the following techniques for ICS\_SCADA\_OT continuous vulnerability management? (Please select all that apply) | |
|  | Before use in production, ensure that any vulnerability scanning tool does not cause adverse conditions that could alter the integrity of the system |  |
|  | Ensure that tools do not automatically deploy software into the production environment, but only report and identify where security updates are needed |  |
|  | Utilize an OEM vulnerability reporting service to identify all known vulnerabilities on the organization's ICS |  |
|  | Utilize passive monitoring tools which identify a specific device and software version and correlate that to known vulnerabilities |  |
|  | Operating system and application updates, security patches, and service packs need to be properly regression tested to ensure availability and reliability of the system will not be adversely affected |  |
|  | Create a test bed that mimics a production environment for specific patch regression testing prior to implementing in production OT environments |  |
| **OT.14.5** | Is there a defined patch management process in place for these devices? |  |