قابلیت های نظارت بر ریسک SEARCH INFORM

SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

Fadak Rayan

فهرست مطالب

قابلیت های نظارت بر ریسک SEARCHINFORM

از نظارت بر ریسک SearchInform (SearchInform RM) برای جمع آوری و تحلیل جریانهای اطلاعاتی درون شبکه محلی استفاده می شود. داده ها از دو طریق گرفته می شود، بسته به مولفه های سرور: SearchInform EndpointController و SearchInform NetworkController. مولفه های سرور بسترهایی هستند که ماژولهای رهگیری داده بر روی آنها عمل می کنند.

هر ماژول رهگیری به عنوان تحلیلگر ترافیک عمل کرده و کانال انتقال داده خود را کنترل می کند.

این سند جزئیات کاملی از ماژول های رهگیری مولفه های سرور SearchInform RM در اختیار شما قرار می دهد.

1 قابلیت های ماژول های رهگیری ENDPOINTCONTROLLER برای ویندوزها

این جدول قابلیتهای SearchInform EndpointController را به شما نمایش خواهد داد. این کنترل از طریق نصب ایجنتهای خود بر روی ایستگاه های کاری شبکه کار خواهد کرد.

ماژول	امکانات	قابلیت ها
KeyLogger	1. دریافت کلید های خورده 2. دریافت کلید های عملکردی 3. دریافت متن از Clipboard	فیلتر برای کاربران/ گروها و یا پروسه ها. قابلیت نادیده گرفتن فعالیت های سیستمی. قابلیت نادیده گرفتن رهگیری کلمات عبور. مسدود سازی کلید PrintScreen. رهگیری فقط کلید های صفحه کلید/ Clipboard/ همگی. تنظیم حجم Clipboard.
FileController	کنترل هر رویداد فایل سیتم (ساخت، تغییر، بازکردن، حذف کردن، غیره.) برای فایلها و پوشه ها	فیلتر برای کاربران/ گروها و یا پروسه ها. قابلیت نادیده گرفتن فعالیت های سیستمی. ممیزی حقوق دسترسی برای فایل/پوشه. قابلیت نادیده گرفتن ممیزی فایلهای آفیس موقت.
CameraController	1. گرفتن اسنپ شات 2. ضبط ویدیو 3. اتصال زنده به دوربین	قالیت تنظیم تناوب برای گرفتن اسسنپ شاتها، گزینه های متفاوت برای ضبط ویدیو، گیزینه های ویژه برای برنامه های کاربردی، کاربران، آدرس های URL منتخب، قابلیت ذخیره اسنپ شات با حجم مشخص (٪ از حجم اصلی)

ماژول	امکانات	قابلیت ها
Cloud & SharePoint	1. Google Drive, Docs 2. OneDrive 3. SkyDrive 4. Office 365 5. DropBox 6. Evernote 7. Yandex.Disk 8. Cloud.mail.ru 9. Amazon S3 10. iCloud 11. DropMeFiles 12. OwnCloud 13. Pcloud 14. OziBox 15. MediaFire 16. OpenDrive 17. 4shared 18. Box 19. Syncplicity 20. CloudMe 21. MiMedia 22. My-Files 23. SharePoint 24. TeamViewer 25. RealVNC 26. Radmin 27. LiteManager 28. Nextcloud 29. Acronis File Advanced	N/a
FTPController	گرفتن فایل هایی که بر روی پروتکل FTP ارسال می شوند	حداکثر حجم یک فایل دریافت شده، تناوب به روز رسانی، تایم اوتهای فعالیت های اخیر

ماژول	امکانات	قابلیت ها
ProgramController	کنترل زمان صرف شده در برنامه ها و وب سایتها کنترل زمان صرف شده در وب سایتها از طریق مرورگرهای زیر امکان پذیر است: ▪ Internet Explorer (from version 8) ▪ Mozilla Firefox (from version 50.1.0) ▪ Google Chrome (from version 55.0.2883.87) ▪ Yandex Browser (16.11.0.2680) ▪ Opera (Presto) (36.0.2130.80) ▪ Opera (Chromium) ▪ Safari ▪ Tor Browser ▪ Netscape Navigator ▪ Amigo (from version 54.0.2840.189) ▪ Sputnik (from version 2.1.1051.0) ▪ Flock (02.06.2001) ▪ Avant Browser ▪ Lunascape ▪ Maxthon ▪ SeaMonkey ▪ K-Meleon ▪ SlimBrowser ▪ Edge (from version 38.14) ▪ Comodo Dragon (from version 52.15.25.664) ▪ CoolNovo (2.0.9.20) ▪ Cốc Cốc (from version 56.3.150) ▪ Titan Browser (from version 33.0.1712.0 (235591) ▪ Uran (from version 43.0.2357.134)	فیلتر برای کاربران/ گروها و یا پروسه ها. قابلیت نادیده گرفتن فعالیت های سیستمی. قابلیت غیره فعال کردن ممیزی فعالیت ها بر روی وب سایتها
PrintController	4. کنترل چاپ بر روی چاپگرهای محلی 5. کنترل چاپ بر روی چاپگرهای تحت شبکه 6. کنترل چاپ بر روی چاپگرهای مجازی	گزینه های کیفیت (فشرده سازی) برای تصاویر. فیلتر کردن بر اساس کاربران، پروسه ها، شرح، چاپگر و مکان. امکان مسدود سازی عملگرهای **Escape** (کنترل از راه دور چاپگر از طریق عمگرهای Escape)
HTTPController	1. دریافت درخواست های POST 2. دریافت درخواست های GET	محدود سازی بر اساس حداقل حجم درخواست. محدود سازی بر اساس نقاط رهیگیری شده، آدرسهای IP، توع درگاه (SSL/non SSL)، پروسه ها. قابلیت افزودن لیستی از ناشناس ساز ها. قابلیت مسدود کردن SPDY و QUIC. قابلیت نادیده گرفتن انواع MIME (صدا، ویدیو، تصاویر). قابلیت مسدود کردن منابعی که مجاز نیستند.

ماژول	امکانات	قابلیت ها
MonitorController	1. گرفتن اسکرین شات 2. ضبط ویدیویی فعالیت های کاربر 3. اتصال به صفحه یک کاربر در حالت زنده	قابلیت تنظیم تناوب برای گرفتن اسکرین شاتها، تناوب برای گرفتن اسکرین شات از Skype، ویدیو کنفرانس های Lync و برای URLها، گزینه های مخصوص برای برنامه ها، کاربران، تنظیمات رنگ، تنظیمات برای چندین صفحه نمایش منتخب. قابلیت ذخیره یک اسکرین شات با حجم مشخص (٪ از فایل اصلی). قابلیت تنظیم رنگ و مستثنا قرار دادن پس زمینه و تنظیمات فرکانس فریم. قابلیت پیکربندی یک جدول زمانی و حالت عملکرد (برای همه / برای منتخب). قابلیت تنظیم دسترسی برای اتصال توسط کلمه عبور و یا برای کاربران مشخص.
MicrophoneController	1. ضبط صدا با یک میکروفن 2. اتصال به میکروفن کاربر در حالت زنده	قابلیت تخصیص تنظیمات برای پروفایلهای In Office/Out of Office: حداکثر مدت، کاهش نویز، ضبط بدون ورود، فعالسازی خودکار میکروفن خاموش، کیفیت ضبط، تشخیص گفتار، لیست نرم افزار، جدول زمان بندی. قابلیت زمانبدی ضبط. قابلیت تخصیص تنظیمات دسترسی برای اتصال توسط کلمه عبور یا برای کاربران مشخص. فناوری گفتار به متن.
MailController	رهگیری پروتکل های زیر: ▪ IMAP ▪ MAPI ▪ POP3 ▪ SMTP ▪ NNTP ▪ Web mail: ▪ mail.ru ▪ gmail.com ▪ tut.by ▪ yandex.ru ▪ rambler.ru ▪ outlook.com ▪ office 365 ▪ ukr.net ▪ yahoo.com ▪ qip.ru ▪ Google Sync ▪ Etc.	**تنظیمات عمومی:** فیلتر بر اساس فرستنده، دریافت کننده، کاربر دامین، موضوع، پروتکل، حجم، تعداد دریافت کننده ها. **تنظیمات فردی برای وب میل:** قابلیت فعال/غیره فعال کردن رهگیری برای ایمیل های ورودی. مسدود کردن پیامهای ایمیل که از طریق SMTP, MAPI, IMAP تنظیم شده اند بر اساس محتوا و یا محدوده زمینه ای.

ماژول	امکانات	قابلیت ها
IMController	رهگیری پروتکل های زیر: 1. ICQ 2. MMP (mail.ru agent) 3. XMPP (Jabber) 4. Gadu-Gadu 5. Lync (Skype for Business, MS Teams) 6. Viber 7. Telegram 8. WhatsApp 9. HTTPIM as part of: ▪ vk.com ▪ ok.ru ▪ facebook.com ▪ mamba.ru ▪ my.mail.ru ▪ LinkedIn ▪ Evernote ▪ Google+ ▪ Yammer ▪ Fotostrana ▪ Slack.com ▪ Web-Skype ▪ Web-Telegram ▪ Web-WhatsApp ▪ icq.com ▪ Bitrix24 ▪ etc.	رهگیری لیست مخاطبین. دریافت چت ها، تماس ها، فایل ها، مخاطبین، تاریخچه. تنظیمات حداکثر حجم فایل، صدا و مدت. ▪ Lync – Chats, calls, files, contacts ▪ Viber – Chats, calls, files, contacts, history ▪ Telegram – Chats, calls, files, contacts ▪ WhatsApp – Chats ▪ Web Skype – Chats, files ▪ Web Telegram – Chats ▪ Web WhatsApp – Chats تشخیص صوتی (رونوشت گفتار به متن).
SkypeController	دریافت تماس ها، پیامها، فایل ها و SMS از طریق Skype برای دسکتاپ	دریافت چت ها، تماس ها، فایل ها، مخاطبین، sms و تاریخچه پیامها. تاریخچه. تنظیمات حداکثر حجم فایل، صدا و مدت. تشخیص صوتی (رونوشت گفتار به متن).
Workstation Indexing	ردگیری دسترس پذیری، کپی کردن، جا به جایی و حذف داده های حساس بر روی ایستگاه های کاری	فیلتر بر اساس محل، و نوع فایل ها. قابلیت نگهداری از فایل های حذف شده به مدت مشخص برای ذخیره سازی.

ماژول	امکانات	قابلیت ها
DeviceController	a) ممیزی + مسدودسازی دسترسی: 1. USB HID devices (except keyboard and mouse) 2. Printers (USB) 3. Bluetooth adapters (USB) 4. Scanners (USB) 5. Tokens 6. Network adapters (USB) 7. All USB devices (except concentrators) 8. COM ports 9. LPT ports 10. Bluetooth 11. Network adapters 12. Printers 13. IR ports 14. Media devices 15. HID devices (except keyboard and mouse) 16. Keyboard and mouse 17. FireWire 18. Smart cards 19. PDA 20. Tape device 21. Block of folders 22. Block of disks 23. Processes 24. Clipboard 25. Modems (PPP connection) 26. Wi-Fi b) ممیزی + مسدودسازی دسترسی + کپی سایه: 1. USB devices 2. CD/DVD-ROM 3. Cameras/Scanners 4. Floppy disks 5. SCSI 6. Network folders 7. RDP (disks, clipboard) 8. Portable devices of Windows ▪ Android ▪ Apple ▪ Blackberry ▪ Palm ▪ Windows Phone 9. All portable devices	قابلیت های عمومی: ▪ حداکثر حجم فایل های پردازش شده ▪ مستثنا قرار دادن کاربران سیستمی ▪ لیست های سیاه و سفید بر اساس نوع، دستگاه، تولید کننده، شماره سریال، کاربر، کامپیوتر ▪ محدود کردن داده های ارسالی به دستگاه قابلیت ها برای گروه **A** ▪ کاربران/گروه ها ▪ کامپیوترها ▪ دسترسی کامل/بدون دسترسی ▪ فعال/غیره فعال کردن ممیزی ▪ مستثنا قرار دادن کاربران سیستمی قابلیت ها برای گروه **B** قابلیت های شرح داده شده در بالا به همراه: ▪ کپی سایه بر اساس نام فایل، نوع فایل، پروسه، کاربر، کامپیوتر ▪ دسترسی بر اساس نام فایل، نوع فایل، پروسه، کاربر، کامپیوتر ▪ کپی سایه از داده های ذخیره شده بر روی دستگاه

ماژول	امکانات	قابلیت ها
FileAuditor	ردگیری دسترس پذیری، کپی کردن، جا به جایی و حذف داده های حساس بر روی ایستگاه های کاری؛ پویش محلی و تحت شبکه هر دو؛ طبقه بندی، کپی برداری سایه، جزئیات حقوق دسترسی فایل ها.	انواع جستجوی در دسترس: ▪ جستجوی متنی (incl. Stemming) ▪ جستجو با استفاده از Regular expressions ▪ جستوجوی ویژگی (نام فایل، نوع، حجم، محل، غیره تعیین تعداد کپی های سایه ذخیره شده از یک نسخه سند..
Data encryption	رمزنگاری تمامی انواع داده ارسالی به دستگاه های ذخیره ساز USB خارجی با استفاده از یک کلید یکتا (تولید شده توسط کاربر)	رمزنگاری برای کاربران و گروه های منتخب در دسترس است. برای فایل های رمزنگاری شده شما می توانید تنظیمات دسترسی پیکربندی کنید برای: ▪ تمامی کاربران به غیر از افرادی که مشخص کرده اید ▪ فقط کاربران مشخص یک فایل فقط زمانی باز می شود که Agent در دسترس باشد و مجوز باز شدن آن داده شده باشد. تنظیمات لیست سیاه و سفید نیزبرای رمزنگاری در دسترس است. شما می توانید تنظیمات کپی سایه را به طوری پیکربندی کنید که فقط فایل های رمزنگاری شده دریافت شوند.
SSL notifications	اعلان ها برای اقدام های ناموق Agent ها برای به دام اندازی ارتباط	اضافه نمودن خودکار چنین ارتباطاتی در استثناها. فیلتر کردن بر اساس زمان، کامپیوتر، کاربر، پروسه، نوع.
Audit of technical details	ممیزی جزییات فنی از PC با Agent های نصب شده: ▪ نرم افزارهای نصب شده ▪ پیکرندی سخت افزار ▪ کاربر فعال ▪ وصعیت ایجنت و کامپیوتر ▪ فضای خالی بر روی دیسک ▪ فعالیت های اخیر ایجنت ▪ ممیزی داده مدیریت تسک	N/a

2 قابلیت های ماژول های رهگیری EndpointController

در پایین، جدولی از امکانات کنترل کننده شبکه SearchInform آمده است که یا با دریافت داده شبکه با استفاده از فناوری SPAN عمل می کند و یا با ادغام با سرور پراکسی. قابلیت مسدودسازی فقط با ادغام با سرور پراکسی از طریق ICAP موجود است.

ماژول	امکانات	در صورت وجود	قابلیت ها
Cloud & SharePoint	رهگیری سرویس های زیر از طریق رابط وب (عدم استفاده از برنامه!): 1. رهگیری سرویس Google Docs 2. رهگیری سرویس One Drive از MS 3. رهگیری سرویس آفیس 365 (آفیس آنلاین) 4. رهگیری سرویس Drop Box 5. رهگیری سرویس Evernote 6. رهگیری سرویس Yandex.Disk 7. رهگیری سرویس Cloud.mail.ru 8. رهگیری OwnCloud 9. رهگیری MediaFile 10. رهگیری MyFiles.ru 11. رهگیری SharePoint	عملکرد تمام عیار، به عنوان قانون، در ICAP (تمامی ارتباطات رمز شده هستند) یا تعویض گواهی + SPAN (مثلا با ابزاری مانند PaloAlto)	محدود سازی بر اساس درگاه ها، فیلترکردن بر اساس میزبان ها، ارسال کننده، حجم و محتوا امکان مسدود سازی بر اساس ویژگی ها. [1]

[1] Blocking is available only via ICAP scheme, it doesn't work with SPAN.

ماژول	امکانات	در صورت وجود	قابلیت ها
MailController	رهگیری پروتکل های زیر: ▪ IMAP ▪ MAPI (without encryption) ▪ POP3 ▪ SMTP ▪ NNTP ▪ WebMail as part of: ▪ mail.ru ▪ gmail.com ▪ tut.by ▪ yandex.ru ▪ rambler.ru ▪ outlook.com ▪ office 365 ▪ ukr.net ▪ yahoo.com ▪ qip.ru ▪ Google Sync	SPAN – تمامی در دسترس ICAP – فقط وب میل	تنظیمات عمومی: فیلترکردن بر اساس ارسال کننده، گیرنده، کاربر دامین، موضوع، پروتکل، حجم، درگاه. تنظیمات انفرادی برای وب میل: قابلیت فعال/غیره فعال کردن رهگیری پیام های ورودی. قابلیت مسدودسازی وب میل بر اساس ویژگی ها.
HTTPController	دریاف درخواست ها POST دریافت درخواست های GET	SPAN و ICAP هر دو GET برای بعضی از سرورهای پراکسی کار نخواهد کرد[2]	محدودسازی بر اساس حداقل حجم درخواست POST. محدودسازی بر اساس نقاط رهگیری شده، IP، درگاه ها، ارسال کننده، حجم. قابلیت افزودن لیستی از ناشناس ساز ها. شما می توانید مسدودسازی را بر اساس ویژگی ها انجام دهید.
FTPController	دریافت فایل های ارسال شده بر روی FTP	SPAN وICAP هر دو	حداکثر حجم یک فایل دریافت شده، تناوب به روزرسانی، تایم اوت های آخرین فعالیت.
IMController	رهگیری پروتکل های زیر: ▪ ICQ ▪ MMP (mail.ru agent) ▪ XMPP(Jabber) ▪ YAHOO! ▪ HTTPIM as part of: ▪ vk.com ▪ ok.ru ▪ facebook.com ▪ mamba.ru ▪ my.mail.ru ▪ LinkedIn ▪ Evernote ▪ Google+ ▪ Yammer ▪ Fotostrana ▪ Web-Skype ▪ icq.com	SPAN – تمامی در دسترس ICAP – فقط وب میل	محدودسازی بر اساس نقاط دریافت شده، IP، درگاه ها، ارسال کننده، حجم. قابلیت افزودن لیستی از ناشناس ساز ها . قابلیت دریافت هر پروتکل مشخص با استفاده از تونل ساختن HTTP. قابلیت مسدود کردن پیام رسان تحت وب بر اساس ویژگی ها.

[2] The proxy servers listed below operate in full (incoming and outgoing traffic): SQUID, BLUE COAT, MCAFEE, WEBSENSE (ForcePoint), ISA/TMG. The proxy servers mentioned further support only outgoing traffic: FortiGate, Check Point. The list is not full and comprehensive. It contains the proxies tested by the SearchInform experts for compatibility with the SearchInform RM solution.

ماژول	امکانات	در صورت وجود	قابلیت ها
Telephony	دریافت تماس های صوتی پیام های نوشتاری از فناوری SIP از طریق استانداردهای: ▪ GSM ▪ A-Law ▪ u-Law ▪ G.722	فقط SPAN	قابلیت محدودسازی بر اساس درگاه ها، کاربران، کامپیوترها، آدرسهای IP، و آدرسهای .MAC.

3 قابلیت های ادغام NERTWORKCONTROLLER با سرورهای میل، ISA/TMG و LYNC (SKYPE FOR BUSINESS)

ماژول	در صورت موجود	امکانات/قابلیت ها
Lync/Skype for Business	رهگیریه: ▪ Chats ممیزیه: ▪ Calls ▪ Files	در حالت ادغام، فقط پیام ها به خوبی رهگیری می شوند. تماس ها و فایل های ارسالی در ممیزی ثبت خواهند شد، اما محتوای آنها در دسترس نخواهد بود. پیشنهاد می شود برای رهگیری تمام عیار فایل ها و تماس ها از بستر کنترل کننده Endpoint استفاده شود.
ISA/TMG	1. رهگیری درخواست های POST 2. رهگیری درخواست های GET	راهکار به صورت کامل در مورد دریافت داده عمل می کند، اما توان مسدودسازی را به علت خصوصیات خاص معماری TMG ندارد (این پراکسی از ICAP پشتیبانی نمی کند.) به همین علت ما از ماژول جداگانه ای برای ادغام استفاده می کنیم.
Mail servers	1. کنترل میل باکس های سازمانی از طریق POP3 و IMAP 2. کنترل میل باکس های سازمانی از طریق EWS 3. رهگیری SMTP	این روش های ادغام به یک تولید کننده خاص و یا نسخه خاصی از سرورهای میل وابسته نیست (به غیر از EWS). این روش ها عمومی بوده و می توان در Exchange، Lotus، Postfix و حتی چندین سرور میل عمومی نیز استفاده شود.

4 قابلیت های رهگیری EndpointController در لینوکس

ماژول	امکانات	قابلیت ها
Cloud & SharePoint	رهگیری سرویس های زیر که از طریق رابط وب کار می کند. (عدم استفاده از برنامه!). ▪ Google Drive, Docs ▪ OneDrive ▪ SkyDrive ▪ Office 365 ▪ DropBox ▪ Evernote ▪ Yandex.Disk ▪ Cloud.mail.ru ▪ Amazon S3 ▪ iCloud ▪ DropMeFiles ▪ OwnCloud ▪ Pcloud ▪ OziBox ▪ MediaFire ▪ OpenDrive ▪ 4shared ▪ Box ▪ Syncplicity ▪ CloudMe ▪ MiMedia ▪ My-Files ▪ SharePoint	N/a
FTPController	رهگیری فایل های ارسالی بر روی FTP	حداکثر حجم فایل دریافت شده، تناوب به روز رسانی، تایم اوت های آخرین فعالیت.
HTTPController	1. دریافت درخواست های POST 2. دریافت درخواست های GET	محدودسازی بر اساس حداقل حجم درخواست POST. محدودسازی بر اساس نقاط رهگیری شده، آدرس های IP، درگاه ها، نوع (SSL/no SSL)، پروسه ها. قابلیت افزودن لیستی از ناشناس ساز ها. قابلیت مسدودسازی SPYD وQUIC . قابلیت مستثنا کردن انواع MIME (صدا، ویدیو، تصاویر).

ماژول	امکانات	قابلیت ها
MailController	رهگیری این پروتکل ها: ▪ IMAP ▪ MAPI (without encryption) ▪ POP3 ▪ SMTP ▪ NNTP ▪ WebMail as part of: – mail.ru – gmail.com – tut.by – yandex.ru – rambler.ru – outlook.com – office 365 – ukr.net – yahoo.com – qip.ru – Google Sync	تنظیمات عمومی: فیلترکردن بر اساس ارسال کننده، گیرنده، کاربر دامین، موضوع، پروتکل، حجم. تنظیمات انفرادی برای وب میل: قابلیت فعال/غیره فعالسازی رهگیری پیام های ایمیل ورودی.
IMController	رهگیری پروتکل های زیر: 1. ICQ 2. MMP (mail.ru agent) 3. XMPP (Jabber) 4. HTTPIM as part of: ▪ vk.com ▪ ok.ru ▪ facebook.com ▪ mamba.ru ▪ my.mail.ru ▪ LinkedIn ▪ Evernote ▪ Google+ ▪ Yammer ▪ Fotostrana ▪ Web-Skype ▪ webim.ru	رهگیری لیست مخاطبین.
SSL notifications	اعلان های اعلام تلاش های ناموفق ایجنت برای به دام انداختن ارتباط	افزودن خودکار چنین ارتباطت هایی به استثناها. فیلتر کردن بر اساس زمان، PC، کاربر، پروسه و نوع.
DeviceController[3]	ممیزی + قفل دسترسی: ▪ دستگاه های ذخیره سازی USB ▪ پوشه های تحت شبکه	عمومی: ▪ کاربران ▪ کمپیوترها ▪ روشن/خاموش کردن ممیزی ▪ دسترسی کامل/بدون دسترسی ▪ لیست های سیاه و سفید بر اساس نوع، دستگاه ها، تولید کننده، شماره سریال.

[3] Capability to block USB devices and network resources is available only for the following Linux OSs: CentOS (7.6 x64), Ubuntu (16.04 x32/x64, 17.04 x32/x64, 18.04 x64).

5 قابلیت های مسدود سازی در SEARCHINFORM RM

نظارت بر ریسک SearchInform نه تنها ممیزی با جزئیات را بر روی داده های در حال انتقال انجام داده و نسخه های کپی سایه از اسناد می سازد، بلکه امکان مسدود سازی داده در حال انتقال بر روی دامنه وسیعی از کانال های داده می دهد. لیست کانال هایی که می توان کنترال کرد با لیست کانال هایی که می توان مسدود کرد متفاوت است، لذا ما در ادامه با توضیحات مفصلی از قابلیت های مسدود سازی SearchInform RM فراهم کرده ایم.

مسدود سازی می تواند در سطوح مختلفی انجام شود: در هنگام انتقال داده بر روی شبکه، بر روی یک endpoint، و در حال استفاده از سرور میل مشتری.

5.1 مسدود سازی در سطح ایجنت

- مسدود سازی هر دستگاه متصلی بر اساس نوع آن، شماره سریال و ویژگی های دیگرش. برای مثال، مسدود سازی COMT، د رگاه های LPT، چاپگرها، اسکنرها و غیره. اولین جدول در سند لیست کاملی از قابلیت های ماژول DeviceController فراهم آورده.
- مسدود سازی داده های ارسال شده به ذخیره سازها (USB, CD/DVD, SCSI, etc)
- مسدود سازی اجرای نرم افزارها، حتی نسخه های قابل حمل
- مسدود سازی انتقال داده در زمان کار با ریموت دسکتاپ (در طریق دیسک های متصل، پوشه های تحت شبکه و clipboard)
- مسدود سازی بر اساس نوع دستگاه متصل شده (Android, Apple, Blackberry, Palm, Windows Phone, etc.)
- مسدود سازی شبکه های بیسیم و رابط های کاربری (WIFI و BlueTooth)
- مسدود سازی انتقال داده به ذخیره سازهای تحت شبکه (SMB)
- مسدود سازی کار با پوشه های محلی
- مسدود سازی کار با دیسک های محلی
- مسدود سازی منابع وب ممنوع از طریق HTTP(S)

5.2 مسدود سازی در سطح شبکه

سیستم این امکان را می دهد تا ترافیک های شبکه HTTP(S) را بر اساس متن منتقل شده، کاربران منتخب، میزبان ها، URL، POST، GET و خیلی از ویژگی های دیگر مسدود شود. این سبک از مسدود سازی، به غیر از ممنوعیت انتقال یک متن مشخص، این امکان را می دهد تا طرح های امن برای کارکرد با وب میل، چتها، فوروم ها و ذخیره سازهای ابری اجرا کرد. برای مثال، این امکان هست که ارسال یک فایل از شبکه سازمان به یک ذخیره ساز ابری مسدود شود (دانلود همچنان آزاد است). همچنین، این قابلیت هست که پیشنویس ها و پیوست ها در زمان کار با وب میل ذخیره شوند، قابلیت مسدود کردن بارگذاری در شبکه اجتماعی (دیگر عملکردهای شبکه اجتماعی مسدود نشود)، و خیلی از قابلیت های دیگر.

روش	گزینه ها	می تواند شامل
Text		
	All words	Text or regular expression
	Any word	Text or regular expression
	Exact word or phrase	Text or regular expression
	None of the given words	Text or regular expression

Date		
	Equal	Date/month/year
	NE	Date/month/year
	In range	Range of dates/months/years
	Out of range	Range of dates/months/years
Time		
	In range	Hours
	Out of range	Hours
Day of week		
	Equal	Days of week
	NE	Days of week
User		
	Equal	Users
	NE	Users
IP address		
	Local address	Address or range of addresses
	Remote address	Address or range of addresses
HTTP method		
	GET	
	POST	
	CONNECT	
	PUT	
Web field		
	URI	Contains, missing, present, starting with, ending with, equal, NE, in range, out of range, etc.
	HOST	Contains, missing, present, starting with, ending with, equal, NE, in range, out of range, etc.
	USER-AGENT	Contains, missing, present, starting with, ending with, equal, NE, in range, out of range, etc.
	Content-length	Contains, missing, present, starting with, ending with, equal, NE, in range, out of range, etc.

این گزینه با ترافیک رمزنگاری نشده و SSL هر دو، در سطح شبکه وجود دارد. مسدود سازی می تواند بر روی PC و یا هر تجهیزات دیگر شبکه در داخل یک سازمان فارغ از نوع اتصال (اترنت یا WIFI) برای ترافیک HTTP(S) یا FTP(S) اعمال گردد.

با ترکیب این قوانین، شخص می تواند تنظیم دقیق مسدود سازی سرویس ها و یا امکانات بر روی این سرورها داشته باشد. برای مثال،

- The rule (**Web field** = **host** contains **mail.ru**) AND (**Web field URI** contains **attaches/add**) will block the possibility to save or send attachments in *mail.ru* working via web interface.
- The rule (**Web field** = **host** contains **vk.com**) AND (**Web field URI** contains **act=do_add** or **act=add_doc** or **act=album_photo**) will block the possibility to load files to *vk.com*.
- The rule (**Web field** = **URI** contains **/objects**) AND (**Web field host** contains **api.asm.skype.com**) AND (**HTTP method** = **PUT**) will block the possibility to send files over web Skype.

5.3 مسدود سازی ایمیل در سطح ایستگاه کاری و سرور میل (ایجنت)

همچنین، سیستم اجازه مسدود سازی خروج ایمیل های سازمانی بر روی پروتکل های SMTP، MAPI و IMAP را می دهد. این امر از طریق ایجنت مسدود کننده نصب شده بر روی سرور میل مقصد (edge) یا کامپیوتر شخصی محلی با بررسی بیشتر تمامی مکاتبات خروجی انجام می پذیرد. یک پیام ایمیل که سیاست های امنیتی را نقض کرده باشد قبل از بررسی دستی متوقف می شود، بعد از بررسی، نهایتا پیام می تواند مسدود و یا به مقصد ارسال شود. مسدود سازی می تواند به صورت:

- **مفاد**: فرستنده، گیرنده، نوع فایل (بیش از 100 قالب)، حجم، پیوست و خیلی از ویژه گی های دیگر
- **محتوا**: بر اساس وجود داده محرمانه در سندهای منتقل شده. برای مثال، اثر انگشت دیجیتال، عبارات، مترادف ها، اشکال مورفولوژیکی، regular expressions، پیوست های رمزنگاری شده، تصاویر با شباهت بصری به گذرنامه ها، کارت های اعتباری، اسناد حاوی مهر رسمی، اسناد جعل شده.

همچنین این امکان وجود دارد تا منابع که مجاز نیستند بر روی HTTP(S) مسدود شوند.

6 محافظت از داده در حالت ذخیره:

SearchInform RM می تواند داده های محرمانه را در فایل های ذخیره شده برای ذخیره سازهای داده زیر ممیزی و شناسایی کند:

- Local PCs (Windows)
- Roaming user profiles (in Active Directory or Novel eDirectory)
- Network folders (Windows, Linux, Unix, Mac)
- Corporate NAS (Synology, HP, QNAP, etc.)
- Corporate storages SharePoint
- Text fields in popular DBMSs (MS SQL, MySQL, PostgreSQL, Oracle, etc.)
- Databases of web sites
- Web mail
- Cloud storages (Dropbox, Yandex.Disk, OneDrive and CMIS)
- Personal portable storage devices (USB HDD, flash drives) – when connected to corporate equipment.
- Personal mobile devices (telephones, tablets) - when connected to corporate equipment in the file system access mode.

در ادامه، لیست غیره جامعی از قالب هاای ممکن که SearchInform RM می تواند با آنها کار کند آماده است. افرون بر آن، امکان این وجود تا نوع فایل را خودتان بسازید و تجزیه کننده مناسب را به آن اختصاص دهید (پردازش به عنوان باینری، متن، xml، غیره.)

پسوندها	دسته بندی
DOC, DOCX, DOT, DOCM, DOTX, DOTM, XLS, XLSX, XLSB, XLSM, XLTX, XLTM, XLT, PPT, POT, PPTX, PPTM, POTX, POTM, PPSX, PPS, PPSM, RTF, VSD, VST, VSDX, VSSX, VSTX, VSDM, VSSM, VSTM, VDW, VSS	MS Office files
MDB, ACCDB	Databases
HTM, HTML, SHTML, CSS, JS, MAFF	Internet files
MSG, EML, PST	Emails
TXT, CSV, PDF, DJVU, XML, LST, CHM, BAT, LOG, INI, WRI, MHT, HLP	MS Windows programming files
7Z, ARJ, RAR, ZIP, JAR, TAR, ISO, GZ, GZIP, TGZ, TPZ, CAB, LZH, LHA, Z, TAZ, LZMA, BZ2, BZIP2, TBZ2, TBZ, HFS, 001	Archives and compressed files
JAVA, PAS, DFM, DPR, BAS, CPP, HPP, C, C++, H, CS, SQL, JSP, ASP, ASPX, PHP, WSDL, PY, PL, INC, VB, VBS, XLA, CMD, SH	Files of programming languages
SRA, SRJ, SRW, SRU, SRM, SRS, SRF, SRD, SRQ, SRP	PowerBuilder files
MP3, AVI, WAV	Audio/video files
SXW, STW, ODT, ODS	OpenOffice files
DWG, DXF	CAD files
JPG, JPEG, TIF, TIFF, BMP, PNG, GIF	Graphics
LEX, ASC	Old text formats