به نام خدا

سند هدف امنیتی سامانه

نظارت تصویری شیردال

نسخه ۶,۰,۰,۱۵۳۹

شرکت پردازش تصویر کمان

بهمن ماه – ۱۴۰۱

نسخه ۱,۷

فهرست

۱- معرفی سند هدف امنیتی

۱-۱- مرجع سند هدف امنیتی

عنوان سند هدف امنیتی	سند هدف امنیتی سامانه نظارت تصویری شیردال
نسخه	۱,۷
تاریخ	بهمن ماه ۱۴۰۱
نویسندگان	شرکت پردازش تصویر کمان

۱-۲- مرجع هدف ارزیابی

نام تولید کننده (شرکت)	شرکت پردازش تصویر کمان
نام محصول	شیردال
نوع محصول	سامانه نظارت تصویری
نسخه	۶,۰,۰,۱۵۳۹

۱-۳- مرور کلی هدف ارزیابی

۱-۳-۱- توابع امنیتی اصلی هدف ارزیابی

عنوان تابع امنیتی	عملکرد
مدیریت امنیت	سرپرست مجاز قادر به پیکره بندی، نظارت و مدیریت هدف ارزیابی است
ممیزی امنیت	هدف ارزیابی گزارشهایی براساس فعالیت کاربر تولید می کند
احراز هویت	با استفاده از الگوریتم مخصوص و با رعایت موارد ایمنی هویت کاربران احراز می گردد
اضافه کردن دوربین	با توجه به مشخصات دوربین، دوربین بر روی نرم افزار تعریف می شود
ضبط و پخش تصاویر	تصاویر دوربین ها بر اساس نیاز و درخواست کاربر ضبط و پخش می گردد
سطح دسترسی	تعریف سطوح دسترسی مربوط به دوربین ها، کاربران و مواردی که در نرم افزار تعریف شده اند
کنترل دوربین	فرامین لازم برای کنترل و چرخش دوربین های متحرک ایجاد می شود

۱-۳-۲- نوع هدف ارزیابی

نرم افزار نظارت تصویر شیردال یک نرم افزار کلاینت سروری است که براساس پروفایل برنامه کاربردی تحت ویندوزمی باشد.

۳-۳-۱- نرم‌افزار/سخت‌افزار/میان‌افزار پیش نیاز هدف ارزیابی

در جدول زیر سخت‌افزار، نرم افزار و میان افزارهای لازم برای کارکرد محصول بیان شده است:

کامپوننت‌ها	حداقل الزامات
کلاینت شیردال	CPU: Intel Atom RAM: 4GB LAN: 100 Mb/s
سیستم عامل کلاینت	Windows 10 64/bit
سرور شیردال	CPU: Intel Atom RAM: 2GB LAN: 100 Mb/s
سیستم عامل سرور	CentOS: 7.9 64bit
دوربین تحت شبکه	به منظور ارسال و دریافت استریم تصویر
شبکه ارتباطی	10 Mb/s
کتابخانه نرم افزاری	آخرین نسخه بروز شده libcrypto موجود در CentOS 7.9

۴-۱- توصیف هدف ارزیابی

سامانه نظارت تصویری شیردال به منظور مدیریت ضبط ، پخش و کنترل تصاویر دوربین های مداربسته مورد استفاده قرار می گیرد. با بهره گیری از بستر شبکه انتقال تصاویر از دوربین به سرور و همچنین سرور به کلاینت انجام میگیرد.

این سامانه با ساختار سرور/کلاینتی که در آن سرور با سیستم عامل لینوکس و کلاینت با سیستم عامل ویندوز پیکربندی شده است و کاربر با استفاده از کلاینت می تواند وظیفه مدیریت، ضبط و بازبینی تصاویر دوربین ها را انجام دهد.

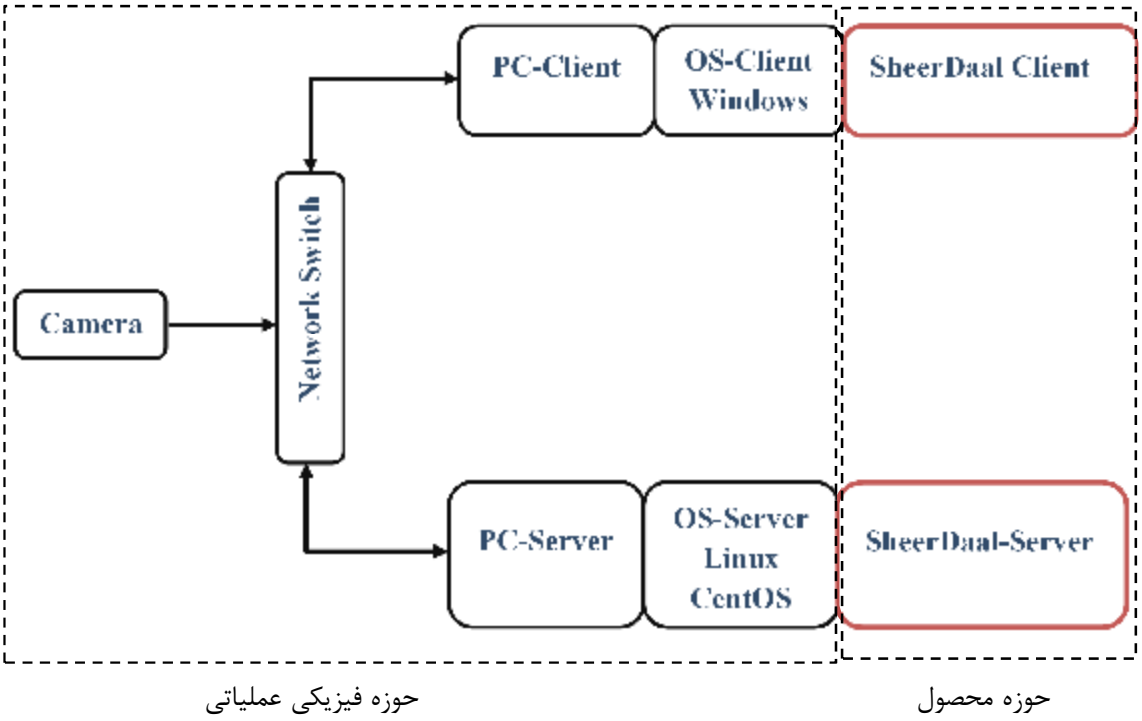
تصاویر با استفاده از پروتکل های رایج TCP یا UDP دریافت می شوند. نرم افزار قابلیت ارتباط با انواع دوربین های مداربسته را داراست. کلاینت شیردال ابزاری برای مدیریت سرور شیردال است. اضافه کردن دوربین روی سرور ، تعریف کاربران و اختصاص سطح دسترسی به هرکدام، تعریف نقشه، مدیریت ضبط و پخش تصاویر، تعریف روال توسط کلاینت انجام می شود. تمامی تنظیمات در سرور ذخیره می شود.

نرم افزار نظارت تصویری شیردال تصاویر دوربین های مداربسته را دریافت کرده و در فضای ذخیره سازی تعریف شده ضبط می نماید.

۱-۴-۱- حوزه فیزیکی

عناصر سخت‌افزاری و نرم‌افزاری مورد استفاده در جدول زیر معرفی می‌شود:

عناصر محصول	شماره مدل یا نسخه
سیستم عامل لینوکس برای سرور شیردال	CentOS 7.9 64bit
سیستم عامل ویندوز برای کلاینت شیردال	Windows 10 64bit
سرور	2 cores CPU
کلاینت	2 cores CPU
شبکه ارتباطی	LAN



شکل ۱: حوزه فیزیکی محصول با تفکیک حوزه محصول و محیط عملیاتی آن

۲-۴-۱- حوزه منطقی

کارکردهای امنیتی هدف ارزیابی تحت عنوان حوزه منطقی شناخته می‌شود که باید به صورت مشخص هریک از کارکردها و شرح آنها در این قسمت مطرح شود.

کارکردها	توصیف
مدیریت امنیت	*هدف ارزیابی سرپرست مجاز را قادر به پیکره بندی، نظارت و مدیریت هدف ارزیابی برای رسیدن اهداف امنیتی می کند. سرپرست مجاز، هدف ارزیابی را از طریق کنسول لینوکس و اتصال تحت شبکه به کمک نرم افزار کلاینت پیکره بندی می کند.*
ممیزی امنیت	*هدف ارزیابی گزارش هایی را بر اساس فعالیت های کاربر تولید می کند.*
احراز هویت	*ابتدا یک درخواست Nonce به سرور ارسال میشود و پس از دریافت آن یک hash اولیه از رمز عبور کاربر ساخته شده و به همراه Nonce یک HMAC_Hash تولید شده و به سرور ارسال میگردد. سرور نیز HMAC_Hash مشابهی را انجام میدهد و در صورت یکسان بودن Hashها هویت کاربر را تایید میکند و برای وی یک Session بصورت Unique ایجاد می‌کند.*
ذخیره‌سازی پروفایل	*سمت کلاینت برای حفاظت از اطلاعات کاربر ابتدا احراز هویت کاربر ویندوز انجام می‌گردد. در صورت تایید یک HMAC_SHA3 از اطلاعات کاربر ویندوز با* الگوریتم تولید شده و به کمک آن اطلاعات هویتی و تنظیمات کاربر با الگوریتم AES رمز شده و ذخیره می‌گردد.
اضافه کردن دوربین	*دوربین با توجه به آدرس IP، نام کاربری، رمز عبور اختصاص یافته و نوع آن توسط شیردال کلاینت بر روی سرور شیردال اضافه می شود.*
ضبط و پخش تصاویر	*تصاویر براساس درخواست کاربر و توسط سرور از دوربین دریافت شده و در فضای ذخیره سازی تعریف شده ضبط می گردد. مدیریت ضبط و پخش تصاویر برای کاربران دارای مجوز انجام می گیرد.*
سطح دسترسی	*سطوح دسترسی اعم از امکان اضافه/حذف کردن دوربین، امکان فعال/غیرفعال سازی ضبط دوربین، امکان تعریف/حذف کاربر، امکان کنترل/عدم کنترل دوربینها، امکان مشاهده مشخصات سخت افزاری سیستم، امکان تغییر در تنظیمات دوربین و مواردی از این دست در کلاینت شیردال قابل انجام است.*
کنترل دوربین	*با استفاده از نرم افزار شیردال کلاینت می توان کنترل حرکت دوربین های متحرک را در اختیار گرفت. این کارکرد بر اساس سطح دسترسی تعریف شده برای کاربر قابل کنترل است.*

۲- ادعای انطباق

۲-۱- انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استاندارد ارزیابی امنیتی معیار	ISO/IEC 15408, version 3.1, revision 5, April 2017

مشترک	
انطباق با SFRها (قسمت دوم از CC)	**توسعه یافته**
انطباق با SARها (قسمت سوم از CC)	**منطبق**

۲-۲- انطباق با پروفایل حفاظتی

نام پروفایل حفاظتی	*این سند هدف امنیتی با پروفایل حفاظتی برنامه کاربردی مهرماه ۹۵ نسخه ۱،۰ و با اصلاحاتی از نسخه ۱,۴ پروفایل حفاظتی برنامه کاربردی NIAP انطباق دارد.*

۲-۳- انطباق با سطح تضمین امنیتی

سطح تضمین امنیتی	EAL1

۳- تعریف مسائل امنیتی

۳-۱- خطمشی

خطمشی	توصیف
هیچ گونه خط مشی امنیتی برای سامانه نظارت تصویری شیردال وجود ندارد.	

۳-۲- تهدیدات

تهدید	توصیف
T.NETWORK_ATTACK	**فرد مهاجم روی یک کانال ارتباطی یا هر جای دیگری از زیرساخت شبکه قرار می‌گیرد. مهاجمان ممکن است سعی در برقراری ارتباط با برنامه کاربردی نمایند یا در ارتباطات میان نرم‌افزار برنامه کاربردی و دیگر نقاط پایانی دست ببرند تا بتوانند به آن نفوذ کنند.**
T.NETWORK_EAVESDROP	**فرد مهاجم روی یک کانال ارتباطی یا هر جای دیگری از زیرساخت شبکه قرار می‌گیرد. مهاجمان ممکن است داده‌های انتقالی بین برنامه کاربردی و دیگر نقاط پایانی را مشاهده کنند یا به آن‌ها**

تهدید	توصیف
	دسترسی یابند.
T.LOCAL_ATTACK	**فرد مهاجم ممکن است از طریق نرم‌افزارهای عادی (نرم‌افزارهایی که امتیاز دسترسی ویژه ندارند) موجود روی پلت‌فرمی که برنامه کاربردی روی آن اجرا می‌شود، وارد عمل شود. مهاجمان ممکن است ورودی‌های آلوده را در قالب فایل یا ارتباطات محلی، وارد برنامه کاربردی کنند.**
T.PHYSICAL_ACCESS	**مهاجم ممکن است به اطلاعات حساس بایگانی‌شده، دسترسی پیدا کند.**

۳-۳- فرضیات

فرضیه	توصیف
A.PLATFORM	اجرای محصول منوط به یک پلتفرم رایانشی قابل‌اعتماد است و شامل پلتفرم زیرین و هرگونه محیط زمان اجرا که پلتفرم برای پلت فرم فراهم کرده است، است.
A.PROPER_USER	کاربر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمی‌زند و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، به کار می‌گیرد.
A.PROPER_ADMIN	راهبر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمی‌زند، بی‌دقت نیست و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، راهبری می‌نماید.

۴- اهداف امنیتی

۱-۴- اهداف امنیتی برای هدف ارزیابی

هدف امنیتی	توصیف
O.INTEGIRITY	محصولات انطباق‌پذیر، صحت نصب خود و بسته‌های به‌روزرسانی را تضمین می‌کنند و همچنین اقدامات اجرایی محیط محور را در جهت کاهش تهدیدات، تسهیل می‌نمایند. نرم‌افزارهای خیلی کمی، اگر نگوییم هیچ، عاری از خطا هستند؛ بنابراین، توانایی نصب بسته‌های تعمیر و عیب‌یابی و به‌روزرسانی نرم‌افزارهای نصب‌شده به‌صورت

هدف امنیتی	توصیف
	منسجم، اقدامی ضروری برای امنیت شبکه‌های سازمانی است. سازندگان پردازشگرها، برنامه‌نویسان کامپایلر، فروشندگان محیط‌های اجرا و فروشندگان سیستم‌عامل‌ها، اقدامات اجرایی محیط‌محوری را در جهت کاهش تهدیدات ایجاد کرده‌اند که با پیچیده‌تر کردن وظایف سیستم‌ها، کار نفوذ به آن‌ها را برای مهاجمان، دشوارتر و پرهزینه‌تر می‌کند. نرم‌افزارهای برنامه کاربردی اغلب می‌توانند از این سازوکارها بهره ببرند. این کار با استفاده از APIهایی انجام می‌شود که در زمان اجرا فراهم‌شده است؛ یا توسط فعال‌سازی این سازوکارها از طریق کامپایلر یا لینکر.
O.QUALITY	برای تضمین کیفیت پیاده‌سازی، محصولات انطباق‌پذیر به‌جای پیاده‌سازی سرویس‌ها و APIهای خود، سرویس‌ها و APIهایی را به کار می‌گیرند که توسط محیط زمان اجرا تأمین‌شده است. اهمیت این کار به‌طور خاص برای سرویس‌های رمزنگاری و دیگر عملیات پیچیده‌ای مثل تجزیه فایل و رسانه، بیشتر است. بهره‌گیری از این قابلیت پلتفرم، فقط منوط به استفاده از APIهای مستند و پشتیبانی شده است.
O.MANAGEMENT	برای تسهیل روند مدیریت توسط کاربران و سازمان، محصولات انطباق‌پذیر، واسط‌های منسجم و پشتیبانی‌شده‌ای را برای نگهداری و پیکربندی امنیتی خود فراهم می‌کنند. این کار شامل پیاده‌سازی و به‌روزرسانی برنامه کاربردی با استفاده از قالب‌ها و سازوکار پیاده‌سازی پشتیبانی شده توسط پلتفرم و همچنین فراهم کردن سازوکاری برای پیکربندی است.
O.PROTECTED_STORAGE	برای جلوگیری از افشای اطلاعات محرمانه‌ی کاربر در نتیجه‌ی حوادثی که منجر به از دست رفتن کنترل فیزیکی ابزارهای ذخیره‌سازی می‌شوند، محصولات انطباق‌پذیر از شیوه‌های حفاظت داده‌های بایگانی‌شده استفاده می‌کنند. این کار شامل رمزگذاری داده‌ها و ذخیره کلیدها توسط محصول است تا از دسترسی غیرمجاز به این داده‌ها جلوگیری شود.
O.PROTECTED_COMMS	برای جلوگیری از حملات تهدیدآمیز فعال (دست‌کاری بسته‌های داده)

هدف امنیتی	توصیف
	و غیرفعال (استراق سمع)، محصولات انطباق‌پذیر از یک کانال مورد اعتماد برای انتقال داده‌های حساس استفاده می‌کنند. داده‌های حساس شامل کلیدهای رمزنگاری، گذرواژه‌ها و هرگونه داده‌های دیگری است که مربوط به برنامه کاربردی بوده و نباید خارج از برنامه کاربردی، در معرض دید باشند.

۲-۴- اهداف امنیتی برای محیط عملیاتی

هدف امنیتی	توصیف
OE.PLATFORM	اجرای محصول متکی به یک پلتفرم رایانشی مورد اعتماد است. این شامل سیستم‌عامل زیرین و هرگونه محیط اجرایی دیگری نیز می‌شود که در اختیار محصول قرارگرفته است.
OE.PROPER_USER	کاربر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمی‌زند و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، به کار می‌گیرد.
OE.PROPER_ADMIN	راهبر برنامه کاربردی بی‌دقت نیست و از روی عمد دست به اشتباه یا خرابکاری نمی‌زند و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، راهبری می‌نماید.

۵- نیازمندی‌های امنیتی

الزامات کارکرد امنیتی زیر مطابق با **پروفایل حفاظتی برنامه کاربردی(مهر۹۵ نسخه ۱)** تهیه شده است.
در سند جاری کلیه عملگرهای انتخاب به صورت زیرخط دار و عملگرهای اختصاص به صورت **بولد** نوشته شده اند و براکت ها نیز برای عملگرها لحاظ شده است.

۵-۱- الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول زیر هستند. در ادامه هر یک از الزامات شرح و بسط داده شده‌اند.

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
۱	پشتیبانی از رمزنگاری	تولید بیت تصادفی ۱	FCS_RBG_EXT.1.1
۲		ذخیره‌سازی اسرار ۱	FCS_STO_EXT.1.1
۳	حفاظت از داده ها	دسترسی به منابع پلتفرم ۱	FDP_DEC_EXT.1.1
۴		دسترسی به منابع پلتفرم ۲	FDP_DEC_EXT.1.2
۵		ارتباطات شبکه‌ای۱	FDP_NET_EXT.1.1
۶		رمزگذاری داده‌های حساس برنامه کاربردی ۱	FDP_DAR_EXT.1.1
۷	محرمانگی	استفاده کاربر از یک سرویس بدون افشاء هویت ۴	FPR_ANO_EXT.1.1
۸	مدیریت امنیت	سازوکار پیکربندی پشتیبان‌شده ۱	FMT_MEC_EXT.1.1
۹		تأمین امنیت با پیکربندی پیش‌فرض۱	FMT_CFG_EXT.1.1
۱۰		تأمین امنیت با پیکربندی پیش‌فرض ۲	FMT_CFG_EXT.1.2
۱۱		کارکرد مدیریتی محصول ۱	FMT_SMF.1.1
۱۲	حفاظت از محصول	استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۱	FPT_API_EXT.1.1
۱۳		قابلیت‌های ضد اکسپلویت ۱	FPT_AEX_EXT.1.1
۱۴		قابلیت‌های ضد اکسپلویت ۲	FPT_AEX_EXT.1.2
۱۵		قابلیت‌های ضد اکسپلویت ۳	FPT_AEX_EXT.1.3
۱۶		قابلیت‌های ضد اکسپلویت ۴	FPT_AEX_EXT.1.4
۱۷		قابلیت‌های ضد اکسپلویت ۵	FPT_AEX_EXT.1.5

شماره المان	نام کلاس	نام المان	تطابق الزام با استاندارد
۱۸		به‌روزرسانی امن ۱	FPT_TUD_EXT.1.1
۱۹		به‌روزرسانی امن ۲	FPT_TUD_EXT.1.2
۲۰		به‌روزرسانی امن ۳	FPT_TUD_EXT.1.3
۲۱		به‌روزرسانی امن ۴	FPT_TUD_EXT.1.4
۲۲		به‌روزرسانی امن ۵	FPT_TUD_EXT.1.5
۲۳		به‌روزرسانی امن ۶	FPT_TUD_EXT.1.6
۲۴		استفاده از کتابخانه‌های شخص ثالث ۱	FPT_LIB_EXT.1.1
۲۵	کانال ها و مسیرهای مورداعتماد	حفاظت از تبادل داده‌ها ۱	FTP_DIT_EXT.1.1
الزامات پیوست			
۳۳		عملیات رمزنگاری – رمزنگاری/رمزگشایی ۱ (۱)	FCS_COP.1.1(1)
۳۴		عملیات رمزنگاری – درهم‌سازی ۱ (۲)	FCS_COP.1.1(2)
۳۷		پروتکل FCS_TLSC_EXT.1.1	FCS_TLSC_EXT.1.1
۳۸	پشتیبانی از رمزنگاری	پروتکل FCS_TLSC_EXT.1.2	FCS_TLSC_EXT.1.2
۳۹		پروتکل FCS_TLSC_EXT.1.3	FCS_TLSC_EXT.1.3
۴۰		پروتکل FCS_TLSC_EXT.3.1	FCS_TLSC_EXT.3.1
۴۱		پروتکل FCS_TLSC_EXT.4.1	FCS_TLSC_EXT.4.1
۴۲		پروتکل FCS_TLSC_EXT.5.1	FCS_TLSC_EXT.5.1
۵۳		الزامات پروتکل X509 (1)	FIA_X509_EXT.1.1
۵۴		الزامات پروتکل X509 (2)	FIA_X509_EXT.1.2
۵۵	شناسایی و احرازهویت	الزامات پروتکل X509 (3)	FIA_X509_EXT.2.1
۵۶		الزامات پروتکل X509 (4)	FIA_X509_EXT.2.2

۱-۱-۵- کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱	**تولید بیت تصادفی ۱ (FCS_RBG_EXT.1.1)**
برنامه‌ی کاربردی برای عملیات رمزنگاری • [باید از عملکرد تولید بیت تصادفی قطعی که توسط پلتفرم ارائه شده است کمک بگیرد.]	
۲	**ذخیره‌سازی اسرار ۱ (FCS_STO_EXT.1.1)**
برنامه‌ی کاربردی در فضای حافظه‌ی غیر فرّار • [باید عملکردی را برای ذخیره امن گذرواژه ها پیاده سازی کند.]	

۲-۱-۵- کلاس حفاظت از داده ها

شماره الزام	نام الزام
۳	**دسترسی به منابع پلت‌فرم ۱ (FDP_DEC_EXT.1.1)**
برنامه کاربردی باید کاربر را از قصد خود برای دسترسی به این منابع، آگاه کند: • [اتصال شبکه]	
۴	**دسترسی به منابع پلت‌فرم ۲ (FDP_DEC_EXT.1.2)**
برنامه کاربردی باید کاربر را از قصد خود برای دسترسی به این منابع، آگاه کند: • [هیچ نوع از منابع اطلاعات حساس]	
۵	**ارتباطات شبکه‌ای۱ (FDP_NET_EXT.1.1)**
برنامه کاربردی باید ارتباطات شبکه ای خود را محدود کند به • [ارتباط کلاینت با سرور • ارتباط سرور با دوربین • ارتباط سرور با سیستم ذخیره سازی در صورت وجود	

شماره الزام	نام الزام
	• ارتباط کلاینت با دوربین]
۶	**رمزگذاری داده‌های حساس برنامه کاربردی ۱ (FDP_DAR_EXT.1.1)**
برنامه کاربردی باید • [از عملکرد ارائه‌شده توسط پلت‌فرم برای رمزگذاری داده‌های حساس استفاده کند.]	

۳-۱-۵- کلاس محرمانگی

شماره الزام	نام الزام
۷	**استفاده کاربر از یک سرویس بدون افشاء هویت ۴ (FPR_ANO_EXT.1.1)**
برنامه کاربردی باید • [اطلاعات شناسایی شخصی(PII) در شبکه انتقال ندهد.]	

۴-۱-۵- کلاس مدیریت امنیت

شماره الزام	نام الزام
۸	**سازوکار پیکربندی پشتیبان‌شده ۱**
برنامه کاربردی باید سازوکار توصیه‌شده توسط تولیدکننده‌ی پلتفرم را برای ذخیره‌سازی و تنظیم گزینه‌های پیکربندی، استفاده نماید.	
۹	**تأمین امنیت با پیکربندی پیش‌فرض ۱**
هنگامی که برنامه کاربردی بدون اعتبارنامه یا با اعتبارنامه پیش‌فرض پیکربندی‌شده است، برنامه کاربردی باید اقدامات لازم برای ایجاد اعتبارنامه جدید را فراهم آورد.	
۱۰	**تأمین امنیت با پیکربندی پیش‌فرض ۲**
برنامه کاربردی باید به‌طور پیش‌فرض طوری پیکربندی شود که با قرار دادن مجوزهای دسترسی به فایل مناسب،	

شماره الزام	نام الزام
خود برنامه کاربردی و داده‌های آن را از دسترسی‌های غیرمجاز محافظت کند.	
۱۱	**کارکرد مدیریتی محصول ۱ (FMT_SMF.1.1)**
محصول باید قابلیت اجرای کارکردهای امنیتی زیر را داشته باشد: • [فعال‌سازی/ غیر فعال‌سازی تبادل هرگونه اطلاعاتی که سخت‌افزار، نرم‌افزار یا پیکربندی سیستم را توصیف می‌کند.]	

۵-۱-۵- کلاس حفاظت از محصول

شماره الزام	نام الزام
۱۲	**استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۱**
برنامه کاربردی باید تنها از واسط برنامه‌نویسی کاربردی‌های (API) پلتفرم پشتیبانی شده استفاده کند.	
۱۳	**قابلیت‌های ضد اکسپلویت ۱ (FPT_AEX_EXT.1.1)**
برنامه کاربردی جز برای [هیچ مورد استثنا] نباید درخواست نگاشت حافظه به آدرس مشخصی نماید.	
۱۴	**قابلیت‌های ضد اکسپلویت ۲ (FPT_AEX_EXT.1.2)**
برنامه کاربردی باید • [هیچ بخشی از حافظه را هم زمان هم به نوشتن اطلاعات و هم اجرای مجوزها اختصاص ندهد.]	
۱۵	**قابلیت‌های ضد اکسپلویت ۳**
برنامه کاربردی باید با امکانات امنیتی که توسط تولیدکننده‌ی پلتفرم ارائه‌شده است، سازگار باشد.	
۱۶	**قابلیت‌های ضد اکسپلویت ۴**
برنامه کاربردی نباید فایل‌هایی را که توسط کاربر قابل‌تغییر هستند در دایرکتوری‌هایی بنویسد که حاوی فایل‌های اجرایی‌اند، مگر این‌که کاربر به‌طور مستقیم چنین دایرکتوری‌ها را انتخاب نماید.	
۱۷	**قابلیت‌های ضد اکسپلویت ۵**
برنامه کاربردی باید با قابلیت محافظت از سرریز بافر مبتنی بر پشته کامپایل شود.	
۱۸	**به روز رسانی امن ۱ (FPT_TUD_EXT.1.1)**
برنامه کاربردی باید [این قابلیت را ارائه کند] که به روزرسانی ها و وصله های برنامه های کاربردی را بررسی نماید.	

شماره الزام	نام الزام
۱۹	**به‌روزرسانی امن ۲**
برنامه کاربردی باید با استفاده از قالب مدیریت بسته که توسط آن پلتفرم پشتیبانی می‌شود، توزیع و منتشر شود.	
۲۰	**به‌روزرسانی امن ۳**
برنامه کاربردی باید طوری بسته‌بندی شود که حذف آن، منجر به پاک شدن تمامی آثار برنامه کاربردی شود؛ به‌استثناء تنظیمات پیکربندی، فایل‌های خروجی و ثبت وقایع/ ممیزی.	
۲۱	**به‌روزرسانی امن ۴**
برنامه کاربردی نباید کد باینری خود را دانلود، اصلاح، جایگزین یا به روزرسانی کند.	
۲۲	**به روز رسانی امن ۵ (FPT_TUD_EXT.1.5)**
برنامه کاربردی باید [این قابلیت را برای پلتفرم فراهم نماید] تا نسخه فعلی برنامه کاربردی را بازیابی کند.	
۲۳	**به‌روزرسانی امن ۶**
بسته‌ی نصب برنامه کاربردی و نسخه‌های به‌روزرسانی آن باید به‌طور دیجیتالی امضا شوند به‌طوری‌که پلتفرم بتواند رمزنگاری آنان را قبل از نصب برنامه کاربردی، چک کند.	
۲۴	**استفاده از کتابخانه‌های شخص ثالث ۱** (FPT_LIB_EXT.1.1)
هدف از این الزام آن است که ارزیاب، کتابخانه‌های شخص ثالث غیرضروری یا پیش‌بینی‌نشده در برنامه کاربردی را تشخیص و ثبت نماید. این شامل کتابخانه‌هایی که جهت امور تبلیغاتی ایجادشده‌اند نیز می‌شود که می‌تواند تهدیدی برای حریم خصوصی به شمار رود. همچنین شامل تضمین مستندسازی این کتابخانه‌ها برای مواقعی که آسیب‌پذیری‌هایی در آینده کشف شوند نیز است.	

۶-۱-۵- کلاس کانال ها و مسیرهای مورداعتماد

شماره الزام	نام الزام
۲۵	**حفاظت از تبادل داده‌ها ۱ (FTP_DIT_EXT.1.1)**
برنامه کاربردی باید بین خود و دیگر محصولات مورد اعتماد IT • [تمامی داده های حساس مورد تبادل را با استفاده از حداقل یکی از این [پروتکل TLS] رمزنگاری کند.]	

۷-۱-۵- الزامات پیوست

شماره الزام	نام الزام

شماره الزام	نام الزام
۳۳	**عملیات رمزنگاری – رمزنگاری/رمزگشایی ۱ (۱)**(FCS_COP.1.1(2))
برنامه کاربردی باید رمزنگاری/رمزگشایی را مطابق با الگوریتم‌های رمزنگاری زیر انجام دهد:] • AES-CBC mode (به صورتی که در NIST SP 800-38A تعریف‌شده)، • و هیچ مد دیگر] و اندازه کلید رمزنگاری ۱۲۸ بیت و [۲۵۶ بیت]	
۳۴	**عملیات رمزنگاری – درهم‌سازی ۱ (۲)**(FCS_COP.1.1(1))
برنامه کاربردی باید خدمات درهم‌سازی رمزنگاری را مطابق با الگوریتم درهم‌سازی SHA-1 و [SHA-256،SHA-384، SHA-512] و اندازه چکیده پیام ۱۶۰ و[۲۵۶، ۳۸۴، ۵۱۲] بیت انجام دهد که استاندارد FIPS Pub 180-4 را برآورده می‌نماید	
۳۷	**پروتکل (FCS_TLSC_EXT.1.1)**
برنامه کاربردی باید از TLS 1.2 و [هیچ نسخه TLS قدیمی] پشتیبانی نمایدو همچنین از مجموعه رمز اختیاری] TLS_RSA_WITH_AES_128_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5246، TLS_RSA_WITH_AES_256_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5246، TLS_RSA_WITH_AES_256_CBC_SHA384 به‌صورت تعریف‌شده در RFC 5288، TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5246، TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5246، TLS_DHE_RSA_WITH_AES_256_CBC_SHA384 به‌صورت تعریف‌شده در RFC 5288، TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5289، TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 به‌صورت تعریف‌شده در RFC 5289، TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 به‌صورت تعریف‌شده در RFC 5289، TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 به‌صورت تعریف‌شده در RFC 5289، TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5289، TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 به‌صورت تعریف‌شده در RFC 5289، TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 به‌صورت تعریف‌شده در RFC 5289، TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 به‌صورت تعریف‌شده در RFC 5289] وهمچنین از قابلیت [تجدید نشست] پشتیبانی نماید.	

شماره الزام	نام الزام
38	**پروتکل (FCS_TLSC_EXT.1.2)**
برنامه کاربردی باید منطبق بودن شناسه ارائه شده با شناسه مرجع را بر طبق ۶۱۲۵ RFC وارسی نماید.	
39	**پروتکل (FCS_TLSC_EXT.1.3)**
برنامه کاربردی در صورت معتبر نبودن گواهی همتا، نباید هیچ کانال امنی برقرار نماید [مگر در صورت تایید کاربر معتبر].	
40	**پروتکل (FCS_TLSC_EXT.3.1)**
برنامه کاربردی باید از افزونه signature_algorithms در مرحله Hello کلاینت از الگوریتم های هش [SHA256، SHA384 و SHA512] و هیچ الگوریتم هش دیگری پشتیبانی نماید.	
41	**پروتکل (FCS_TLSC_EXT.4.1)**
برنامه کاربردی باید از تجدید نشست امن از طریق استفاده از افزونه TLS "renegotiation_info" منطبق با RFC5746 پشتیبانی نماید.	
42	**پروتکل (FCS_TLSC_EXT.5.1)**
برنامه کاربردی باید از افزونه گروه های پشتیبانی شده در مرحله Hello کلاینت [secp256r1 ، secp521r1 ، secp384r1] پشتیبانی نماید.	
53	الزامات پروتکل **X509(1) (FIA_X509_EXT.1.1)**
برنامه کاربردی باید [کارکرد ارائه شده توسط پلتفرم را درخواست نماید] تا مطابق با قوانین زیر، گواهی‌ها را معتبر نماید: • اعتبارسنجی گواهی و مسیر گواهی RFC 5280 • مسیر گواهی باید با یک گواهی CA امن خاتمه یابد. • برنامه کاربردی باید مسیر گواهی را اعتبارسنجی نماید با تضمین نمودن وجود آیتمbasicConstraints و اینکه پرچم CA برای تمامی گواهی‌نامه‌ها وضعیت TRUE داشته باشد. • برنامه کاربردی باید وضعیت لغو گواهی را با استفاده از [پروتکل وضعیت گواهی آنالینOCSP به صورت	

شماره الزام	نام الزام
مشخص شده در RFC 2560] استعلام نماید. • برنامه کاربردی باید فیلد extendedKeyUsage را مطابق با قوانین زیر اعتبارسنجی نماید: ○ گواهی استفاده شده برای به روزرسانی امن و بررسی صحت کد اجرایی باید در فیلد extendedKeyUsage دارای هدف Signing Code باشد (id-kp3 با OID 1.3.6.1.5.5.7.3.3) ○ گواهی‌های سرور ارائه شده برای TLS باید در فیلد extendedKeyUsage دارای هدف احراز هویت سرور باشد (id-kp1 با OID 1.3.6.1.5.5.7.3.1) ○ گواهی‌های کالینت ارائه شده برای TLS باید در فیلد extendedKeyUsage دارای هدف احراز هویت کالینت باشد (id-kp2 با OID 1.3.6.1.5.5.7.3.2) ○ گواهی های S/MIME ارائه شده برای امضاء و رمزنگاری ایمیل باید در فیلد extendedKeyUsage دارای هدف حفاظت از ایمیل باشد (id-kp4 با OID 1.3.6.1.5.5.7.3.4) ○ گواهی‌های OCSP ارائه شده برای پاسخهای OCSP باید در فیلد extendedKeyUsage دارای هدف امضای OCSP باشد (id-kp9 با OID 1.3.6.1.5.5.7.3.9) ○ گواهی‌های سرور ارائه شده برای EST باید در فیلد extendedKeyUsage دارای هدف مرکز ثبت گواهی CMC باشد (id-kp-cmcRA با OID 1.3.6.1.5.5.7.3.28)	
54	الزامات پروتکل **X509(2) (FIA_X509_EXT.1.2)**
برنامه کاربردی باید در صورت وجود basicConstraints extension و true بودن CA Flag ،گواهی را به عنوان گواهی CA تلقی نماید.	
55	الزامات پروتکل **X509(3) (FIA_X509_EXT.2.1)**
برنامه کاربردی باید از گواهی X.509v3 به‌صورت تعریف شده توسط RFC ۵۲۸۰ استفاده نماید تا از احراز هویت برای [TLS] پشتیبانی نماید.	
56	الزامات پروتکل **X509(4) (FIA_X509_EXT.2.2)**
زمانی که برنامه کاربردی نمی‌تواند جهت تعیین اعتبار گواهی، اتصالی را برقرار نماید؛ برنامه کاربردی باید [پذیرش گواهی در این مورد به سرپرست داده می‌شود].	

۲-۵- الزامات تضمین امنیتی

الزامات عملکرد تضمین توصیف کننده چگونگی ارزیابی هدف ارزیابی است. در این بخش الزامات EAL1 آورده می-شود که لیست الزامات آن در جدول زیر آمده است.

نام کلاس	نام مؤلفه	توضیحات
Development	**ADV_FSP.1**	مشخصات کارکرد ابتدایی
Guidance Documents	**AGD_OPE.1**	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Tests	**ATE_IND.1**	آزمون مستقل-منطبق
Vulnerability Assessment	**AVA_VAN.1**	تحلیل آسیب‌پذیری
Life cycle Support	**ALC_CMC.1**	برچسب گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول

۶- خلاصه مشخصات هدف ارزیابی

۶-۱- پشتیبانی از رمزنگاری

محصول مورد ارزیابی از عملکرد تولید بیت تصادفی که توسط پلتفرم صورت می گیرد استفاده می کند. همچنین از الگوریتم رمزنگاری تایید شده AES برای ذخیره امن گذرواژه ها و تنظیمات پیکربندی استفاده می کند. از توابع تصادفی دلفی (Random و Randomize) در تولید نشست استفاده می شود.

FCS_RBG_EXT.1.1
FCS_STO_EXT.1.1

۶-۲- حفاظت از داده ها

محصول مورد ارزیابی کاربر را از قصد خود برای دسترسی به شبکه آگاه می سازد. به هنگام Log in کردن وضعیت اتصال به شبکه نمایش داده می شود. همچنین همواره وضعیت ارتباط شیردال کلاینت به سرور سامانه نظارت تصویری شیردال قابل مشاهده است.

محصول مورد ارزیابی به هیچ یک از منابع اطلاعات حساس دسترسی ندارد.

ارتباطات شبکه ای سامانه نظارت تصویری شیردال به ارتباط کلاینت با سرور، ارتباط سرور با دوربین، ارتباط سرور با سیستم ذخیره سازی و ارتباط کلاینت با دوربین محدود شده است.

محصول مورد ارزیابی از رمزنگاری تائید شده AES استفاده می کند . سامانه شیردال برای ذخیره سازی اطلاعات

کاربران، اطلاعات سرور، اطلاعات دوربین ها، اطلاعات نقشه، اطلاعات فضای ذخیره سازی، اطلاعات روال ها، اطلاعات فضای کاری و اطلاعات زمانبندی ازالگوریتم AES استفاده می کند.
ماژولهای رمزنگاری تائید شده AES که در محصول پیاده سازی شده است، با تمام بخشهای سطح یک امنیتی تطابق داشته و با واسطها و پورتهای ماژول رمزنگاری، قوانین، خدمات و احراز هویت و تضمین طراحی موجود در سطح دو امنیتی نیز تطابق دارد.
برای رمزگذاری داده های حساس از الگوریتم AES با کلیدهای ۱۲۸ بیت یا بزرگتر استفاده شده است.

FDP_DEC_EXT.1.1
FDP_DEC_EXT.1.2
FDP_NET_EXT.1.1
FDP_DAR_EXT.1.1

۳-۶- محرمانگی

سامانه نظارت تصویری شیردال اطلاعات کاربر را در شبکه ارسال نمی کند.

FPR_ANO_EXT.1.1

۴-۶- مدیریت امنیت

در سامانه نظارت تصویری شیردال از سازوکار لینوکس برای نصب و تنظیم پیکربندی مورد نیاز استفاده می شود.
همچنین امکان تغییر و اصلاح رمز عبور و نام کاربری کاربران برای کاربران که مجوز دارند فراهم شده است.
در صورت تنظیم رمز عبور مناسب برای سیستم لینوکس و ویندوز از دسترسی غیر مجاز به برنامه کاربردی و داده های آن محافظت می شود
در سامانه نظارت تصویری شیردال می توان با تنظیم دسترسی برای کاربران مختلف امکان مشاهده مشخصات سخت افزار، نرم افزار و پیکربندی سیستم را محدود کرد.
طبق الزام سامانه برای نگهداری اطلاعات پیکربندی کلاینت باید از ساختار پلتفرم که رجیستری است استفاده نماید اما در سامانه شیردال با توجه به اینکه اطلاعات کاربر به صورت رمز شده ذخیره می شود و اینکار سطح امنیتی بالاتری نسبت به ذخیره سازی در رجیستری دارد، اطلاعات پیکربندی نیز در کنار اطلاعات کاربر و به صورت رمز شده ذخیره می گردد.

FMT_MEC_EXT.1.1

FMT_CFG_EXT.1.1
FMT_CFG_EXT.1.2
FMT_SMF.1.1

۵-۶- حفاظت از محصول

سامانه نظارت تصویری شیردال با امکانات امنیتی سیستم عامل ویندوز و لینوکس سازگار است و همچنین می تواند براساس قالب مدیریت بسته ای که توسط آنها پشتیبانی می شود توزیع و منتشر شود.

این سامانه نمی تواند کد باینری خود را دانلود و اصلاح ، جایگزین و یا به روزرسانی کند.

قابلیت بروزرسانی خودکار سرور/کلاینت در این سامانه وجود ندارد.

فرایند بروزرسانی به صورت offlineانجام می گیرد که بدین شرح است:

۱- ارسال فایل بروزرسانی کلاینت/سرور برای ادمین توسط شرکت کمان

۲- کپی فایل بروزرسانی در سرور توسط ادمین

۳- اجرای فایل بروزرسانی در کلاینت توسط ادمین

در سامانه نظارت تصویری شیردال از کتابخانه های FFMPEG و Live555 به عنوان کتابخانه های شخص ثالث استفاده شده است.

از کتابخانه Live555 متن باز برای دریافت تصویر دوربین با پروتکل RTSP استفاده شده است که در فایل کتابخانه libOpenRTSP.dll کامپایل شده است.

از کتابخانه FFMPEG متن باز برای encode/decode تصاویر دریافتی از دوربین ها استفاده می شود که شامل فایل های زیر است:

- avcodec-58.dll
- avformat-58.dll
- avutil-56.dll
- swresample-3.dll
- swscale-5.dll

FPT_API_EXT.1.1
FPT_AEX_EXT.1.1
FPT_AEX_EXT.1.2
FPT_AEX_EXT.1.3

FPT_AEX_EXT.1.4
FPT_AEX_EXT.1.5
FPT_TUD_EXT.1.1
FPT_TUD_EXT.1.2
FPT_TUD_EXT.1.3
FPT_TUD_EXT.1.4
FPT_TUD_EXT.1.5
FPT_TUD_EXT.1.6
FPT_LIB_EXT.1.1

۶-۶- کانال ها و مسیرهای مورد اعتماد

سامانه نظارت تصویری شیردال از پروتکل TLS 1.2 ارائه شده توسط کتابخانه openssl 1.0.2 مربوط به پلتفرم برای ارتباط بین سرور و کلاینت استفاده می شود که شامل فایلهای زیر است:

- ssleay32.dll
- libeay32.dll

ابتدا ادمین باید کلیدها و گواهی ها را جداگانه تولید کرده و در شاخه اصلی شیردال سرور کپی نماید. سامانه برای ارتباط بین کلاینت و سرور با توجه به این گواهی و کلید پروتکل TLS را اجرا می کند.

FTP_DIT_EXT.1.1