Solution should be able to setup "Data class" attribute for captured files and documents based on 1.3.9 data classification methods. 3.10 Solution should be able to capture from documents and check TITUS tags 3.11 Solution should be able to use in policy verification condition current daily UBA indicator for particular user 3.12 Solution should be able to copy existing policy 3.13 Solution should be able to setup duration period for particular policy and execution schedule (once, daily, weekly etc.) 3.14 Solution should be able to use as verification condition other policies that that was used on earlier verification steps for this particular object 3.15 Solution should be able to capture text from file combined from several binary objects with text 3.16 Solution should be able to setup required level of nested levels in archive file for data capturing 3.17 Solution should be able to perform backup export of all system settings data to structured file 3.18 Solution should be able to write incidents to SIEM instance using UDP and TCP protocol with the following protocols: CEF, LEEF, BSD syslog (RFC 3164), Syslog (RFC 5424) 3.19 Solution should be able to protect endpoint agent module against uninstallation in Programs and features console on workstation 3.20 Solution should be able to setup customizable uninstall password for agent module in Programs and features console on workstation 3.21 Solution should be able to perform hiding endpoint agent signs in the following in MS Windows consoles: – Agent processes in "Task manager" console – Entry in "Programs and features" console – Entry in "System services" console – File Explorer of OS. 3.22 Solution should provide endpoint agent launch in secure boot in MS Windows on workstation 3.23 Solution should be able to receive incidents and perform data sharing with workstations, which are not included in corporate MS Active Directory domain 3.24 Solution should be able export list of workstations where DLP agent is installed with the following details: host name and IP, DLP modules version, last synchronization date\time, policies and configuration settings 3.25 Solution should be able to open live monitoring session in management web console for particular workstation and user with the following options: – User's workspace live monitoring session – Making snapshots form the local web camera.5.10 Solution should be able to perform control and block file operations with files in peripheral and removable devices connected over MTP protocol 5.11 Solution should be able to manage size of the local storage of logs and shadow copies on endpoints 5.12 Solution should be able to perform selective file encryption to a USB removable device based on the contents analysis permission or file type of the copied file for particular policy 5.13 Solution should be able to perform files decryption only on workstations with installed endpoint DLP module 5.14 Solution should be able to capture microphone record from user workstation based on policies 5.15 Solution should be able to capture keystrokes from keyboard on user workstation 5.16 Solution should be able to capture photos from web-camera on user's workstation 5.17 Solution should be able to launch live monitoring session of user's workspace in active OS session by command from officer 5.18 Solution should be able to create snapshot of web-camera on user's PC by command from officer 5.19 Solution should be able to add customizable watermark in user's workspace on top of specific application launched in workstation 5.20 Solution should be able to add customizable text to the watermark for specific application or groups of applications 5.21 Solution should be able to block print screen operation in workstation for specific application launched 5.22 Solution should have application launch control module at endpoint to log and block EXE file execution on workstation 5.23 Solution should be able to create and apply new category

in the launch control policies with customized group of applications 5.24 Solution should be able to create new application entity with file path to its EXE or CRC fingerprint of target EXE file 5.25 Solution should be able to capture screenshots of workspace from user workstation (PNG and JPG file formats) 5.26 Solution should be able to process request from the user to obtain advanced access within the current set of local policies by means of the following methods: – Request to the system administrator over email – Unique code ID sharing and confirmation response code ID from system administrator over telephone.Detailed requirements for policy server module 3.1 Solution should have unified single policy server with the following policy creation schema: Selected Channel – Scope of verification rules – Auto executable system action 3.2 Solution should have single DLP management modern look web console for system officers and administrators to perform policy customization in policy creation wizard 3.3 Policy server should be able to implement particular policy to all or the following selected channels: Web Internet, SMTP mail, Instant Messengers, Printers, Removable devices, Clipboard, Keyboard on Workstation, Screen in workstation, Microphone in workstation, Web camera in workstation and Discovery crawler 3.4 Solution should be able to setup in policy creation wizard the following verification rules: – Incident attributes verification (User name, IP address, host name, file size, channel, recipient name, sender name, file text, body text, device name, incident type, web service, process, document metadata properties, current user's UBA index, user status, triggered policy, amount of printed pages, user belong to specific domain etc.) – Verification using particular digital fingerprints – Verification using particular dictionaries – File type verification (text, graphic, audio, video, archive, executable, encrypted data, unknown type) 3.5 Solution should be able to setup in policy creation wizard the following auto executable system actions: – Create incident in system repository with the following attributes: o Incident severity (high, medium or low) o Assign specific label to the incident o Assign customizable risk score value.Detailed requirements for Traffic Control module 4.1 Solution should be able to capture mail traffic both at mail server and at endpoint agent module 4.2 Solution should be able to capture SMTP, IMAP, POP3 mail traffic 4.3 Solution should be able to receive and analyze outgoing and incoming SMTP mail traffic from corporate SMTP mail servers 4.4 Solution should be able to control internal mail traffic from internal users on MS Exchange server 2007/2010/2013/2016 4.5 Solution should be able to install DLP interceptor plugin module on MS Exchange server 2007/2010/2013/2016 4.6 Solution should be able to receive over POP3 and HTTPS protocols mirrored mail traffic from operate mail SMTP server 4.7 Solution should be able to block mail in system mail quarantine 4.8 Solution should be able to install mail interceptor plugin module in Microsoft Outlook 2007/2010/2013/2016 and Mozilla Thunderbird at user's workstation 4.9 Solution should be able to capture HTTP/HTTPS traffic both at operational web-gateway module over ICAP protocol and at endpoint agent module 4.10 Solution should be able to decrypt and capture https traffic at endpoint using man in the middle (MITM) algorithm 4.11 Solution should be able to decrypt and capture https traffic at endpoint using deep API integration with the following browsers: Chrome, IE 8+, Firefox, Opera and Edge 4.12 Solution should be able to block web traffic in browser level using deep API integration without MITM tools 4.13 Solution should be able to capture FTP traffic 4.14 Solution should be able to capture the traffic from the following list of public web services: Gmail, Yahoo Mail, Google Docs, Office 365, OneDrive, Google Search, Facebook, Dropbox, LinkedIn, Live

Journal, Twitter, YouTube, Deposit files etc.4.15 Solution should be able to capture the traffic from Outlook Web App 4.16 Solution should be able to capture and log instant messenger traffic for the following messengers: WhatsApp, Telegram, ICQ, Skype, Viber and Jabber 4.17 Solution should be able to capture and block the following objects from WhatsApp thick client traffic flow: text chat messages and attached files 4.18 Solution should be able to capture and block the following objects from Telegram thick client traffic flow: text chat messages, attached files, audio records of voice session 4.19 Solution should be able to decrypt, capture and block instant messenger traffic from WhatsApp web service and Telegram web service opened in web browser on workstation 4.20 Solution should be able to decrypt, capture and log the following traffic from Skype application: text chat messages, attached files, audio records of voice session 4.21 Solution should be able to block launch of Skype application at user's workstation 4.22 Solution should be able to block file transfer via Skype application at user's workstation 4.23 Solution should be able to capture and log the following traffic from MS Teams desktop and Web Teams application: text chat messages, attached files, audio records of voice session 4.24 Solution should be able to setup the list of the applications whose internet traffic is processed by the endpoint DLP agent 4.25 Solution should be able to setup the list of the applications whose internet traffic is ignored by the endpoint DLP agent 4.26 Solution should be able to setup the lists of applications whose internet traffic should and should not be controlled or blocked by the agent 4.27 Solution should be able to setup the list of the applications that are allowed to establish incoming\outgoing connections 4.28 Solution should be able to setup the list of the applications whose incoming\outgoing connections are blocked 4.29 Solution should be able to setup the list of the hosts whose incoming and outgoing SSL traffic is not decrypted and not analyzed 4.30 Solution should be able to specify when the agent controls traffic on endpoint agent: – Corp domain available locally: the computer is connected to the local network – Corp domain available via VPN: the computer is connected to the domain via VPN – Corp domain unavailable: there is no active connection between the workstation and corp domain.1.2 Solution should have unified policy server where all system policy with filtering and verification rules, data classification methods and verification algorithms will be stored 1.3 Solution should have unified repository server to gather and retain all incidents from all monitored channels and users workstation with system attributes and shadow copy of original violated file or document 1.4 Solution should have unified DLP management web console for system officers and administrators to perform policy violation cases investigations, settings management and policies customization for all DLP modules and components 1.5 Solution should allow system officers and administrators to manage all settings and get access to incidents repository over unified DLP management web console 1.6 Solution should be able to collect and retain all incidents in one single database in system repository server based on RDBMS MS SQL Server 2019 and any later or PostgreSQL 9.6/10 or above 1.7 Solution should have unified single log server to log and store all system logs from other system servers and modules 1.8 Solution should have single deployment management server module to manage endpoint agents deployment 1.9 Solution should be able to deploy all server modules and components on single server instance with Microsoft Windows Server 2008R2/2012/2012R2/16/19/22 (x64) and Ubuntu Linux LTS 22.04.Detailed requirements for Device Control module 5.1 Solution should be able to setup access control list (ACL) for particular

peripheral and removable devices based on set of active policies for specific user 5.2 Solution should be able to setup access control list (ACL) for particular peripheral and removable devices (USB devices, Removable media etc) for the specific user with the following access rights: Full Access, Reading, Writing 5.3 Solution should be able to perform file operations control with peripheral and removable devices based on set of active policies for specific user 5.4 Solution should be able to perform file content analysis for file and document on peripheral and removable devices based on set of active policies for specific user 5.5 Solution should be able to perform control and block file operations with files in peripheral and removable USB devices based on the following policy verification rules: file attributes, document text digital fingerprints, content analysis with dictionaries and file types 5.6 Solution should be able to capture and create shadow copy for all violated files and documents 5.7 Solution should be able to perform control of printing operations and block file printing on printer devices based on the following policy verification rules: file attributes, document text digital fingerprints, content analysis with dictionaries and file types 5.8 Solution should have the following list of built-in device types classification for the use in device control policy creator wizard: – Typical device classes: USB devices, network devices, DVD/CD drives, removable media, printers, hard drives, PCMCAI adapters, modems, IrDA etc.Detailed requirements for Discovery Control module 6.1 Solution should be able to perform files scanning on workstations with installed endpoint DLP module in live mode or based on the schedule 6.2 Solution should be able to capture and create shadow copy for all violated files and documents 6.3 Solution should be able to perform scanning based on the following policy verification rules: file attributes, document text digital fingerprints, content analysis with dictionaries and file types 6.4 Solution should be able to setup target scope of folder on workstations that would not be scanned 6.5 Solution should have crawler module to perform remote scanning in shared folders on the file server 6.6 Solution should have crawler module to perform remote scanning in MS SharePoint and MS Exchange instances 6.7 Solution should be able to perform OCR recognition for analyzed files 6.8 Solution should be able to delete violated files from disc on specific workstation and create incident profile in system repository with copy of the original file.Solution should be able to extract text data and perform content analysis from files following types: HTML, MHT, CHM, XML, PDF, TXT, DOC, DOCX, RTF, PPT, PPTX, XLS, XLSX, XLSB, EML, MPP, MSG, ODB, ODF, ODG, ODP, ODS, ODT, PST, TNEF, WPS, WRI, CDW, FRW, M3D 2.2.Solution should have unified policy server with the following content analysis algorithms and techniques: – Dictionaries with keywords, also using wildcards (*, ?, ^, !, #, @) – Sets of customizable regular expressions and templates (credit cards, user SSN, etc.) – Digital fingerprint for the following entities: o Documents with the text content o Pictures and images o Set of target rows of source database – Bayesian probabilistic analysis method with dictionaries – Support Vector machine learning algorithm.– Place and block violator object in system mail quarantine – Send customizable notification over SMTP mail service – Push user notification alert in system tray in workstation – Remove violator object from mail body – Remove violator object from workstation – Create incident in event log instance – Write data to Syslog – Encrypt copied file – Create snapshot of user's workspace in active OS session – Create snapshot of web camera on user's PC – Assign specific status label to the selected user – Add Data Class – Active windows session logoff on target PC for the user with the following options: o

Repeated logon is impossible (logon blocking) o Block user account in domain active directory with specified duration.Solution should be able to extract text data and perform content analysis from archive files following types: 7z, ARC, ARJ, bzip2, CAB, gzip, ISO, RAR, tar, ZIP 2.3.Detailed requirements for data classification and categorization module 2.1.2.3.4.5.6.7.