عنوان پروژه	طراحی و توسعهٔ سامانهٔ شناسایی تهدیدات نوین سایبری مبتنی بر SIEM
پژوهشکده	امنیت
گروه	فناوری امنیت شبکه
تاریخ	۱۴۰۳/۲/۲۲

۱ مقدمه (شامل انگیزه تعریف پروژه و سوابق آن):

SIEM[1]های سنتی لاگ‌ها و رویدادهای سامانه‌های مختلف امنیتی و غیر امنیتی در سطح کارگزار و مشتری را جمع‌آوری و پردازش نموده و امکان تعیین آستانه برای ویژگی‌های مختلف رویدادهای امنیتی و در نتیجه تولید هشدار را فراهم می‌کنند. این سامانه‌ها محیط متمرکزی برای کارشناسان مراکز امنیت فراهم می‌کنند تا ایشان بتوانند ضمن مشاهدهٔ رویدادهای امنیتی، آنها را تجزیه و تحلیل نموده و حوادث امنیتی را شناسایی و پیگیری نمایند. با وجود اینکه سامانه‌های SIEM از ضروری‌ترین سامانه‌های مراکز امنیت هستند، به تاکید اکثر کارشناسان امنیت، در نوع سنتی این سامانه‌ها کارایی چندانی ندارند و عملا کمک ناچیزی در شناسایی تهدیدات سایبری و پاسخ‌دهی به حوادث امنیتی ایفا می‌کنند. برخی دلایل این امر موارد زیر هستند:

- حجم بالای لاگ‌های ورودی
- پیچیدگی عملیات تشخیص تهدید و نیاز به کارشناسان خبره جهت تحلیل رویدادها
- عملکرد صرفا مبتنی بر قانون[2] و عدم استفاده از هوش مصنوعی و یادگیری ماشین
- عدم تشخیص بر اساس سناریو و تشخیص بر اساس تک رویدادها
  - به ظاهر نرمال بودن تک‌رویدادها ← لزوم حرکت به سمت تشخیص بر اساس سناریو
  - عملکرد بسیار ضعیف در تشخیص تهدیدات خصوصا تهدیدات نوین سایبری و روز صفر
  - ناتوانی در کمک به پاسخ‌دهی به حادثه
- عدم کارایی کافی در تشخیص، بررسی و پاسخ به تهدید و حادثه
- مقیاس‌پذیر نبودن

جهت شناسایی تهدیدات نوین سایبری، ناگزیر باید از راه‌حل‌های هوش تهدید استفاده نمود. مطابق با تعریف گارتنر[3] هوش تهدید دانشی است مبتنی بر شواهد (شواهدی از قبیل زمینه، مکانیزم، شاخص‌ها، پیامدها و توصیه‌های عملی) درباره یک تهدید یا خطر موجود یا در حال ظهور برای دارایی‌ها، که می‌تواند برای اطلاع‌رسانی تصمیم‌گیری

[1] SIEM, Security Information and Event Managment
[2] Rule Based
[3] https://www.gartner.com/doc/2487216/definition-threat-intelligence

در مورد واکنش به آن تهدید یا خطر استفاده شود. این مفهوم هوش عملی[4] است. در واقع به هرگونه هوش که بتواند به اقدامات واقعی منتقل شود و برای راه‌اندازی یک اقدام پیشگیرانه یا تهیه یک استراتژی متقابل استفاده شود هوش عملی گفته می‌شود.

چارچوب MITRE ATT&CK در سال ۲۰۱۳ میلادی متولد شد. چارچوب MITRE ATT&CK به عنوان یک پایگاه دانش مدیریت‌شده و مشترک جهانی از تاکتیک‌ها، تکنیک‌ها و رویه‌های متخاصم، یک طبقه‌بندی مشترک از حملات و دفاع‌ها برای مدل‌سازی بهتر تهدید، هوش تهدید سایبری، شبیه‌سازی خصمانه و غیره ارائه می‌دهد. در سطح بالا، ATT&CK یک مدل رفتاری است که شامل تاکتیک‌ها، تکنیک‌ها، استفاده دشمنان از تکنیک‌ها و رویه‌های آن‌ها و کاهش‌های مرتبط است.

۱-۱ تجمیع SIEM سنتی با هوش تهدید

محصولات SIEM ارائه شده قابلیت‌های SIEM سنتی را دارا هستند و علاوه بر آن، قابلیت‌های اضافه‌ای نیز در اختیار کاربران قرار می‌دهند. بر اساس دانش ما که حاصل از مطالعهٔ سامانه‌های فوق و نیز بهره‌گیری از مشاوران خبره در حوزهٔ امنیت سایبری است، محصولات انگشت‌شمار SIEMای وجود دارند که شناسایی تهدیدات سایبری را تا حدی پشتیبانی می‌کنند که همهٔ این محصولات تجاری هستند و قیمت‌های کلانی دارند. ارائه دهندگان خدمات داخلی مراکز امنیت نیز از نسخه‌هایی (احتمالا کرک شده) از این سامانه‌های تجاری استفاده کرده و آن را در سازمان مشتریان خود راه‌اندازی می‌کنند. بنابراین تجمیع SIEM با هوش تهدید یکی از زمینه‌های مهم پژوهش روز در زمینهٔ امنیت سایبری است و با توجه به تجمیع کلیهٔ لاگها در SIEM و در دسترس نبودن سامانهٔ بومی مشابه، توسعه و بومی‌سازی سامانهٔ داخلی بسیار مورد نیاز کشور است.

جهت شناسایی تهدیدات نوین سایبری بر اساس SIEM، ناگزیر باید این سامانه‌ها را با هوش تهدید تجمیع نمود. با افزودن قابلیت استفاده از هوش تهدید، سامانه‌های SIEM می‌توانند سناریوهای تهدیدات را استخراج نموده و

[4] Actionable Intelligence

با دریافت iocها به صورت بروز تهدیدات سایبری را شناسایی نمایند. از مهم‌ترین قابلیت‌هایی که هوش تهدید فراهم می‌کند این است که ضمن شناسایی تهدیدات، اطلاعات دقیق و جامعی از تهدید در اختیار کارشناسان و مدیران امنیتی قرار می‌دهد. بخش مهمی از این اطلاعات که به هوش عملی معروف است شامل اطلاعات مهمی از جمله روش مقابله با و پاسخ دهی به تهدید و حادثه است.

۱-۲ شرح سامانهٔ شناسایی تهدیدات نوین سایبری مبتنی بر SIEM

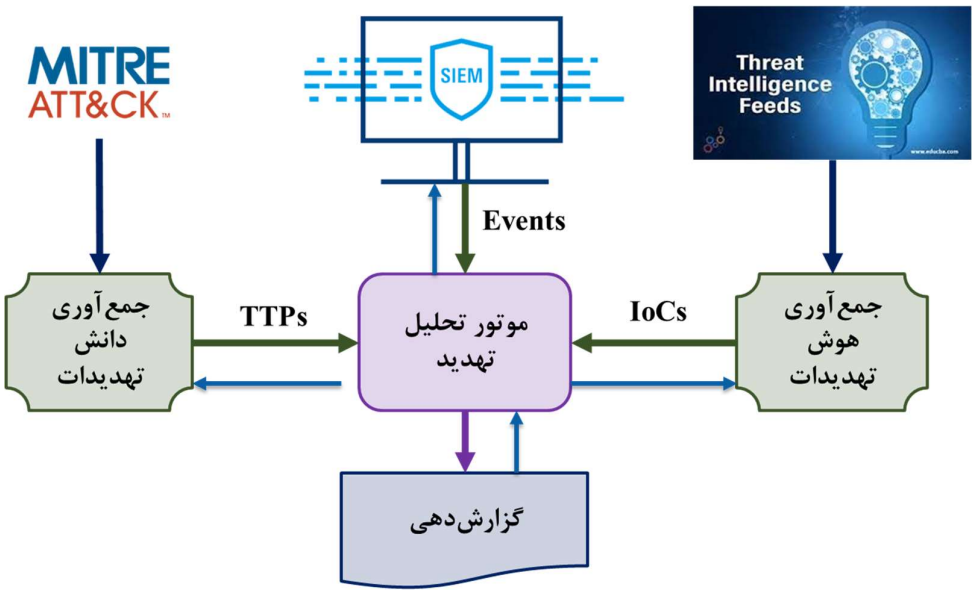
سامانهٔ شناسایی تهدیدات نوین سایبری مبتنی بر SIEM، در واقع، قابلیت شناسایی تهدیدات نوین سایبری را به یک سامانهٔ SIEM سنتی اضافه می‌کند. با توجه به اینکه شناسایی تهدیدات سایبری با بهره‌برداری از هوش تهدید امکان‌پذیر است، سامانهٔ تشخیص تهدیدات نوین سایبری مبتنی بر SIEM سامانه‌ایست که راه‌حل‌های هوش تهدید را با SIEM تجمیع می‌کند.

از مهم‌ترین ویژگی‌های این سامانه می‌توان به موارد زیر اشاره نمود:

- جمع‌آوری لاگ‌های مورد نیاز جهت تشخیص تهدیدات (با کمک SIEM) و تولید رویدادهای مربوطه
- جمع‌آوری هوش تهدید (IoCها) به صورت بروز از بسترهای هوش تهدید معروف
- استخراج سناریوی تهدیدات روز از پایگاه حملات Mitre و ایجاد پایگاه دانش تهدیدات سایبری
- استخراج سناریوهای تهدید بر اساس چند تهدید مهم
- تجمیع رویدادهای SIEM با هوش تهدید بروز
- تشخیص تهدیدات یا حوادث (در محدودهٔ تهدیدات مشخص شده)
- ارائه راهکار جهت پاسخ‌دهی به حوادث یا تهدیدات تشخیص داده شده
- نمایش تهدیدات تشخیص داده شده و اطلاعات در داشبورد و تولید فایل STIX مربوطه
- امکان جستجو و گزارش‌گیری

شکل ۱ به صورت انتزاعی، مولفه‌های مفهومی و جریان دادهٔ سامانه را نشان می‌دهد. جهت شناسایی تهدیدات سایبری مبتنی بر SIEM باید پایگاه دانش سناریوهای حملات و تهدیدها ایجاد گردد. برای این منظور باید TTPهای تهدیدهای مورد نظر از پایگاه دانش حملات MITRE استخراج گردیده و در پایگاه دانش ذخیره گردد. همچنین، باید

خوراک هوش تهدید از پلتفرم‌های هوش تهدید مختلف جمع‌آوری و تجمیع شده و در قالب IoC در اختیار موتور تحلیل تهدید قرار بگیرد. موتور تحلیل تهدید رویدادهای تولید شده توسط SIEM را بر اساس TTPها و هوش تهدید در دسترس مورد تجزیه و تحلیل قرار داده و تهدیدات را شناسایی می‌نماید.



شکل ۱- نمودار جریان داده سامانهٔ شناسایی تهدیدات نوین سایبری مبتنی بر SIEM

۲ هدف پروژه

- ارائه طرح سامانهٔ شناسایی تهدیدات نوین سایبری مبتنی بر SIEM شامل بخش‌های:
  - زیرسامانه هوش تهدید
  - زیرسامانهٔ استخراج سناریوهای تهدید و حمله از پایگاه دانش تهدیدات Mitre
  - زیرسامانهٔ تحلیل رویدادهای SIEM بر اساس هوش تهدید به‌روز و سناریوهای تهدید استخراج شده
- پیاده‌سازی سامانه

۳ تعاریف و اختصارات

جدول1 - اختصارات

کلمه اختصاری	عبارت کامل	ترجمه فارسی	توضیح
SIEM	Security Information and Event Management	مدیریت اطلاعات و رویدادهای امنیتی	یک نوع نرم‌افزار یا سرویس که اطلاعات و رویدادهای مربوط به امنیت سیستم‌ها را جمع‌آوری، ذخیره، تحلیل و گزارش می‌کند
CTI	Cyber Threat Intelligence	هوش تهدیدات سایبری	اطلاعات و آگاهی در مورد تهدیدات سایبری که به سازمان یا شبکه‌ها وارد می‌شوند
IoC	Indicator of Compromise	شاخص تعارض/ شاخص‌های نفوذ	یک نوع داده یا اثری که نشان می‌دهد یک سیستم یا شبکه به بدافزار یا حمله معرض شده است
TTP	Tactics, Techniques, and Procedures	تاکتیک‌ها، تکنیک‌ها و روش‌ها	یک اصطلاح که برای توصیف رفتارها و روش‌هایی که متخاصمان سایبری برای انجام حملات خود استفاده می‌کنند به کار می‌رود
STIX	Structured Threat Information Expression	بیان اطلاعات ساختاریافته تهدید	یک نوع قالب بندی برای انتقال اطلاعات مربوط به تهدیدهای سایبری به صورت ساختاریافته و قابل فهم برای انسان و ماشین
CVSS	Common Vulnerability Scoring System	سامانه امتیازدهی آسیب‌پذیری‌های مشترک	یک نوع سامانه که برای اندازه‌گیری و ارزیابی شدت آسیب‌پذیری‌های سیستم‌ها و نرم‌افزارها استفاده می‌شود
NVD	National Vulnerability Database	پایگاه داده ملی آسیب‌پذیری‌ها	یک پایگاه داده که توسط دولت آمریکا اداره می‌شود و شامل اطلاعات در مورد آسیب‌پذیری‌های شناخته شده در سیستم‌ها و نرم‌افزارها است

JSON	JavaScript Object Notation	نشانه‌گذاری شیء جاوااسکریپت	یک نوع قالب بندی برای انتقال داده‌ها به صورت ساختاریافته و قابل فهم برای انسان و ماشین
XML	Extensible Markup Language	زبان نشانه‌گذاری قابل توسعه	یک نوع قالب بندی برای انتقال داده‌ها به صورت ساختاریافته و قابل توسعه
IP	Internet Protocol	پروتکل اینترنت	پروتکلی که برای انتقال داده‌ها بین دستگاه‌های متصل به اینترنت استفاده می‌شود
CVE	Common Vulnerabilities and Exposures	آسیب‌پذیری‌ها و افشاگری‌های رایج	سیستمی که برای شناسایی و ثبت آسیب‌پذیری‌های شناخته شده در سیستم‌ها و نرم‌افزارها استفاده می‌شود
UML	Unified Modeling Language	زبان مدلسازی یکپارچه	
UX	User Experience	تجربه کاربری	مفهومی که برای توصیف احساسات، نگرش‌ها و رضایت کاربران از استفاده از یک محصول، سرویس یا سیستم به کار می‌رود
C&C	Command and Control	فرمان و کنترل	یک سرور یا گروهی از سرورها که توسط یک حمله‌کننده برای کنترل بدافزارهایی که در سیستم‌های هدف نصب شده‌اند، استفاده می‌شود
APT	Advanced Persistent Threat	تهدید پیشرفته مداوم	یک حمله مخرب و مداوم که توسط یک گروه یا سازمان با منابع و توانایی‌های بالا انجام می‌شود و معمولاً هدف آن دسترسی به اطلاعات محرمانه یا تخریب سیستم‌های حیاتی است

جدول2 – عبارات تخصصی

عبارت تخصصی	ترجمه انگلیسی	توضیح
روز صفر	Zero Day	**این اصطلاح معمولاً به ابتدای وقوع یک حادثه، بازگشت نسخه یا عملکرد جدید یک برنامه یا سیستم اشاره داره. اصطلاحاً به لحظه‌ای اشاره می‌کنه که یک موضوع مهم و جدید ظاهر می‌شه.**
نرخ مثبت نادرست	False Positive Rate	**نسبت تعداد نتایج غلط مثبت به کل نتایجی که به اشتباه به عنوان مثبت تشخیص داده شده‌اند.**
نرمال‌سازی	Normalization	**فرایند تبدیل داده‌های ورودی به یک فرم استاندارد یا نرمال شده.**
آنتولوژی	Ontology	**ساختاری فرهنگی یا دانشی که مفاهیم و روابط بین آن‌ها را تعریف می‌کند.**
آسیب‌پذیری در سطح Pre-NVD	Pre-NVD Vulnerability	**مربوط به آسیب‌پذیری‌هایی است که قبل از ثبت و گزارش در پایگاه داده آسیب‌پذیری ملی (NVD) شناسایی شده‌اند.**
گارتنر	Gartner	**یک شرکت مشاوره و تحقیقاتی که در زمینه‌های مختلف فناوری اطلاعات، امنیت سایبری، تجارت الکترونیک و غیره فعالیت می‌کند**
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and	**یک مجموعه از تاکتیک‌ها، تکنیک‌ها و دانش مشترک در مورد رفتارهای متخاصمان سایبری که توسط شرکت میتر توسعه داده شده است**

	Common Knowledge	
فیشینگ	Phishing	**یک روش کلاهبرداری از طریق جعل هویت یک شخص یا سازمان معتبر در یک ارتباط دیجیتال برای بدست آوردن اطلاعات حساس کاربران**
باج‌افزار	Ransomware	**یک نوع بدافزار که دسترسی به سیستم یا داده‌های کاربر را محدود می‌کند و برای رفع محدودیت درخواست باج می‌کند**

۴ الزامات و مشخصات فنی

۴-۱ الزامات عملکردی

جدول زیر الزامات و مشخصات فنی عملکردی سامانه را به تفکیک مولفه‌های جمع‌آوری، تحلیل و گزارش‌دهی ارائه می‌دهد. پیشنهاد پروژهٔ ارائه شده باید تامین الزامات و مشخصات فنی فوق در طرح ارائه شده را تضمین نماید.

جدول ۳- الزامات و مشخصات فنی

الزامات و مشخصات فنی کلی سامانه	
شماره	الزامات و مشخصات فنی
۱-۱	سامانه باید کل چرخه حیات هوش و نظارت پیشگیرانه (proactive) تهدید را خودکار کرده و تشخیص و پاسخ حادثه را تسریع کند.
۱-۲	سامانه باید به کاربران اجازه دهد که امکان بررسی دستی داده‌ها یا اعتبارسنجی هوش تهدید را داشته باشند.
۱-۳	سامانه باید از ادغام با SIEM برای یکپارچه‌سازی فیدها پشتیبانی کند.
۱-۴	سامانه باید دارای ارجاع به منبع اطلاعات باشد، چه از طریق لینک مستقیم به منبع یا از طریق یک کپی ذخیره‌شده.
۱-۵	سامانه باید حداقل با یکی از SIEMهای بومی موجود قابل ادغام باشد و توانایی حفاظت از تهدیدات پیشرفته را داشته باشد.
الزامات و مشخصات فنی مولفه‌های جمع‌آوری	
شماره	الزامات و مشخصات فنی
۲-۱	فرایند جمع‌آوری و تجمیع داده‌های هوش تهدید باید به‌صورت خودکار انجام شود.
۲-۲	جمع‌آوری هوش از منابع مختلف باید بصورت خودکار باشد. به صورتی‌که امکان جمع‌آوری انبوه هوش با نرخ مثبت نادرست کم در زمان واقعی فراهم گردد.
۲-۳	سامانه باید کل فرایند تحقیق، جمع‌آوری، تجمیع و سازمان‌دهی داده‌های هوش تهدید را خودکار و ساده‌سازی کند. علاوه بر این، نرمال‌سازی، حذف موارد تکراری و غنی‌سازی داده‌ها را نیز به‌صورت خودکار و ساده انجام دهد.

۲-۴	هوش جمع‌آوری‌شده باید حداقل داده‌های ۲ سال اخیر را داشته باشد و باید در نتایج پرس‌وجو در پورتال با جزئیات گنجانده شود.
۲-۵	سامانه باید هر IoC را با امتیازات قابلیت اطمینان، کیفیت تشخیص یا امتیاز ریسک ارائه دهد. این امتیازات باید با منطق مناسبی توجیه شوند. امتیازات همچنین باید پویا باشند تا ریسک بلادرنگ خودکار IoC مذکور را نشان دهند.
۲-۶	همزمان با جمع‌آوری اطلاعات یا زمینه‌های جدید از منابع مختلف، هوش باید در بازه‌های زمانی مشخص‌شده (روزانه) ارائه و به‌روزرسانی شود.
۲-۷	سامانه باید قابلیت جمع‌آوری اطلاعات حداقل ۵ APT مهم که حتما دو تا از آنها منتسب به کشورهای آمریکا و اسرائیل باشند را داشته باشد.
۲-۸	سامانه باید قابلیت مقیاس پذیری در حوزهٔ جمع‌آوری اطلاعات سایر APT ها را نیز داشته باشد.
۲-۹	سامانه باید از دریافت داده‌ها از فرمت‌های مختلف مانند STIX/TAXII، JSON، XML و CSV برای تحلیل پشتیبانی کند.
۲-۱۰	سامانه باید فیدهای هوش تهدید منبع باز که به طور خودکار در سامانه وارد می‌شود را ارائه دهد.
۲-۱۱	فیدها باید لیست ریسک آسیب‌پذیری‌ها را ارائه کنند.
۲-۱۲	فیدها باید لیست خطرات IP مخرب، دامنه مخرب، URLو hash را ارائه دهند.
۲-۱۳	فیدها باید اطلاعات زمینه‌ای و قابل اجرا را همراه با شواهدی ارائه کنند که کار تیم پاسخدهی برای انجام اقدامات لازم تسهیل گردد.
۲-۱۴	اطلاعات IoC باید با زمینه کامل موجودیت‌های مرتبط، مانندhash های مرتبط، IP، CVEو عوامل تهدید، بردارهای تهدید، بدافزارها، محصولات تحت‌تأثیر و غیره ارائه شود.
۲-۱۵	سامانه باید فیدهای هوش تهدید را از مهم‌ترین منابع منبع باز سراسر دنیا جمع‌آوری کند. برخی از این منابع عبارتند از: • AlienVault Open Threat Exchange • URLhaus • Abuse.ch • VirusTotal • VirusShare • FireHOL IP lists • PhishTank
۲-۱۶	فید هوش تهدید باید ویژگی‌های اساسی را به عنوان بخشی از فیدهای داده بر اساس در دسترس‌بودن ارائه دهد، مانند:

	• IP • دامنه • شهرت، آبرو • اطمینان • رفتار • لیست‌کردن در یک پنجره ۹۰ روزه • ویژگی‌های موقعیت جغرافیایی • ویژگی‌های صنعت • ویژگی‌های مالکیت IP/دامنه • ویژگی‌های ثبت IP/دامنه • جزئیات رفتار حمله • جزئیات رفتار بدافزار • جزئیات رفتار فیشینگ • جزئیات رفتار کلاهبرداری • جزئیات رفتار ربات • جزئیات رفتار C&C
الزامات و مشخصات فنی مولفه تحلیل	
شماره	الزامات و مشخصات فنی
۳-۱	سامانه باید داده‌های جمع‌آوری شده را با استفاده از آنتولوژی‌ها طبقه‌بندی کند و تحلیلگران را قادر سازد تا جست‌وجوهای قدرتمند و شهودی را انجام دهند که فراتر از کلمات کلیدی ساده و قوانین همبستگی ساده است.
۳-۲	سامانه باید قابلیت شناسایی حداقل ۵ APT مهم که حتما دو تا از آنها منتسب به کشورهای آمریکا و اسرائیل باشند را داشته باشد.
۳-۳	سامانه باید قابلیت مقیاس پذیری در حوزهٔ شناسایی سایر APT ها را نیز داشته باشد.
۳-۴	سامانه باید بتواند در فرایند تحلیل از موارد زیر پشتیبانی کند: • روندها و توسعه‌ها به‌صورت روزانه • نگاه تاریخی به رویدادهای مرتبط • نقش‌های درگیر در رویدادها (مهاجمان/بازیگران تهدید، اهداف/سازمان‌ها) • TTPهای گزارش‌شده (بردارهای حمله، بدافزارها، سوءاستفاده‌ها)

	• شاخص‌های گزارش‌شده (آدرس‌های IP، دامنه‌ها، hashها، URLها و غیره) • عملیات مرتبط • دسترسی به مراجع اصلی با محتوای ذخیره‌شده برای منابع غیردائمی • سایر جزئیات زمینه‌ای در مورد رویدادها
۳-۵	سامانه باید توانایی پیوند رویدادهای امنیتی گزارش‌شده با دانش زمان واقعی از دارایی‌هایی که هدف قرار می‌گیرند را فراهم کند.
الزامات و مشخصات فنی مولفه گزارش‌دهی	
شماره	الزامات و مشخصات فنی
۴-۱	سامانه باید بتواند هشدارهایی را از طریق پورتال، ایمیل و غیره ارائه دهد.
۴-۲	سامانه باید گزارشات را در قالب‌های استاندارد باز OpenIoC و STIX ارائه دهد.
۴-۳	گزارش تهدید شناسایی شده باید شامل موارد زیر باشد: • تحلیل بدافزار • پروفایل بازیگران تهدید • تحلیل اخبار امنیتی روزانه • روند و پیش‌بینی • پروفایل ریسک کشور • پروفایل ریسک صنعت • سناریوهای آینده • تحلیل آسیب‌پذیری • ردیابی بهره‌برداری آسیب‌پذیری • هشدار در مورد تحولات مهم تهدید • IoCها • باج‌افزار • APTها • بازیگران مالی، ایدئولوژیکی، دولتی و با انگیزه استراتژیک • تهدیدات فناوری‌های نوظهور
۴-۴	در صورت عدم امکان تامین برخی اطلاعات مورد قبل، گزارش تهدید شناسایی شده حداقل باید شامل موارد زیر باشد: • اهداف بازیگر تهدید

	• شرایطی که تحت آن تهدید احتمالاً از یک آسیب‌پذیری سوءاستفاده می‌کند • نوع تهدید • فعالیت فعلی که تهدید را در بر می‌گیرد • پیامد تهدید برای سازمان، اگر تهدید با موفقیت اجرا شود • شاخص‌هایی که نشان می‌دهد تهدید در حال حاضر علیه سازمان عمل می‌کند یا به دارایی‌های سازمان آسیب می‌رساند • دفاع در برابر تهدیدات • ارزیابی قابلیت اطمینان منبع اطلاعات • قابلیت اطمینان خود اطلاعات
۴-۵	سامانه باید داشبورد و نمایش بصری بینش‌ها و یافته‌ها را ارائه دهد به‌صورتی‌که بتواند در قالب‌های مختلف مانند PDF، CSV، Word و غیره دانلود شود.

۴-۲ الزامات غیرعملکردی

سامانه باید قابلیت‌های مقیاس‌پذیری، توزیع‌شدگی، تحمل خطا، توزیع بار، دسترس‌پذیری و مقیاس‌پذیری را در تمام لایه‌های معماری و طراحی سامانه فراهم آورد. هم‌چنین طراحی سامانه باید به صورت ماژولار انجام شود به گونه‌ای که طراحی و پیاده‌سازی سامانه قابلیت ارتقا و گسترش با کمترین هزینه را داشته باشد.

۵ مراحل اجرا و شرح خدمات پروژه

فاز ۱: طراحی معماری سامانه (۳ ماه)

- طراحی سیستمی سامانه
- طراحی عملیاتی سامانه
- طراحی فناورانه سامانه
- تهیهٔ مجموعه دادهٔ مورد نیاز جهت تست
- طراحی بستر راه‌اندازی تست سامانه
- ارائه تجربه کاربری (ux) سامانه
- انتقال دانش فنی

فاز ۲: پیاده‌سازی سامانه و راه‌اندازی بستر تست نرم‌افزار (۶ ماه)

- پیاده‌سازی سامانه مشتمل بر مولفه‌های:
  - جمع‌آوری
  - پایگاه دانش
  - تحلیل
  - داشبورد و واسط کاربری
- تهیهٔ روال‌های تست سامانه مشتمل بر تست‌های
  - عملکردی (Functional)
  - غیر عملکردی شامل کارایی (Performance)، بار (load)، استرس (stress) و امنیت سطح یک
- آماده‌سازی بستر راه‌اندازی تست سامانه
- تست اولیهٔ سامانه توسط تیم پیاده‌سازی
- انتقال دانش فنی

فاز ۳: راه‌اندازی سامانهٔ پیاده‌سازی شده (۲ ماه)

- تست سامانه بر اساس روال‌های تست تدوین شده
- رفع اشکالات احتمالی سامانه

- راه‌اندازی و انتقال دانش فنی

فاز ۴: پشتیبانی سامانهٔ پیاده‌سازی شده (۱ ماه)

۶ خروجی‌های هر مرحله از اجرای پروژه

خروجی‌های پیش‌بینی‌شده برای هر یک از مراحل اجرای پروژه، عبارت‌اند از:

خروجی‌های فاز یک:

- طرح سامانه شامل:

معماری مفهومی، سیستمی، عملیاتی و فناورانه سامانه

- مجموعه دادهٔ مورد نیاز جهت تست
- سند طراحی بستر راه‌اندازی تست سامانه
- تجربه کاربری (ux) سامانه

خروجی‌های فاز دو:

- (راه‌اندازی) سامانهٔ پیاده‌سازی شده مشتمل بر مولفه‌های:
  - جمع‌آوری هوش تهدیدات
  - جمع‌آوری دانش تهدیدات
  - تحلیل تهدید
  - پایگاه دانش
  - داشبورد و واسط کاربری
- سند فنی پیاده‌سازی مشتمل بر مشخصات فنی و امنیتی سامانه، روش‌ها و پروتکل‌های ادغام با SIEM به تفکیک مولفه‌های ذکر شده
- سند بررسی و استخراج سناریوهای حمله از پایگاه دانش Mitre
- روال‌های تست سامانه مشتمل بر تست‌های
  - عملکردی (Functional)
  - غیر عملکردی شامل کارایی (Performance)، بار (load)، استرس (stress) و امنیت سطح یک
- سند آزمون و اعتبارسنجی بر اساس روال‌های تست
- بستر راه‌اندازی شدهٔ تست سامانه

خروجی‌های فاز سه:

- (راه‌اندازی) نسخه‌های رفع اشکال شدهٔ سامانه بر اساس نتایج تست
- انتقال دانش فنی

۷ حداکثر مدت‌زمان مجاز و اعتبار برای ارائه پیشنهاد اجرای پروژه

۷-۱ حداکثر مدت‌زمان مجاز برای ارائه پیشنهاد

دریافت‌کننده RFP، می‌بایست حداکثر ۱۴ روز پس از دریافت RFP، پیشنهاد خود را بر اساس مکانیسم پیش‌بینی‌شده دربند ۸ این RFP، تحویل پژوهشگاه ارتباطات و فناوری اطلاعات نماید. پیشنهادهای ارائه‌شده پس‌ازاین تاریخ، قابل وصول توسط پژوهشگاه ارتباطات و فناوری اطلاعات نخواهند بود.

۷-۲ حداکثر مدت‌زمان مجاز برای اجرای پروژه

حداکثر مدت‌زمان پیش‌بینی‌شده و قابل‌پذیرش برای اجرای این پروژه، ۱۲ ماه بر اساس مراحل اجرا و شرح خدمات گفت شده می‌باشد. چنانچه پیشنهاددهنده در فرم پیشنهاد پروژه، مدت‌زمان اجرای پروژه را بیش از مدت‌زمان مجاز اعلام نماید، قابل وصول توسط پژوهشگاه ارتباطات و فناوری اطلاعات نخواهد بود.

۷-۳ سایر الزامات و محدودیت‌های موجود در اجرای پروژه

علاوه بر محدودیت موجود در خصوص زمان اجرای پروژه، لازم است پیشنهاددهندگان در تنظیم پیشنهاد خود، موارد ذیل را نیز رعایت فرمایند :

۱. پیشنهاد باید در قالب آخرین نسخه از "فرم پیشنهاد پروژه" موجود در سایت پژوهشگاه ارتباطات و فناوری اطلاعات (حوزه معاونت پژوهش و توسعه ارتباطات علمی، دفتر امور پژوهشی، فرم‌ها)، تنظیم و ارائه گردد.

۲. در جدول ساختار شکست پروژه پیش‌بینی‌شده در بخش ۷-۳-۲ فرم پیشنهاد پروژه، لازم است شرح فعالیت‌های هر مرحله از پروژه (مطابق شرح فعالیت‌های پیش‌بینی‌شده در RFP به همراه موارد احتمالی که پیشنهاددهنده، انجام آن‌ها را ضروری می‌داند) به همراه کلیه اطلاعات درخواست شده در فرم، به تفکیک برای هر فعالیت و مرحله، ارائه گردد. از خالی گذاشتن ستون‌های این جدول برای فعالیت‌های پروژه، خودداری گردد.

۳. در جدول مشخصات منابع انسانی پیش‌بینی‌شده در بخش ۳-۱ فرم پیشنهاد پروژه، لازم است نام و سایر مشخصات درخواست شده برای کلیه پرسنلی که در اجرای پروژه به‌صورت واقعی مشارکت دارند با ذکر میزان مشارکت درج گردد.

۴. هزینه‌های سربار، تنها برای پیشنهاددهندگان حقوقی (دانشگاه‌ها) پیش‌بینی‌شده است و شرکت‌ها می‌توانند بجای هزینه سربار، هزینه‌های اضافی متحملِ بابت این پروژه را عنوان نمایند.

۵. مجری پروژه باید در تمام مراحل طراحی و پیاده‌سازی و همچنین، در پایان پروژه منابع کدها را در اختیار کارفرما قرار دهد.

۸ تحویل پیشنهاد به پژوهشگاه ارتباطات و فناوری اطلاعات

۸-۱ حداقل شرایط پیشنهاد قابل تحویل

پیشنهادهایی قابل وصول می‌باشند که شرایط مندرج دربندهای ۶ و ۷ این RFP را کاملاً رعایت نموده باشند. در زمان ارائه پیشنهاد به پژوهشگاه ارتباطات و فناوری اطلاعات، رعایت شرایط مذکور، کنترل‌شده و در صورت عدم رعایت هر یک از موارد، از تحویل پیشنهاد، خودداری خواهد شد. پیشنهاد دهندگانی که در حال حاضر محصولات SIEM بومی و خدمات SOC ارائه می‌دهند، در اولویت خواهند بود.

۸-۲ نحوه تحویل پیشنهاد

پیشنهاددهندگان می‌بایست پیشنهاد خود را به نام معاونت پژوهش و توسعه ارتباطات علمی به دبیرخانه پژوهشگاه ارتباطات و فناوری اطلاعات، تحویل داده و رسید دریافت نمایند. (درصورتی‌که مدارک به سایر واحدهای دیگر پژوهشگاه تحویل داده شود در فراخوان ثبت نخواهد شد و این پژوهشگاه در قبال آن هیچ‌گونه مسئولیتی ندارد)

۸-۳ نحوه ارزیابی پیشنهاد

ارزیابی پیشنهادهای رسیده بر اساس پارامترهای زیر خواهد بود:

۱- میزان تسلط به ابعاد و جوانب پروژه (امتیاز این ردیف با توجه به سمینار ارائه‌شده توسط پیشنهاددهنده و نیز مطالب ارائه‌شده در فرم پیشنهاد پروژه در خصوص شرح خدمات، خروجی‌ها، اهداف و . . . تعیین می‌گردد)

۲- نحوهٔ تخصیص منابع انسانی شامل کیفیت و کمیت نیروها (رزومه و سابقه کاری لازم در ارتباط با انجام خدمات موردنیاز پروژه، تعداد و تناسب نیروها با توجه به حجم کار، نوع رابطه استخدامی نیروها بر اساس مدارک ارائه‌شده)

۳- کیفیت ساختار شکست پروژه متناسب با شرح خدمات و اهداف پروژه

۴- کیفیت ساختار سازمانی پیش‌بینی‌شده برای انجام پروژه(تیم‌های اجرایی، مدیریت پروژه و...)

۵- ساختار و روال‌های پیش‌بینی‌شده برای کنترل و مدیریت پروژه و تأیید صحت خروجی‌ها

۶- روال‌ها، متدولوژی و استانداردهای پیشنهادی برای اجرای شرح خدمات

۷- نحوه ارائه زمان‌بندی و پوشش کامل و به‌موقع شرح خدمات