دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۴، جلد ۲۳، شماره ۱ (۱۹-۴۴)
https://monadi.isc.org.ir

تحلیل چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های پشتیبان توسعه شواهد تهدید در سازمان

امین چهاردولی[۱]، ابوذر عرب سرخی[۲،*]

[۱] دانشکده مدیریت، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
[۲] پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران

اطلاعات مقاله

تاریخچه مقاله:
تاریخ دریافت: ۲۷ اردیبهشت ۱۴۰۳
تاریخ پذیرش: ۱۵ دی ۱۴۰۳
انتشار آنلاین: ۲۴ اردیبهشت ۱۴۰۴

کلمات کلیدی:
شواهد تهدید
چارچوب‌ها
پلتفرم‌ها
استانداردهای مرجع
ائتلاف‌ها

نوع مقاله: پژوهشی

چکیده

در دنیای مدرن امروزی و با ظهور پیشرفت‌های فناورانه، امنیت سایبری به یکی از مسائل حیاتی تبدیل شده است. هر روزه میلیون‌ها قلم داده در سطح اینترنت جابجا می‌شوند و سازمان‌ها و افراد را با تهدیداتی همچون نفوذهای سایبری، دسترسی غیرمجاز به اطلاعات و ... مواجه نموده است. در این محیط پویا، شواهد تهدید به عنوان یک ابزار برجسته و کارآمد برای مقابله با این تهدیدات –به دور از اغماض و حساسیت‌های لازم– مورد توجه قرار گرفته است. این رویکرد نوین، سازمان‌ها را قادر می‌سازد تا با تحلیل دقیق داده‌های شواهد تهدید و به صورت پیشگیرانه، واکنش مناسبی را نسبت به حملات سایبری ارائه دهند و شرایط امنیت اطلاعات مدنظر خود را تضمین نمایند. با توجه به روند رو به رشد حملات سایبری، دولت‌ها و سازمان‌های مختلف در سراسر جهان به دنبال راهبردها و راهکارهایی برای تقویت ظرفیت‌های شواهد تهدید در سطح نهادی هستند. در این مقاله، محقق ضمن مطالعه مقایسه‌ای چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید (به عنوان ابزارهای کلیدی برای افزایش سطح امنیت سایبری و پیشگیری از حملات)، به بررسی تحلیلی و دقیق‌تری از این ابزارها و نحوه نقش‌آفرینی آن‌ها در تقویت نظام امنیت سایبری پرداخته‌است. در واقع، این تحقیق با تمرکز بر نقاط قوت ساختار و مؤلفه‌های پیاده‌سازی شواهد تهدید در سازمان‌ها و با بهره‌گیری از تجارب مرتبط دولت‌ها و ائتلاف‌های بین‌المللی، تلاش می‌کند تا نقش اساسی این مؤلفه‌ها در تولید، انتشار و بهره‌برداری از رویکرد شواهد تهدید را برای مخاطب تصویرسازی نماید و اهمیت استفاده مؤثر از این راهکار در چرخه امنیت اطلاعات سازمان را مورد بررسی قرار دهد. دستیابی به شواهد تهدید از طریق چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های مرتبط مستلزم توجه به الزامات و اقدامات متنوعی است. در این راستا و با استفاده از نتایج حاصل از این تحقیق، تصمیم‌سازان و متولیان امر می‌توانند زمینه اقدامات لازم جهت پیاده‌سازی رویکرد شواهد تهدید در سطح سازمان را پیش‌بینی و عملیاتی نمایند. علاوه بر این، پیاده‌سازی چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید نه تنها به سازمان‌ها کمک می‌کند تا از شواهد تهدید بهتر استفاده نمایند، بلکه در امر تصمیم‌گیری و مقابله با حملات سایبری نیز برای مجموعه بسیار حائز اهمیت باشد.

© ۱۴۰۴ انجمن رمز ایران

۱ مقدمه

چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های پشتیبان توسعه شواهد تهدید معرف مهم‌ترین مؤلفه‌ها، ابزارها و رویکردهایی هستند که در چرخه جمع‌آوری، تحلیل و استفاده از رویکرد شواهد تهدید مورد استفاده قرار

*نویسنده مسئول.
آدرس‌های رایانامه: amin.chahardoli@iau.ac.ir (امین چهاردولی)، abouzar_arab@itrc.ac.ir (ابوذر عرب سرخی)
© ۱۴۰۴ تمامی حقوق متعلق به انجمن رمز ایران است.

می‌گیرند. این ابزارها و استانداردها از گذشته تا به امروز به‌شدت پیشرفت کرده‌اند تا سازمان‌ها را در مقابله مؤثر با تهدیدات سایبری یاری نمایند. این مؤلفه‌ها به سازمان‌ها کمک می‌کنند تا رویکرد شواهد تهدید را برای مقابله با حملات و تهدیدات مختلف، به شکلی بهتر تولید، منتشر و پیاده‌سازی نمایند [۱].

این مقاله بر اساس یک مطالعه گسترده و عمیق پیرامون مهم‌ترین چارچوب‌های بین‌المللی در راستای پیاده‌سازی و توسعه شواهد تهدید و نیز به‌کارگیری استانداردها و ساختارهای متناسب با نیازهای سازمان – که شامل اصول، فرآیندها، وظایف و نقش‌های مختلفی است– در چرخه جمع‌آوری، تحلیل و استفاده از اطلاعات شواهد تهدید ارائه شده است. بر اساس تحلیل تجارب مفید منتشر شده و آموزه‌های به‌دست آمده از این تحقیق، امکان ارائه توصیه‌های کاربردی برای سازمان‌ها در زمینه مدیریت شواهد تهدید میسر گردیده است.

تولید، انتشار، تحلیل و استفاده از رویکرد شواهد تهدید برای سازمان‌ها بنا به دلایلی مهم و حائز اهمیت و در شرایطی به‌شدت ضروری است:

(۱) شناسایی و پیش‌بینی تهدیدات: شواهد تهدید به سازمان‌ها در شناسایی و تحلیل الگوها و روندهای حملات سایبری کمک می‌کند. این اطلاعات سازمان‌ها را در پیش‌بینی نوع حملات آینده و برنامه‌ریزی مناسب جهت مقابله با آن‌ها راهنمایی می‌نماید.

(۲) ارتقای پاسخگویی به حملات: با استفاده از رویکرد شواهد تهدید، سازمان‌ها می‌توانند به‌سرعت و به‌شکلی مناسب نسبت به حملات سایبری واکنش نشان دهند. این امر می‌تواند از ایجاد خسارت‌های بیشتر به سازمان جلوگیری نموده و هزینه‌های ناشی از حملات را تا حد امکان کاهش دهد.

(۳) ارتقای امنیت سایبری: سازمان‌ها با استفاده از رویکرد شواهد تهدید می‌توانند بهبودهای لازم را در سیستم‌ها و شبکه‌های خود اعمال و در مقابل حملات سایبری از منابع خود به شکل بهتری محافظت نمایند. این اقدامات شامل تحقیق و توسعه بر روی فناوری‌های امنیتی، اجرای سیاست‌ها و رویه‌های امنیتی کارآمد و ارتقاء آگاهی و آموزش کارکنان است [۲].

تدوین و پیاده‌سازی چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌ها، نه‌تنها به سازمان‌ها کمک می‌کند تا از رویکرد شواهد تهدید بهتر بهره برند، بلکه در تصمیم‌گیری‌ها و مقابله با حملات سایبری نیز حائز اهمیت است.

۲ کلیات تحقیق

۱.۲ مضمون شواهد تهدید

در استاندارد NIST، شواهد تهدید به عنوان فرآیندی تعریف می‌شود که از طریق جمع‌آوری، تحلیل و تفسیر داده‌ها و اطلاعات، به تفسیر تهدیدات محتمل سایبری می‌پردازد. این تعریف بر تشخیص مستمر تهدیدات و اطلاعاتی تأکید دارد که به تصمیم‌گیری‌های امنیتی کمک می‌کنند [۲].

در MITRE، شواهد تهدید به عنوان فرآیندی توصیف می‌شود که از طریق جمع‌آوری، تحلیل و تفسیر داده‌های مرتبط با تهدیدات، کسب اطلاعات پیرامون حملات احتمالی را فراهم می‌نماید. این اطلاعات می‌توانند برای انجام اقدامات مؤثر و به‌موقع جهت جلوگیری از حملات و یا مدیریت مخاطرات استفاده شوند [۱].

در مقاله هوش امنیت، شواهد تهدید به عنوان فرآیندی توصیف می‌شود که شامل جمع‌آوری داده‌هایی است که از منابع مختلف مانند شبکه‌ها، ابزارهای مربوط به امنیت، منابع عمومی و ... تأمین می‌شود و سپس این اطلاعات تحلیل و تفسیر می‌شوند تا تهدیدات را تشخیص داده و مقابله با آن‌ها صورت گیرد [۳].

این تعاریف به صورت کلی بر اهمیت جمع‌آوری و تحلیل داده‌ها و اطلاعات به‌منظور شناخت بهتر و مدیریت تهدیدات سایبری تأکید دارند.

۲.۲ ضرورت پرداخت به موضوع شواهد تهدید

در دنیای فراگیر فناوری اطلاعات، شواهد تهدید به عنوان یک ابزار حیاتی و غیرقابل‌انکار در مقابله با چالش‌های امنیتی سازمان‌ها نقش بسیار مؤثری را ایفا می‌نماید. استفاده از شواهد تهدید در مدیریت امنیت سایبری و مفاهیمی چون شناسایی تهدیدات، تصمیم‌گیری‌های امنیتی مبتنی بر داده، حفاظت از اطلاعات حساس، استراتژی‌های دفاعی، تشخیص زودهنگام و واکنش سریع، پیش‌بینی و مدیریت مخاطره به عنوان عاملی کلیدی در ارتقای سطح امنیت مطرح می‌شود. ضرورت توجه به شواهد تهدید باهدف برجسته کردن اهمیت این موضوعات و نقش بی‌قیاس آن در پیشگیری و مقابله با تهدیدات سایبری، سازمان‌ها را به بهره‌مندی از این ابزار قدرتمند در حوزه امنیت سایبری تشویق می‌نماید [۳].

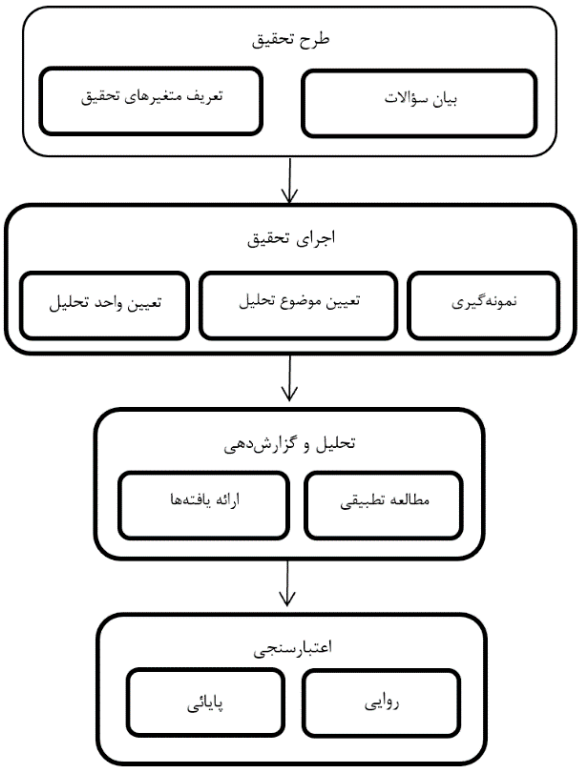
۳.۲ سؤالات تحقیق

براساس مجموعه موارد مطرح‌شده، سؤال اصلی این تحقیق عبارتست از:

- نقش‌های کارکردی چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های پشتیبان شواهد تهدید در سازمان‌ها چیست؟

پاسخ به سؤال فوق مستلزم پاسخگویی به سؤالات فرعی زیر است:

- مؤلفه‌های سازنده و اجزاء چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های پشتیبان شواهد تهدید در سازمان‌ها کدامند؟
- عوامل تاثیرگذار بر انتخاب و بکارگیری چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های پشتیبان شواهد تهدید در سازمان‌ها کدامند؟
- معیارهای تاثیرگذار بر انتخاب و بکارگیری چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های پشتیبان شواهد تهدید در سازمان‌ها کدامند؟
- وضعیت این معیارهای تاثیرگذار پیرامون هریک از چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های منتخب پشتیبان شواهد تهدید در سازمان‌ها چگونه است؟
- ارزیابی و ارزش‌گذاری چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های منتخب پشتیبان شواهد تهدید براساس این معیارها



شکل ۱. چارچوب انجام تحقیق

چگونه خواهد بود؟

۴.۲ چارچوب انجام تحقیق

محقق در راستای تحلیل کاربردپذیری چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های پشتیبان توسعه شواهد تهدید در سازمان‌ها، ضمن بررسی موضوعی و ساختاری هریک از موارد اخیرالذکر، نسبت به بررسی مقایسه‌ای چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های منتخب شواهد تهدید در قالب یک چارچوب نظام‌مند تحقیق اقدام نموده‌است. این چارچوب در قالب شکل ۱ ارائه شده‌است [۴].

در این تحقیق از روش تحلیل محتوی کیفی استفاده شده‌است که یکی از روش‌های انجام پژوهش کیفی است. تحلیل محتوای کیفی در جایی که تحلیل کمی به محدودیت‌هایی می‌رسد، نمود می‌یابد. بنابراین تحلیل محتوی کیفی را می‌توان روش تحقیقی برای تفسیر ذهنی محتوایی داده‌های متنی دانست [۴].

هم اکنون سه رویکرد: سنتی (متعارف) [۱]، هدایت‌شده [۲]، جامع [۳] برای کاربرد تحلیل محتوا مطرح است. در تحلیل محتوی به روش متعارف طبقات به‌گونه مستقیم از متن داده‌ها (براساس موضوعات اصلی تحقیق) استخراج می‌شوند. ستون فقرات تحقیق حاضر مبتنی بر روش تحلیل محتوای متعارف بنا نهاده شده‌است. در این روش، محقق به‌دنبال تفسیر ذهنی محتوای متنی از طریق فرآیندهای بررسی و طبقه‌بندی نظام‌مند و مقوله‌بندی یافته‌های تحقیق در قالب یک چارچوب مشخص است [۴]. پیش‌فرض محقق پیرامون استفاده از این روش تحقیق، جدید بودن پدیده مورد مطالعه (یعنی شواهد تهدید) و محدود بودن منابع نظری پیرامون آن است. در این شرایط، محقق از به‌کارگیری مقوله‌های از پیش تعریف‌شده پرهیز می‌نماید و به‌دنبال به‌کارگیری رویکردی داده‌رانده برای شناسایی مقوله‌ها است. براساس روش پایه انتخابی (تحلیل محتوای متعارف)، محقق مجموعه‌ای از فعالیت‌های مستقل اما بهم‌پیوسته را در قالب سه گام برای پیشبرد تحقیق حاضر پیش‌بینی نموده‌است. این گام‌ها در قالب شکل ۱ ارائه شده‌است [۵].

البته محقق برای غنابخشی به یافته‌های تحقیق از مجموعه‌ای از روش‌ها و تکنیک‌های تحقیق در مرحله سوم (تحلیل و گزارش‌دهی) استفاده نموده‌است. در این گام و برای تحلیل یافته‌های تحقیق –مبتنی بر درس‌های آموخته و تجربیات گزارش‌شده مراجع بین‌المللی– از تکنیک‌های بررسی درون موردی و بین موردی و نیز بررسی مقایسه‌ای راهبردی و عملیاتی (در قالب مجموعه‌ای از جدوال مقایسه‌ای) استفاده شده‌است. در بررسی مقایسه‌ای راهبردی و عملیاتی، محقق به دنبال هدف‌هایی فراتر از توصیف بوده و این‌کار متضمن داوری و بررسی تحلیلی موارد آزمودنی (موضوعات تحلیلی در سطح چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های پشتیبان شواهد تهدید) است. در این نگاه، محقق برای بهبود یافته‌ها از بررسی مقایسه‌ای می‌تواند با هدف تصمیم‌گیری در سطح سازمانی بهره‌برداری نماید [۵]. علاوه‌براین، در تحلیل‌های درون موردی و بین موردی –مبتنی بر ساختار حاکم بررسی موردی چندگانه مطرح‌شده در تحقیق حاضر– محقق به دنبال مقایسه دیدگاه‌های حاکم در سطح چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های پشتیبان شواهد تهدید است [۴].

جهت اعتبارسنجی و ارزیابی تحلیل مقایسه‌ای انجام‌شده محقق از روش دلفی فازی استفاده می‌نماید [۶]. در این راستا، ابتدا برای اعتبارسنجی (در کنار معیارهای معرفی‌شده توسط مراجع معتبر) و وزن‌دهی معیارهای انتخاب و ارزیابی چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های پشتیبان شواهد تهدید از روش دلفی فازی [دو مرحله‌ای/سه مرحله‌ای] بهره‌برداری گردیده است. مبنای انتخاب معیار، وزن‌دهی به آن‌ها و نیز ارزش‌گذاری چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های پشتیبان شواهد تهدید مبتنی بر پنل خبرگی، استفاده از مصاحبه نیمه ساختاریافته (به عنوان روش گردآوری اطلاعات) و بهره‌برداری از روش دلفی فازی و دست‌یابی به اجماع مبتنی بر این روش است. روش دلفی فازی برای مدیریت عدم قطعیت در نظرات کارشناسان بکار می‌رود [۷] و نتایج آن به صورت درصدهای وزن نسبی در جداول آماری بخش‌های چهارگانه این تحقیق نشان داده شده‌اند.

مراحل اجرای روش دلفی‌فازی برای انتخاب و وزن‌دهی معیارهای (در مرحله اول) و نیز ارزیابی و ارزش‌گذاری چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های پشتیبان شواهد تهدید (در مرحله دوم) شامل:

۱) تشکیل گروه کارشناسان (که بسته به حوزه‌های ارزیابی چهارگانه

[1] Conventional [2] Directed [3] Summative

تحقیق متفاوت است که در بخش‌های مربوطه در مقاله حاضر به آن اشاره شده است)،

۲) تعریف معیارهای ارزیابی (که بسته به حوزه ارزیابی و نیز مراجع اولیه إحصاء معیار متفاوت است)،
۳) طراحی پرسشنامه اولیه (اعتبارسنجی معیار، وزن‌دهی آن‌ها و نیز ارزیابی مقوله‌های اصلی تحقیق)،
۴) جمع‌آوری نظرات دور اول و تحلیل نتایج آن،
۵) طراحی پرسشنامه دور دوم بر اساس نتایج دور اول،
۶) جمع‌آوری نظرات دور دوم و تحلیل آن‌ها. این فرآیند تا رسیدن به اجماع نسبی تکرار می‌شود [۷].

نظرات کارشناسان بر اساس معیارهای تعریف‌شده، وزن آن‌ها و نیز ارزیابی چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های پشتیبان شواهد تهدید مبتنی بر این معیارها جمع‌آوری و ارزیابی می‌شوند تا امتیاز نهایی برای هر چارچوب تعیین شود، که به سازمان‌ها کمک می‌کند چارچوب مناسب را انتخاب کنند.

در ادامه این مقاله، به معرفی چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید همراه با ویژگی‌های کلیدی آن‌ها –نظیر هدف، ساختار و اجزاء تشکیل‌دهنده– پرداخته خواهد شد. در ادامه و در بخش ۶، ائتلاف‌های امنیتی فعال شواهد تهدید –براساس نقاط قوت و ضعف و سطح اثربخشی آن‌ها– ارزیابی می‌شوند. در نهایت و در بخش ۷ مقاله، موضوع نتیجه‌گیری همراه با توصیه‌های لازم برای ایجاد ساختار و زیرساخت شواهد تهدید در سازمان ارائه می‌شود.

۳ چارچوب‌های پشتیبان شواهد تهدید

چارچوب‌های پشتیبان شواهد تهدید معرف ابزارها و مدل‌هایی هستند که به سازمان‌ها کمک می‌کنند تا بهترین استفاده را از اطلاعات در مواجهه با تهدیدات سایبری داشته باشند. این چارچوب‌ها شامل مدل‌هایی برای شناسایی، تحلیل و مقابله با تهدیدات هستند [۸]. در دهه حاضر، با پیشرفت فراوان فناوری و گسترش روزافزون تهدیدات سایبری، نیاز به چارچوب‌ها و مدل‌های شواهد تهدید برای تحلیل، مدیریت و حفاظت از امنیت اطلاعات اجتناب‌ناپذیر شده است. این چارچوب‌ها، برای درک الگوها، بهینه‌سازی مقابله با حملات، تحلیل روابط، بهبود وضعیت امنیت سایبری، ارزیابی مقاومت و واکنش سریع به تهدیدات، به عنوان یک راهنمای عملیاتی به سازمان‌ها و تیم‌های امنیتی کمک می‌کنند [۹]. استفاده از هر چارچوب با مزایا و کاربردهای خاص خود، بستگی به نیازها و شرایط سازمان هدف دارد. در ادامه به برخی از مهم‌ترین این چارچوب‌ها اشاره می‌شود.

۱.۳ چارچوب MITRE ATT&CK

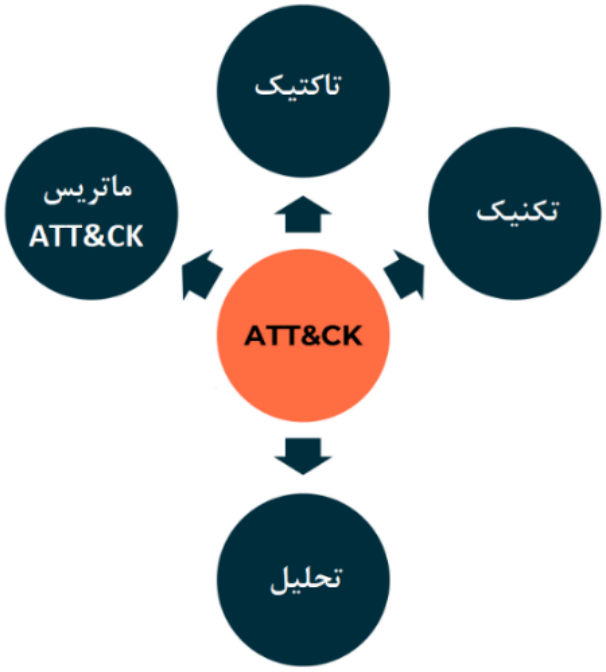
چارچوب MITRE ATT&CK [1] معرف یک مدل گسترده و جامع در حوزه شواهد تهدید است که توسط مؤسسه MITRE Corporation توسعه داده شده است و تمامی مراحلی که یک حمله سایبری ممکن است طی کند را شناسایی می‌نماید. این مدل شامل مجموعه‌ای از تکنیک‌ها، تاکتیک‌ها و روش‌های مورد استفاده مهاجمین در مراحل مختلف یک حمله است. این چارچوب به‌طور جامع روش‌ها، تاکتیک‌ها و تکنیک‌های مورد استفاده حمله‌کنندگان سایبری را شناسایی و دسته‌بندی می‌کند [۱، ۱۰]:

(۱) تاکتیک‌ها [2]: تاکتیک‌ها معرف دستورالعمل‌های کلی هستند که حمله‌کنندگان برای رسیدن به اهداف خود استفاده می‌کنند. نمونه‌هایی از تاکتیک‌ها شامل «استخراج اطلاعات» و «تخریب» می‌شوند.
(۲) تکنیک‌ها [3]: تکنیک‌ها معرف جزئیات عملیاتی هستند که حمله‌کنندگان برای اجرای تاکتیک‌ها انجام می‌دهند. هر تکنیک می‌تواند توسط یک یا چند تاکتیک مورد استفاده قرار گیرد. به عنوان‌مثال، تکنیک «فیشینگ» یکی از روش‌هایی است که حمله‌کنندگان ممکن است برای اجرای تاکتیک «حمله‌های هویتی» استفاده کنند.
(۳) ماتریس ATT&CK: این چارچوب به صورت یک ماتریس سازمان‌یافته است که تاکتیک‌ها و تکنیک‌ها را در قالب دسته‌ها و زیر دسته‌ها نمایش می‌دهد. این ماتریس از دو بُعد «تاکتیک» و «پلتفرم» تشکیل شده است که به تیم‌های امنیتی کمک می‌کند تا الگوها و روش‌های حمله را به‌خوبی درک کرده و به‌طور مؤثرتری از سیستم‌های خود محافظت نمایند.
(۴) استفاده در تحلیل امنیتی: از این چارچوب به عنوان یک ابزار تحلیلی برای بررسی حملات گذشته، شناسایی الگوهای حمله و تدوین راهبردهای بهبود امنیت سیستم استفاده می‌شود. تیم‌های امنیتی می‌توانند از این چارچوب برای افزایش آگاهی از تهدیدات سایبری و بهبود قابلیت‌های دفاعی خود بهره‌برداری نمایند.

در شکل ۲ نمایی از چرخه تکامل تشخیص تهدید توسط این چارچوب نشان داده شده است.

بر اساس این مدل، سازمان قادر خواهد بود تا سیاست‌های امنیتی مناسب را تدوین و عملیاتی نموده و برنامه‌هایی را برای مقابله با حملات سایبری ارائه دهد. در این فرآیند، انتخاب و پیاده‌سازی ابزارهای مناسب برای تشخیص و پاسخ به حملات نیز بسیار حائز اهمیت است. این مدل به سازمان‌ها اجازه می‌دهد تا با توجه به تهدیدات فعلی و مخاطرات آینده، بهبودهای لازم را در بخش‌های مختلف امنیتی خود اعمال کنند و عملکرد امنیتی خود را ارتقاء بخشند.

[1] Adversarial Tactics, Techniques, and Common Knowledge
[2] Tactics
[3] Techniques



شکل ۲. تشخیص تهدید با چارچوب MITRE ATT&CK

۲.۳ چارچوب مدل الماس

چارچوب مدل الماس[1] معرف یک مدل تحلیلی در زمینه شواهد تهدید است که برای درک بهتر حملات سایبری و روابط بین عوامل مختلف در یک حمله مورد استفاده قرار می‌گیرد. این چارچوب توسط کریس زینکس ارائه شده است و بر مبنای چهار جنبه اصلی مشارکت‌کنندگان[2]، ابزارها[3]، زیرساخت‌ها[4] و توازن[5]، تحلیل خود را انجام می‌دهد [۱۱، ۱۲]:

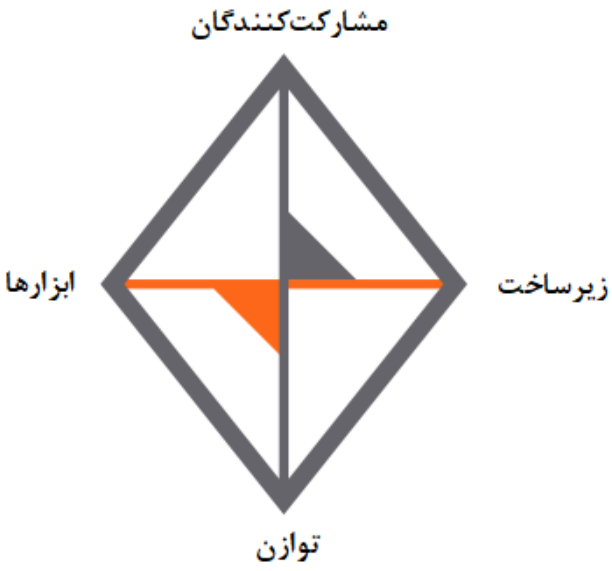
(۱) مشارکت‌کنندگان: این موضوع به شناسایی و تحلیل فرد یا گروهی می‌پردازد که در حمله سایبری دخیل هستند. این مفهوم شامل هکرها، گروه‌های سایبری و یا حتی افراد داخلی سازمان می‌شود. تحلیل مشارکت‌کنندگان کمک می‌کند تا دلایل و هدف حمله روشن شود.

(۲) ابزارها: در این حوزه، ابزارها و تکنیک‌هایی مورد بررسی قرار می‌گیرند که در حمله استفاده می‌شوند. این مفهوم شامل نرم‌افزارهای مخرب، اِسکریپت‌های حمله و یا تکنیک‌های خاصی است که مهاجمان از آن بهره می‌برند.

(۳) زیرساخت: این حوزه به مطالعه زیرساخت‌هایی می‌پردازد که مهاجمان برای انجام حمله خود به کار می‌برند. این مفهوم شامل سرورها، دامنه‌های اینترنتی و یا سایر زیرساخت‌های مورد استفاده در حمله است.

(۴) توازن: این موضوع نقش و ارتباط بین جنبه‌های قبلی را بررسی می‌کند و به تحلیل تعادل مابین مشارکت‌کنندگان، ابزارها و زیرساخت‌ها پرداخته و اهمیت توازن اجزا در انجام موفق یک حمله

[1]Diamond Model [2]Actors [3]Tools [4]Infrastructure [5]Balance



شکل ۳. تشخیص تهدید با چارچوب مدل الماس

را نشان می‌دهد.

با توجه به این چهار جنبه، چارچوب مدل الماس به تیم‌های امنیتی کمک می‌کند تا با دقت بیشتری به تحلیل حملات سایبری بپردازند و بهبودهای مؤثرتری را در سایت‌ها و راهبردهای امنیتی خود ایجاد کنند. در شکل ۳ نمایی از چرخه تکامل تشخیص تهدید توسط این چارچوب نمایش داده شده است.

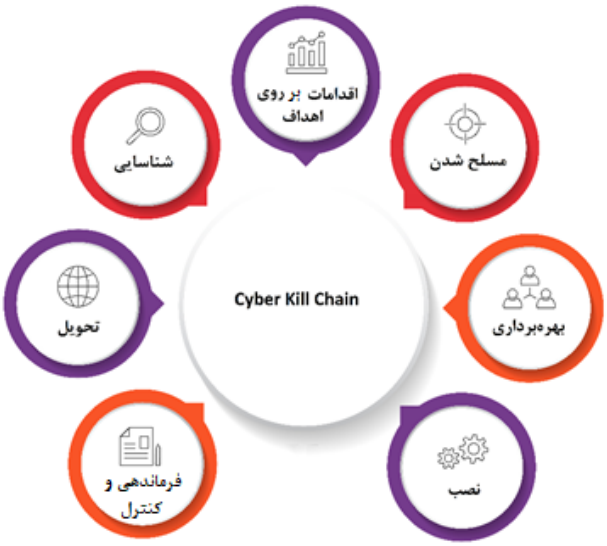
پیاده‌سازی چارچوب مدل الماس در یک سازمان نیازمند شناسایی و بررسی عوامل مختلفی است که در حملات سایبری به ایفای نقش می‌پردازند. بر اساس این مدل، سازمان‌ها می‌توانند برای هر بُعد داده‌های مربوطه را جمع‌آوری، تحلیل و ارزیابی کنند. سازمان با بهره‌گیری از این مدل می‌تواند اقدامات دفاعی خود را به شکلی هوشمندانه تقویت نموده و شرایط امنیت سایبری خود را بهبود بخشد.

۳.۳ چارچوب Cyber Kill Chain

چارچوب Cyber Kill Chain معرف یک مدل تحلیلی است که توسط شرکت لاکهید مارتین ارائه شده است. این چارچوب به‌منظور توصیف مراحل مختلف یک حمله سایبری و فهم بهتر فرآیند حمله توسط مهاجمان به کار می‌رود. این چارچوب متشکل از یک زنجیره مراحل است که هرکدام نقش خاصی را در حمله دارند. مراحل اصلی این چارچوب به شرح زیر هستند [۱۳، ۱۴]:

(۱) شناسایی[6]: در این مرحله، مهاجمان اطلاعاتی را جمع‌آوری می‌کنند تا هدف خود و زیرساخت‌های مرتبط با آن را به‌خوبی بشناسند. این اطلاعات شامل اطلاعاتی درباره کارکنان، سیستم‌ها و ساختار شبکه است.

[6]Reconnaissance



شکل ۴. تشخیص تهدید با چارچوب Cyber Kill Chain

(۲) مسلح شدن[1]: در این مرحله، مهاجمان از اطلاعاتی که در مرحله قبل جمع‌آوری کردند، برای ایجاد ابزارها یا حملات سایبری استفاده می‌کنند. این ابزارها شامل بدافزارها یا نرم‌افزارهای مخرب است.

(۳) تحویل[2]: در این مرحله، ابزارهای مخرب به سیستم هدف انتقال داده می‌شوند. این مرحله از طریق ایمیل‌های فریبنده، وب‌سایت‌های متعلق به مهاجم و یا سایر راه‌های انتقال اطلاعات انجام می‌شود.

(۴) بهره‌برداری[3]: در این مرحله، مهاجمان از آسیب‌پذیری‌ها یا ضعف‌های امنیتی استفاده می‌کنند تا به سیستم وارد شوند. این مرحله شامل بهره‌برداری از آسیب‌پذیری‌های نرم‌افزاری است.

(۵) نصب[4]: در این مرحله، مهاجمان ابزارهای مخرب را در سیستم هدف نصب می‌کنند تا بتوانند فعالیت‌های مختلف را اجرا و کنترل نمایند.

(۶) فرماندهی و کنترل[5]: پس از نصب، مهاجمان نیاز به ایجاد ارتباط با سرورهای کنترل و فرماندهی دارند. این ارتباطات برای ارسال دستورات و دریافت اطلاعات از سیستم هدف استفاده می‌شوند.

(۷) اقدامات بر روی اهداف[6]: در این مرحله، مهاجمان اهداف حمله خود را محقق نموده‌اند. این مرحله شامل دسترسی به اطلاعات حساس، تخریب یا تغییر سیستم‌ها و یا انجام سایر اقدامات مخرب است.

در شکل ۴ نمایی از چرخه تکامل تشخیص تهدید توسط این چارچوب نشان داده شده است.

پیاده‌سازی چارچوب Cyber Kill Chain به سازمان این امکان را می‌دهد تا بهترین راهبردها را برای مقابله با تهدیدات سایبری اتخاذ نماید. این چارچوب به سازمان کمک می‌کند تا مراحل مختلف حمله سایبری را شناسایی و تحلیل نموده و در پاسخ به آن‌ها اقدامات مؤثری را پیش‌بینی و عملیاتی نماید. با اجرای این چارچوب، سازمان می‌تواند از مکانیسم‌های دفاعی مؤثر بهره‌برداری نماید و آگاهی خود را در مورد تهدیدات سایبری افزایش دهد. به‌طورکلی اجرای چارچوب Cyber Kill Chain در سازمان منجر به افزایش سطح امنیتی، کاهش خسارات ناشی از حملات سایبری و تقویت توانایی‌های مدیریت مخاطرات سایبری می‌شود.

۴.۳ چارچوب امنیت سایبری NIST

همزمان با رشد روزافزون فنّاوری و افزایش پیچیدگی در حوزه امنیت سایبری، چالش‌ها و تهدیدات مرتبط با حفاظت از اطلاعات و سیستم‌های رایانه‌ای به‌شدت افزایش یافته‌اند. در این سناریو، چارچوب امنیت سایبری NIST به عنوان یک ابزار استانداردسازی شده توسط مؤسسه ملی استانداردها و فناوری به سازمان‌ها امکان مدیریت بهینه امنیت سایبری را می‌دهد. این چارچوب با تأکید بر پنج مرحله اصلی از شناسایی تا بازیابی، سازمان‌ها را در فرآیندهای مدیریت امنیت هدایت می‌کند. ارائه رهنمودها از تعریف و شناسایی مخاطرات تا حفاظت، تشخیص، پاسخ به حملات و اصلاح، به سازمان‌ها این امکان را می‌دهد که با توجه به نیازمندی‌ها و شرایط خاص خود، راهبردها و راهکارهای امنیتی مؤثر را انتخاب و عملیاتی نمایند [۱۵].

چارچوب امنیت سایبری NIST، یک ابزار مهم و تأثیرگذار در زمینه مدیریت امنیت سایبری است. این چارچوب بر اساس پنج مؤلفه اصلی سازمان‌دهی شده است:

(۱) شناسایی[7]: این مرحله شامل شناسایی و تعریف منابع، فرآیندها و داده‌های مهم مرتبط با تهدیدات برای سازمان است. شناسایی کمک می‌کند تا سازمان بتواند مخاطرات امنیتی خود را به‌دقت تشخیص داده و با آن‌ها مقابله کند.

(۲) حفاظت[8]: در این مرحله، اقدامات و تدابیری برای حفاظت از سیستم‌ها و داده‌ها اعمال می‌شود. این مرحله شامل استفاده از ابزارهای امنیتی، تدابیر پیشگیری و مواردی از این دست است.

(۳) تشخیص[9]: سازمان در این مرحله سعی در شناسایی زودهنگام حملات و خلاءهای امنیتی دارد. استفاده از ابزارها و روش‌های تشخیصی این اهداف را تسهیل می‌کند.

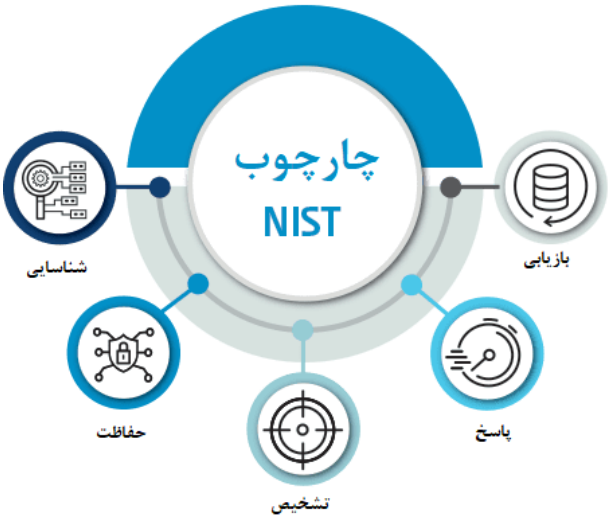
(۴) پاسخ[10]: در صورت وقوع حمله، این مرحله به سازمان کمک می‌کند تا به‌سرعت به حملات پاسخ دهد. این مرحله شامل اقدامات فوری واکنش، انتشار بخشی اطلاعات امنیتی کاربردی و نیز مدیریت بحران است.

(۵) بازیابی[11]: در این مرحله، سازمان اقدام به اصلاح و بازیابی سیستم‌ها و داده‌های خود می‌کند تا به حالت عادی بازگردد. این مرحله شامل برنامه‌ریزی و اجرای روند بازیابی برای کاهش آسیب‌ها می‌شود.

در شکل ۵ نمایی از چرخه تکامل تشخیص تهدید توسط این چارچوب نشان داده شده است.

چارچوب NIST امکان ارزیابی و بهبود فرآیندهای امنیتی را برای سازمان‌ها فراهم می‌آورد و به آن‌ها کمک می‌کند تا بهترین استراتژی‌ها و راهکارها را برای حفظ امنیت دارایی‌های اطلاعاتی در محیط‌های مختلف

[1] Weaponization [2] Delivery [3] Exploitation [4] Installation
[5] Command and Control [6] Actions on Objectives
[7] Identify [8] Protect [9] Detect [10] Respond [11] Recover



شکل ۵. تشخیص تهدید با چارچوب NIST

انتخاب کرده و عملیاتی نمایند.

۵.۳ چارچوب OODA Loop

چارچوب OODA Loop معرف مفاهیم «مشاهده، جهت‌دهی، تصمیم، اقدام [1]» است. این سازوکار یک مدل تصمیم‌گیری اصیل است که در ابتدا برای مقابله با تهدیدات نظامی پیچیده شکل گرفت و اکنون به عنوان یک ابزار چندمنظوره در زمینه‌های مختلف –نظیر امنیت سایبری– به کار گرفته می‌شود. این چارچوب با تمرکز بر مراحل مشاهده، تجزیه و تحلیل سریع اطلاعات، تصمیم‌گیری سریع و اقدام فوری، توانمندی سازمان‌ها و افراد را در مقابله با تهدیدات و وضعیت‌های پویا بهبود می‌بخشد. OODA Loop به عنوان یک ابزار پویا و انعطاف‌پذیر، در مقابله با چالش‌ها و تغییرات سریع محیطی، نقش بسزایی را ایفا می‌کند و سطح توانمندی بالاتری را برای مدیریت واکنش به تهدیدات سایبری فراهم می‌آورد.

چارچوب OODA Loop، یک مدل تصمیم‌گیری است که ابتدا توسط جان بوید ارائه شد که یک افسر نظامی است. این چارچوب در زمینه نظامی برای مقابله با تهدیدها و شرایط پیچیده به کار گرفته می‌شد، اما بعدها به عنوان یک مدل کلی برای تصمیم‌گیری در حوزه‌های مختلف نظیر امنیت سایبری استفاده گردید [۱۶، ۱۷]. مؤلفه‌های سازنده این چارچوب به شرح زیر هستند:

(۱) مرحله مشاهده: در این مرحله، اطلاعات جمع‌آوری می‌شوند. این اطلاعات ممکن است از منابع مختلفی مثل حسگرها، اطلاعات جاری و یا داده‌های مخابراتی به‌دست آمده باشند. هدف این مرحله، به دست آوردن تصویر کامل و دقیقی از وضعیت است.

(۲) مرحله جهت‌دهی: در این مرحله، اطلاعات جمع‌آوری‌شده تحلیل و مقایسه می‌شوند. افراد سعی می‌کنند با در نظر گرفتن اطلاعات، شناخت خود را از موقعیت و تهدیدات به‌روز نمایند. این مرحله شامل

[1] Observe, Orient, Decide, Act

شکل ۶. تشخیص تهدید با چارچوب OODA Loop

درک متغیرهای محیطی، فهم قابلیت‌ها و محدودیت‌ها و تشخیص الگوهای بروز و ظهور تهدیدات سایبری است.

(۳) مرحله تصمیم: پس از تحلیل و ساماندهی اطلاعات، تصمیم‌هایی پیرامون نحوه واکنش به یک وضعیت اتخاذ می‌شود. این تصمیمات شامل انتخاب راهبردها، تعیین اولویت‌ها و تدوین یک طرح عمل امنیت سایبری است.

(۴) مرحله اقدام: در این مرحله، تصمیمات اجرایی شده و اقدامات عملی انجام می‌شود. این مرحله شامل اعمال تغییرات، استفاده از منابع و نیز اعمال کنترل‌ها برای مقابله مؤثر با تهدیدات سایبری است.

در شکل ۶ نمایی از چرخه تکامل تشخیص تهدید توسط این چارچوب نشان داده شده است.

یکی از ویژگی‌های اصلی این چارچوب، سرعت عمل در برابر تغییرات است. با تکرار این چرخه، افراد یا سازمان‌ها توانایی مدیریت واکنش به تهدیدات و وضعیت‌های پیچیده را خواهند داشت. OODA Loop به عنوان یک ابزار منعطف و تطبیقی، در زمینه امنیت سایبری –برای تسریع در امر مقابله با تهدیدات و مواجهه کارآمد با تغییرات محیطی– به کار می‌رود.

۶.۳ چارچوب MISP

چارچوب MISP [2] به عنوان یک ابزار متن‌باز و رایگان به فعالیت می‌پردازد. این چارچوب باهدف جمع‌آوری، اشتراک‌گذاری و تحلیل اطلاعات تهدیدها، در جهت افزایش آگاهی و ارتقاء شیوه مقابله با تهدیدات سایبری به کار گرفته می‌شود. این چارچوب نه‌تنها امکان تبادل

[2] Malware Information Sharing Platform & Threat Sharing

اطلاعات امنیتی را به صورت ایمن بین سازمان‌ها و افراد فراهم می‌آورد، بلکه امکان تحلیل جزئیات تهدیدات، ارتقاء دانش جمعی و تطابق با نیازهای خاص هر محیط سایبری را تأمین می‌نماید. MISP به عنوان یک ابزار چابک و توسعه‌پذیر بر امنیت و حریم خصوصی تأکید دارد. این چارچوب نقشی اساسی را در معماری امنیت سایبری –به‌ویژه در زمینه اشتراک‌گذاری اطلاعات تهدیدها– ایفا می‌کند [۱۸، ۱۹]. مهم‌ترین ویژگی‌ها و عناصر چارچوب MISP به شرح زیر هستند:

(۱) جمع‌آوری اطلاعات تهدیدها: MISP امکان جمع‌آوری اطلاعات مربوط به تهدیدهای امنیتی از منابع مختلف را فراهم می‌آورد. این اطلاعات شامل نمونه‌های بدافزار، آدرس‌های IP مشکوک، الگوهای حمله و سایر جزئیات مرتبط با تهدیدات سایبری است.

(۲) اشتراک‌گذاری اطلاعات: MISP به کاربران خود این امکان را می‌دهد که اطلاعات تهدیدها را با سایر سازمان‌ها، تیم‌ها یا افراد به صورت امن به اشتراک بگذارند. این امکان باعث می‌شود که جوامع امنیت سایبری بتوانند به صورت مشترک از تجربیات و دانش یکدیگر بهره‌مند است.

(۳) تحلیل اطلاعات: MISP امکان ارائه ابزارها و امکانات برای تحلیل اطلاعات تهدیدها را فراهم می‌آورد. این ویژگی شامل امکانات نمایش گرافیکی روابط، تجزیه و تحلیل الگوها و تفسیر داده‌های جمع‌آوری‌شده می‌شود.

(۴) متن‌باز و قابل توسعه: MISP یک پروژه متن باز است که به کاربران اجازه می‌دهد که آن را بر اساس نیازهای خود توسعه دهند و بهبود بخشند. این ویژگی مهم است زیرا به انعطاف و تطابق چارچوب با محیط‌ها و نیازهای مختلف کمک می‌کند.

(۵) امنیت و حریم خصوصی: MISP به‌گونه‌ای طراحی شده است که مسائل امنیتی و حریم خصوصی در آن آدرس‌دهی شده است. این چارچوب امکانات مختلفی را برای مدیریت دسترسی، رمزنگاری اطلاعات و حفظ حریم خصوصی کاربران فراهم می‌آورد.

در شکل ۷ نمایی از تکامل تشخیص تهدید توسط این چارچوب نمایش داده شده است.

۷.۳ تحلیل مقایسه‌ای چارچوب‌ها

براساس روش تحقیقی که در این مطالعه ارائه شده، یک تحلیل و مقایسه جامع از چارچوب‌های شواهد تهدید صورت گرفته است که نتایج آن در قالب جدول ۱ ارائه شده است. در این مطالعه، با بررسی عمیق و مراجعه چندباره به منابع معتبر، ویژگی‌ها، مزایا، محدودیت‌ها و کارکردهای اصلی هر یک از این چارچوب‌ها را بررسی نموده و جنبه‌های بکارگیری هرکدام از چارچوب‌ها بیان شده است. بنابراین امکان تصمیم‌گیری پیرامون چارچوب‌های شواهد تهدید از طریق ارجاع به اطلاعات قابل اعتماد و مطابق با نیازهای سازمان هدف برای ذینفعان در قالب جدول ۱ میسر می‌گردد.

شکل ۷. تشخیص تهدید با چارچوب MISP

۴ پلتفرم‌های مطرح پشتیبان شواهد تهدید

در دنیای امروزی که تهدیدات سایبری به گستردگی و پیچیدگی بالایی دست یافته‌اند، استفاده از ابزارها و پلتفرم‌های شواهد تهدید[1] (TIPs) به‌منظور مقابله با این تهدیدات، امری اساسی و حیاتی برای سازمان‌ها و شرکت‌ها محسوب می‌شود. این پلتفرم‌ها با ارائه امکاناتی چون جمع‌آوری داده، تحلیل شواهد تهدید، گزارش‌دهی و اشتراک‌گذاری اطلاعات، تیم‌های امنیتی را در فرآیند تصمیم‌گیری و پاسخ به تهدیدات سایبری مشارکت می‌دهند [۲۰].

در این فضا، پلتفرم‌های شواهد تهدید به عنوان ابزارهای یکپارچه و جامع، به تیم‌های امنیتی کمک می‌کنند تا از اطلاعات شواهد تهدید به بهترین شکل بهره برده و تصمیماتی پویا و مؤثر در مواجهه با تهدیدات را اجرا نمایند. این پلتفرم‌ها نه‌تنها قابلیت‌های تحلیلی پیشرفته برای شناسایی الگوها و تاکتیک‌های حمله را فراهم می‌آورند، بلکه امکان ادغام با سایر ابزارهای امنیتی را نیز میسر می‌سازند.

انتخاب و استفاده مناسب از این پلتفرم‌ها، یک گام مهم به‌سوی افزایش قابلیت‌های مدیریت تهدیدات و بهبود شرایط امنیت سایبری در سازمان‌ها محسوب می‌شود. در ادامه به مرور و بررسی برخی از پلتفرم‌های شواهد تهدید پرداخته خواهد شد.

۱.۴ پلتفرم Splunk Phantom

Phantom معرف یک پلتفرم خودکارسازی امنیتی پیشرفته است که در جهت بهبود عملکرد تیم‌های امنیت سایبری سازمان‌ها به‌کار گرفته می‌شود. این پلتفرم با ارائه قابلیت‌های گسترده‌ای نظیر خودکارسازی فرآیندها، جمع‌آوری، تجزیه و تحلیل اطلاعات شواهد تهدید و تعامل با سایر

[1] Threat Intelligence Platforms

چارچوب	هدف	مزایا	معایب	موارد استفاده	قابلیت تطبیق
NIST	مدیریت مخاطرات سایبری	استاندارد جهانی، قابل تنظیم	پیاده‌سازی زمان‌بر، نیاز به تخصص	سازمان‌های بزرگ با منابع کافی	بالا
ATT&CK MITRE	دانش‌نامه تکنیک‌ها و تاکتیک‌های حملات	دقیق و جامع، قابل استفاده در شناسایی حملات	نیاز به دانش فنی پیشرفته	تحلیل تکنیک‌های حمله	متوسط
Chain Kill Cyber	شناسایی مراحل حملات سایبری	شناسایی نقاط ضعف، طراحی دفاع‌های چندلایه	محدودیت در حملات پیچیده	دفاع چندلایه	بالا
Loop OODA	تصمیم‌گیری سریع در مواجهه با تهدیدات	سرعت و انعطاف‌پذیری	نیاز به تجربه، مناسب نبودن برای تحلیل‌های بلندمدت	محیط‌های پویا و پیچیده	متوسط
MISP	اشتراک‌گذاری اطلاعات تهدیدات	افزایش همکاری، ابزارهای خودکار	نیاز به اعتماد و همکاری	همکاری بین سازمان‌ها	بالا
مدل الماس	تحلیل تعاملات مابین مهاجم و قربانی، زیرساخت و توانایی‌ها	جامع و قابل فهم، تحلیل عمیق	نیاز به داده‌های دقیق، مناسب نبودن برای تحلیل سریع	تحلیل عمیق تهدیدات	بالا

جدول ۱. مقایسه کلان چارچوب‌های شواهد تهدید

ابزارها، سازمان‌ها را قادر می‌سازد تا با سرعت و کارایی بیشتری به تهدیدات سایبری پاسخ دهند. از ویژگی‌های برجسته Splunk Phantom می‌توان به تجزیه و تحلیل گسترده، رابط کاربری گرافیکی هوش و قابلیت گزارش‌گیری و نمودارسازی اطلاعات اشاره نمود. این پلتفرم از استانداردها و نرم‌افزارهای منبع باز نیز پشتیبانی می‌نماید و امکان اتصال به ابزارهای متنوع امنیتی را به‌سادگی فراهم می‌آورد. با استفاده از Splunk Phantom، سازمان‌ها قادر به ایجاد محیطی هوشمند و کارآمد برای مدیریت و پاسخ به چالش‌های امنیتی سایبری خود خواهند بود [۲۱].

برخی از ویژگی‌ها و قابلیت‌های Splunk Phantom به شرح زیر است:

(۱) خودکارسازی فرآیندها: Splunk Phantom به کاربران این امکان را می‌دهد تا فرآیندهای امنیتی خود را خودکارسازی کنند. این ویژگی شامل تحلیل شواهد تهدید، اجرای اِسکریپت‌ها، ارسال هشدارها و انجام اقدامات دیگر مرتبط با امنیت سایبری است.

(۲) ادغام با منابع شواهد تهدید: این پلتفرم به کاربران این امکان را می‌دهد تا اطلاعات شواهد تهدید را از منابع مختلف جمع‌آوری کنند و در یک محیط متمرکز تجزیه و تحلیل و تجمیع نمایند.

(۳) پشتیبانی از بسترهای منبع باز: Splunk Phantom از استانداردها و بسترهای منبع‌باز پشتیبانی می‌کند. این ویژگی به کاربران این امکان را می‌دهد که از ابزارهای متن‌باز برای توسعه و ادغام پیشرفته‌تر با این پلتفرم استفاده نمایند.

(۴) تجزیه و تحلیل گسترده: Splunk Phantom قابلیت تجزیه و تحلیل گسترده‌ای از داده‌های امنیتی را فراهم می‌آورد تا تصمیمات هوشمندانه‌تری ـ بر اساس اطلاعات به‌دست آمده ـ اتخاذ شوند.

(۵) تعامل با سایر ابزارها: این پلتفرم قابلیت اتصال به سایر ابزارهای امنیتی ـ نظیر فایروال‌ها، آنتی‌ویروس‌ها و سایر سیستم‌های امنیتی ـ را دارد.

(۶) رابط کاربری گرافیکی: اِسپلانک فانتوم از یک رابط کاربری گرافیکی قوی استفاده می‌کند که به کاربران این امکان را می‌دهد تا به‌راحتی فرآیندها و اقدامات امنیتی را پیکربندی و مدیریت نمایند.

(۷) گزارش‌گیری و نمودارسازی: این پلتفرم اطلاعات تجزیه و تحلیل شده را در قالب گزارش‌ها و نمودارها ارائه می‌دهد تا به کاربران کمک کند تا شرایط را درک و تصمیمات بهتری را در مورد شرایط امنیت سایبری سازمان اتخاذ نمایند.

اِسپلانک فانتوم با ترکیب و تجزیه و تحلیل شواهد تهدید، خودکارسازی فرآیندها و تعامل با سایر ابزارها، به سازمان‌ها کمک می‌کند تا به‌سرعت و با کارایی بالا به تهدیدات سایبری پاسخ دهند.

۲.۴ پلتفرم MISP

MISP به عنوان یک پلتفرم متن‌باز و جامعه‌محور[1] شواهد تهدید، در ارتقاء توانمندی‌های تیم‌های امنیت سایبری نقش بسزایی را ایفا می‌کند. این پلتفرم به کاربران امکان می‌دهد تا اطلاعات مرتبط با تهدیدات را جمع‌آوری و با سایر اعضای جامعه به اشتراک بگذارند. افزایش انطباق و ایجاد دیدگاه جامعه‌محور نسبت به تهدیدات سایبری از دیگر ویژگی‌های این پلتفرم است. با استفاده از استانداردهای معتبری همچون STIX و TAXII، MISP اطلاعات شواهد تهدید را به صورت استانداردسازی شده مدیریت می‌کند. این پلتفرم با ویژگی‌های انعطاف‌پذیری ـ نظیر ایجاد نمودارها و گراف‌ها برای تجسم ارتباطات تهدیدات ـ به کاربران کمک می‌کند تا به بهترین شکل ممکن شرایط امنیتی را درک و تصویرسازی نمایند [۱۸].

برخی از ویژگی‌ها و قابلیت‌های MISP به شرح زیر هستند:

(۱) جامعه‌محور: MISP به عنوان یک پروژه متن‌باز جامعه‌محور طراحی شده است که به کاربران اجازه می‌دهد اطلاعات خود را به اشتراک بگذارند و از تجربیات یکدیگر بهره‌مند شوند.

[1] Community-Driven

(۲) جمع‌آوری و مدیریت اطلاعات شواهد تهدید: MISP قابلیت جمع‌آوری اطلاعات شواهد تهدید از منابع مختلف را فراهم می‌آورد و این اطلاعات را در یک مخزن به اشتراک‌گذاری شده مدیریت می‌کند.
(۳) استانداردسازی اطلاعات: این پلتفرم از استانداردهایی مانند STIX و TAXII برای سازگار نمودن اطلاعات شواهد تهدید و تبادل نظام‌مند آن‌ها استفاده می‌کند.
(۴) پشتیبانی از حجم بالا: MISP به‌خوبی با حجم بالای داده‌ها و اطلاعات شواهد تهدید سازگاری دارد و قابلیت مدیریت و تجزیه و تحلیل این حجم از اطلاعات را فراهم می‌آورد.
(۵) انعطاف‌پذیری در تعریف اطلاعات: کاربران می‌توانند قوانین و تعریف‌های خود را برای اطلاعات شواهد تهدید در این پلتفرم تعریف کرده و به دلخواه تنظیمات مختلفی را برای تحلیل اطلاعات تعیین نمایند.
(۶) پیش‌نمایش گرافیکی اطلاعات: MISP قابلیت ایجاد نمودارها و گراف‌ها برای نمایش ارتباطات میان اطلاعات شواهد تهدید را دارد. این قابلیت به کاربران در درک بهتر ارتباطات و الگوهای حمله کمک می‌کند.
(۷) پشتیبانی از API: این پلتفرم از API پیشرفته برای اتصال به سایر ابزارها و سیستم‌ها استفاده می‌کند و به کاربران این امکان را می‌دهد تا به‌راحتی با دیگر ابزارهای امنیتی تعامل نمایند.
(۸) پشتیبانی از گزارش‌گیری: MISP قابلیت تولید گزارش‌های جامع در مورد اطلاعات شواهد تهدید را دارد و از این ویژگی برای پشتیبانی از تیم‌های مدیریت امنیت و تصمیم‌گیری مبتنی بر داده در سازمان استفاده می‌کند.

MISP به دلیل مشارکت بالای ائتلاف‌های امنیتی، انعطاف‌پذیری و نیز قابلیت گسترش کاربرد با استفاده از API به یکی از پلتفرم‌های محبوب در حوزه شواهد تهدید تبدیل شده است.

۳.۴ پلتفرم ThreatConnect

ThreatConnect معرف یک پلتفرم جامع شواهد تهدید است که به تیم‌های امنیت سایبری امکان جمع‌آوری، تحلیل و مدیریت اطلاعات شواهد تهدید را می‌دهد. این پلتفرم از ویژگی‌هایی چون جمع‌آوری اطلاعات شواهد تهدید از منابع مختلف، اجرای وظایف امنیتی مبتنی بر اطلاعات شواهد تهدید، تحلیل گرافیکی، تصمیم‌گیری، ادغام با ابزارهای دیگر، مدیریت تیم و همکاری مؤثر، پشتیبانی از استانداردهای شواهد تهدید، تحلیل خودکار تهدید و نیز ایجاد ارتباطات مؤثر بین اطلاعات شواهد تهدید و سایر ابزارها برخوردار است. این ویژگی‌ها باعث می‌شود ThreatConnect به یک ابزار کامل و قدرتمند در جهت مقابله با تهدیدات سایبری و بهبود راهبردهای امنیتی سازمان‌ها تبدیل شود [۲۲].

برخی از ویژگی‌ها و قابلیت‌های ThreatConnect به شرح زیر هستند:

(۱) جمع‌آوری و تجزیه و تحلیل اطلاعات شواهد تهدید: ThreatConnect امکان جمع‌آوری اطلاعات شواهد تهدید از منابع مختلف –ازجمله اطلاعات مشاهده شده عمومی، موارد اشتراک‌گذاری شده ائتلاف‌ها و سایر پلتفرم‌های شواهد تهدید– را فراهم می‌آورد.
(۲) انجام وظایف امنیتی: این پلتفرم امکان اجرای اقدامات امنیتی مبتنی بر اطلاعات شواهد تهدید را فراهم می‌آورد. ایجاد قوانین تشخیص، اعمال پارامترهای امنیتی و خودکارسازی فرآیندهای امنیتی از عمده این اقدامات محسوب می‌شوند.
(۳) تحلیل گرافیکی: قابلیت تحلیل گرافیکی و نمایش ارتباطات بین محصولات شواهد تهدید به شکل‌های گرافیکی موجب درک بهتر تهدیدات و ارتباطات موجود بین آن‌ها می‌شود.
(۴) تصمیم‌گیری: ThreatConnect از طریق استفاده از اطلاعات شواهد تهدید به تیم‌های امنیتی کمک می‌کند تا تصمیمات کارآمدتری را در مورد پاسخ به تهدیدات سایبری اتخاذ نمایند.
(۵) ادغام با ابزارهای دیگر: این پلتفرم قابلیت تعامل با سایر ابزارهای امنیتی را فراهم می‌آورد تا اطلاعات به صورت مؤثرتری با سایر ابزارها به اشتراک گذاشته شوند.
(۶) مدیریت تیم و همکاری: ThreatConnect امکان مدیریت تیم‌ها و همکاری مؤثر مابین اعضای تیم امنیتی را فراهم می‌آورد تا افراد مختلف بتوانند در کنار یکدیگر به تجزیه و تحلیل اطلاعات شواهد تهدید بپردازند.
(۷) پشتیبانی از استانداردهای مختلف: ThreatConnect از استانداردهای مختلف شواهد تهدید –نظیر STIX و TAXII –پشتیبانی می‌کند.
(۸) تحلیل خودکار تهدید: این پلتفرم دارای قابلیت تحلیل خودکار تهدیدات است که موجب کاهش زمان تصمیم‌گیری و واکنش سریع به تهدیدات امنیت سایبری می‌شود.

هر یک از ویژگی‌های فوق باعث می‌شود تا ThreatConnect به یک ابزار کارآمد و پرکاربرد برای مدیریت شواهد تهدید در سازمان‌ها تبدیل شود.

۴.۴ پلتفرم Anomali ThreatStream

Anomali ThreatStream معرف یک پلتفرم شواهد تهدید است که به تیم‌های امنیتی کمک می‌کند تا اطلاعات شواهد تهدید را جمع‌آوری و تجزیه و تحلیل کنند و بر اساس آن‌ها تصمیمات امنیتی مناسب را اتخاذ نمایند. این پلتفرم از منابع متنوعی –نظیر اطلاعات اشتراک‌گذاری شده جمعی، رویدادهای ثبت‌شده و سایر منابع داده‌ای– استفاده می‌کند تا اطلاعات شواهد تهدید را جمع‌آوری نماید. Anomali ThreatStream ارائه‌گر قابلیت‌های تجزیه و تحلیل پیشرفته شواهد تهدید، اشتراک‌گذاری اطلاعات با سایر سازمان‌ها، پیگیری زمانی تهدیدات، ادغام با سایر ابزارهای امنیتی و نیز تولید گزارش‌های تحلیلی است [۲۳].

برخی از ویژگی‌ها و قابلیت‌های Anomali ThreatStream به شرح زیر هستند:

(۱) جمع‌آوری اطلاعات شواهد تهدید: Anomali ThreatStream از منابع مختلف هوش –نظیر اطلاعات اشتراک‌گذاری شده جمعی (STIX/TAXII)، اطلاعات پیرامون تهدیدهای جاری، رویدادهای ثبت‌شده و نیز سایر منابع– برای جمع‌آوری و ترکیب اطلاعات جمع‌آوری شده از تهدیدات سایبری استفاده می‌کند.
(۲) تجزیه و تحلیل شواهد تهدید: این پلتفرم قابلیت تجزیه و تحلیل داده‌های شواهد تهدید را با استفاده از الگوریتم‌ها و ابزارهای تجزیه و تحلیل پیشرفته فراهم می‌آورد تا مدیران امنیت بتوانند الگوها و رفتارهای تهدید سایبری را شناسایی نمایند.
(۳) هماهنگی و همکاری: Anomali ThreatStream امکان اشتراک‌گذاری اطلاعات شواهد تهدید را با سایر سازمان‌ها و جوامع شواهد تهدید فراهم می‌آورد. این ویژگی به سازمان‌ها این امکان را می‌دهد تا از تجربیات دیگران بهره‌مند شوند و سطح هماهنگی در مقابله با تهدیدات سایبری را افزایش دهند.
(۴) پیگیری تهدیدات: این پلتفرم امکان پیگیری تهدیدات به صورت زمان‌بندی‌شده یا زنده را فراهم می‌آورد تا تیم‌های امنیتی بتوانند به‌سرعت نسبت به تهدیدات سایبری واکنش نشان دهند.
(۵) ادغام با سایر ابزارهای امنیتی: Anomali ThreatStream به تعامل با سایر ابزارهای امنیتی نظیر SIEM، فایروال‌ها و سایر سازوکارهای امنیتی کمک می‌نماید.
(۶) پشتیبانی از استانداردها: این پلتفرم استانداردهای امنیتی مهم مانند STIX و TAXII را پشتیبانی می‌کند. این امر به اشتراک‌گذاری و تبادل اطلاعات جمع‌آوری شده از تهدیدات سایبری با سایر سیستم‌ها کمک می‌نماید.
(۷) گزارش‌گیری: Anomali ThreatStream امکان تولید گزارش‌های تحلیلی بر اساس اطلاعات شواهد تهدید را دارد که تصمیم‌گیری‌های امنیتی مدیران سازمان را پشتیبانی می‌نماید.

از آنجایی که حوزه شواهد تهدید پیوسته در حال توسعه و تغییر است، پلتفرم‌هایی مانند Anomali ThreatStream تلاش می‌کنند تا با ارائه ویژگی‌های جدید و به‌روزرسانی‌های مداوم، با نیازهای روزافزون تیم‌های امنیتی هماهنگ شوند.

۵.۴ پلتفرم EclecticIQ

پلتفرم EclecticIQ معرف یک سازوکار شواهد تهدید تخصصی است که باهدف تقویت قابلیت‌های سازمان‌ها در زمینه مدیریت شواهد تهدید، جمع‌آوری اطلاعات و نیز تحلیل تهدیدها طراحی شده است. این پلتفرم ارائه‌دهنده ابزارهای پیشرفته تجزیه و تحلیل داده‌های شواهد تهدید است و قابلیت ادغام با ابزارهای امنیتی مختلف را دارد. از امکانات مهم آن می‌توان به جمع‌آوری اطلاعات شواهد تهدید از منابع متنوع، به اشتراک‌گذاری اطلاعات امنیتی در سازمان یا با شرکای خارجی و ارائه تحلیل‌های پیشرفته برای تشخیص و پیش‌بینی تهدیدات امنیت سایبری اشاره نمود. با بهره‌گیری از استانداردهای شواهد تهدید و فنّاوری‌های مدرن، پلتفرم EclecticIQ به سازمان‌ها کمک می‌کند تا به صورت کامل به چالش‌های امنیت سایبری خود پاسخ دهند و به‌طور فعال وضعیت مدیریت مخاطرات امنیت سایبری مجموعه را بهبود بخشند [۲۴].

برخی از ویژگی‌ها و قابلیت‌های پلتفرم EclecticIQ به شرح زیر هستند:

(۱) جمع‌آوری اطلاعات شواهد تهدید: EclecticIQ امکان جمع‌آوری اطلاعات شواهد تهدید از منابع گوناگون –نظیر منابع عمومی، تأمین‌کنندگان اطلاعات شواهد تهدید و مراجع مختلف دیگر– را فراهم می‌آورد.
(۲) تجزیه و تحلیل شواهد تهدید: این پلتفرم ابزارهای پیشرفته تجزیه و تحلیل داده‌های شواهد تهدید را فراهم می‌آورد و به تیم‌های امنیت سایبری این امکان را می‌دهد تا تهدیدات امنیت سایبری را به‌دقت بررسی و تحلیل کنند.
(۳) اشتراک‌گذاری اطلاعات شواهد تهدید: پلتفرم EclecticIQ امکان به اشتراک‌گذاری اطلاعات شواهد تهدید با سایر سازمان‌ها یا اعضای یک ائتلاف اطلاعات شواهد تهدید را به صورت امن و کارآمد فراهم می‌آورد.
(۴) ادغام با ابزارهای امنیتی: این پلتفرم قابلیت تعامل با ابزارهای امنیتی دیگر را دارد تا اطلاعات تهدیدات سایبری را به سیستم‌ها و ابزارهای امنیتی دیگری منتقل کند که در محیط سازمان استفاده می‌شوند.
(۵) پشتیبانی از استانداردهای شواهد تهدید: پلتفرم EclecticIQ با استفاده از استانداردهای معتبر در حوزه شواهد تهدید –نظیر STIX و TAXII– اطلاعات را به صورت استاندارد و قابل تبادل سازمان‌دهی می‌کند.
(۶) تحلیل تهدیدهای پیشرفته: این پلتفرم از تحلیل تهدیدهای پیشرفته، ابزارهای تجزیه و تحلیل شواهد تهدید و هوش مصنوعی برای تشخیص و پیش‌بینی نسل جدید تهدیدات امنیت سایبری بهره می‌برد.
(۷) مدیریت اطلاعات شواهد تهدید: این پلتفرم امکان مدیریت و ذخیره‌سازی اطلاعات شواهد تهدید به صورت سازمان‌دهی شده و امن را فراهم می‌آورد.
(۸) پیش‌بینی تهدیدات: پلتفرم EclecticIQ با بهره‌گیری از فنّاوری‌های روز، امکان پیش‌بینی تهدیدات و مشکلات امنیتی را فراهم می‌آورد.

این پلتفرم به عنوان یک ابزار جامع برای تقویت توانایی‌های شواهد تهدید و مدیریت مخاطرات سایبری در سازمان‌ها شناخته می‌شود.

۶.۴ تحلیل مقایسه‌ای پلتفرم‌ها

با توجه به اهمیت روزافزون امنیت سایبری و افزایش تنوع و دامنه حملات سایبری، استفاده از پلتفرم‌های شواهد تهدید به عنوان اساسی برای شناسایی، پیشگیری و مدیریت تهدیدات سایبری محسوب می‌شود. مبتنی بر مطالعات انجام‌شده، جدول ۲ ارائه‌گر نتایج مقایسه کلان جهت معرفی و بررسی این پلتفرم‌ها است این‌کار با هدف ارائه رهنمودهایی

ویژگی / پلتفرم	Splunk Phantom	MISP	ThreatConnect	Anomali ThreatStream	EclecticIQ
امکانات اتوماسیون فرآیندها و عملیات	بله	خیر	بله	بله	خیر
تحلیل مبتنی بر تکنیک‌های هوش مصنوعی	بله	خیر	بله	بله	بله
پیشبرد اقدامات پیشگیرانه امنیت سایبری	بله	خیر	بله	بله	خیر
ارتباط با API ابزارهای خارجی	بله	بله	بله	بله	بله
مدیریت حوادث امنیت سایبری	بله	خیر	بله	بله	بله
قابلیت تعامل و هماهنگی با سایر ابزارها	بله	بله	بله	بله	بله
قابلیت انتقال داده‌های امنیت سایبری	بله	بله	بله	بله	بله
قابلیت تحلیل گرافی و ارتباطات داده‌ای	بله	خیر	بله	بله	بله
قابلیت مشارکت و تعامل انسانی	بله	بله	بله	بله	بله

جدول ۲. مقایسه کلان پلتفرم‌های شواهد تهدید

به مدیران و تصمیم‌گیران امنیت سایبری سازمان‌ها برای انتخاب بهترین ابزار برای تامین نیازهای امنیتی مجموعه است.

مطالعه عمیق و نظام‌مند هر یک از پلتفرم‌های شواهد تهدید براساس بررسی موردی چندگانه و یک تحلیل مقایسه‌ای جامع و منطقی انجام شده و در این راه از تجربه کاربری واقعی نیز استفاده گردیده است.

۵ استانداردهای پشتیبان شواهد تهدید

در فضای سایبری، اطلاعات شواهد تهدید به عنوان یک ابزار حیاتی برای مقابله با تهدیدات سایبری و افزایش سطح امنیت به ایفای نقش می‌پردازد. در این زمینه الگوریتم‌های ذخیره‌سازی اطلاعات و سازوکارهای به اشتراک‌گذاری اطلاعات معرف ابزارهای اساسی شواهد تهدید هستند. استفاده از استانداردها و فناوری‌های مدرن، سازمان‌ها را قادر می‌سازد تا اطلاعات شواهد تهدید را به صورت کارآمد و امن تولید، منتقل، ذخیره و به اشتراک بگذارند. این اقدامات نه‌تنها به بهبود قابلیت تشخیص و پاسخ به تهدیدات سایبری کمک می‌کنند، بلکه همکاری بین سازمان‌ها را تقویت و امنیت سایبری را به سطح جدیدی ارتقاء می‌دهند. به‌طورکلی، استانداردها و پروتکل‌ها در این حوزه به سازمان‌ها کمک می‌کنند تا اطلاعات شواهد تهدید را به امانت و با استفاده از روش‌های استاندارد منتقل کرده و در سیستم‌هایی با امنیت بالا ذخیره نمایند. این اقدامات نه‌تنها امکان دریافت بهتر اطلاعات را فراهم می‌آورند بلکه به ارتقاء همکاری و تبادل سریع اطلاعات برای مقابله با تهدیدات سایبری کمک می‌کنند.

در ادامه به بررسی مهم‌ترین این استانداردها پرداخته خواهد شد.

۱.۵ پروتکل‌های اختصاصی شواهد تهدید

در فضای امنیت سایبری، تحلیلگران امنیتی باید با استفاده از انواع استانداردها، فرآیندها و پروتکل‌های معتبر برای جمع‌آوری، تحلیل، توصیف و انتشار اطلاعات شواهد تهدید به صورت هماهنگ عمل نمایند.

یک سیستم شواهد تهدید باید قادر باشد این استانداردها را با سایر بخش‌های صنعت امنیت سایبری هماهنگ نماید و از سازگاری بخش‌های مختلف این صنعت بهره‌مند شود. لازم به ذکر است اکثر استانداردهای مرتبط با رویکرد شواهد تهدید تعریف‌های گسترده‌ای از مفاهیم مورد نیاز برای توسعه مدل‌های مرجع شواهد تهدید را فراهم نمی‌آورند؛ ازاین‌رو، پروتکل‌های اختصاصی شواهد تهدید بر روی روش‌های خاص مرتبط با شواهد تهدید (مانند اشتراک‌گذاری اطلاعات شواهد تهدید) تمرکز داشته و آن‌ها را استانداردسازی می‌کنند. پروتکل‌های اختصاصی شواهد تهدید در قالب جدول ۳ ارائه شده است.

TLP	Cyber Kill Chain	CPE	YARA
TAXII	CybOX	MAEC	CWE
IODEF	STIX	CAPEC	CVE
VERIS	Diamond Model	ATT&CK	CCE

جدول ۳. پروتکل و استانداردهای اختصاصی شواهد تهدید

۲.۵ استفاده از زبان‌های مشترک در توصیف تهدیدات

با گسترش استفاده از فناوری‌های اطلاعات و نفوذ بیشتر فضای سایبری، تهدیدات جدیدی در حوزه امنیت به وجود آمده است. در این سناریو، نیاز به استانداردسازی و اشتراک اطلاعات مربوط به تهدیدات بین سازمان‌ها و افراد حرفه‌ای حوزه امنیت به‌شدت احساس می‌شود. به عنوان یک پاسخ به این نیاز، استفاده از زبان‌های مشترک در توصیف تهدیدات به عنوان یک راهکار مؤثر برای ایجاد توافق و اطلاع‌رسانی درباره تهدیدات سایبری به میان آمده است.

استفاده از زبان‌های مشترک در توصیف تهدیدات، به عنوان یک سازوکار استانداردسازی در حوزه امنیت سایبری، اشتراک داده‌ها، تبادل اطلاعات و تدوین گزارش‌ها در بین سازمان‌ها و محققان امنیت مطرح است. این زبان‌ها به صورت معمول بر اساس فرهنگ و استانداردهای

صنعتی ایجاد می‌شوند تا ارتباطات و تفاهم بین افراد و سازمان‌ها را تسهیل نمایند. در ادامه به برخی از مزایای استفاده از زبان‌های مشترک در توصیف تهدیدات اشاره می‌شود [۲۵]:

(۱) یکپارچگی و توافق: استفاده از یک زبان مشترک (مانند STIX یا TAXII) باعث می‌شود که اطلاعات مربوط به تهدیدات به یک فرمت استاندارد تبدیل شود و از به‌کارگیری فرمت‌ها و ساختارهای مختلف در این زمینه جلوگیری به عمل آید.
(۲) تسهیل ارتباطات: زبان‌های مشترک به محققان و افراد حرفه‌ای امنیت اجازه می‌دهند که با استفاده از یک زبان استاندارد، اطلاعات و داده‌های مربوط به تهدیدات را به اشتراک بگذارند و با همکاری بیشتر، به طراحی راهکارهای بهتر و مؤثرتر پرداخته و نسبت به جلوگیری از حملات سایبری اقدام نمایند.
(۳) توجه بیشتر به جزئیات: با استفاده از زبان‌های مشترک، می‌توان به جزئیات مهم‌تری از تهدیدات سایبری توجه نمود و اطلاعات را در یک فرمت ساختاری و قابل‌تحلیل قرار داد که به بررسی و تحلیل مؤثرتر این اطلاعات کمک می‌کند.
(۴) توسعه بیشتر: با استفاده از زبان‌های مشترک امکان توسعه ابزارها و سامانه‌هایی فراهم می‌شود که برای جمع‌آوری، تحلیل و انتقال اطلاعات مربوط به تهدیدات سایبری استفاده می‌شوند. این ابزارها می‌توانند از رویکردها و الگوهای استاندارد برای ارائه خدمات مبتنی بر شواهد تهدید استفاده کنند.

۳.۵ استاندارد STIX

در عصری که فناوری به‌سرعت در حال پیشرفت است و فضای سایبری به‌طور گسترده‌تری وارد زندگی‌های ما انسان‌ها می‌شود، حفظ امنیت اطلاعات از اهمیت فوق‌العاده‌ای برخوردار است. سازمان‌ها و شرکت‌ها با چالش‌های جدیدی روبرو هستند که ازجمله آن‌ها می‌توان به تهدیدات سایبری اشاره نمود. در این شرایط، نیاز به مدیریت و پاسخگویی سریع به این تهدیدات امنیتی بیش‌ازپیش احساس می‌شود. در این راستا، اطلاعات امنیتی به عنوان یکی از دارایی‌های بسیار مهم در هر سازمان باید به‌طور مؤثر مدیریت و تحلیل شوند تا بتوان بهترین راهکارها را برای مقابله با تهدیدات مدنظر قرار داد. بنابراین استفاده از استانداردها و فرمت‌های مناسب برای تبادل اطلاعات امنیتی در این فضا از اهمیت بسیار زیادی برخوردار است. یکی از این استانداردها، STIX است که به شناسایی، توصیف و به اشتراک‌گذاری اطلاعات ساختارمند مربوط به تهدیدات سایبری می‌پردازد. در ادامه به بررسی نقش و اهمیت STIX در چرخه مدیریت تهدیدات سایبری و امنیت اطلاعات پرداخته خواهد شد [۲۶].

استاندارد STIX جهت تبادل اطلاعات مربوط به تهدیدات سایبری به شکلی نظام‌مند بکار گرفته می‌شود. این استاندارد توسط کنسرسیوم تدوین استانداردهای اطلاعاتی ساخت‌یافته [1] (OASIS) توسعه داده شده است و برای تبادل اطلاعات مربوط به حملات، تهدیدات، زمان‌بندی‌های حملات، منابع مشکوک، شواهد دیجیتالی و سایر داده‌های امنیتی بکار می‌رود [۲۶].

اهداف اصلی استاندارد STIX به شرح زیر هستند:

(۱) توصیف متناسب با استاندارد: ایجاد یک ساختار استاندارد برای توصیف اطلاعات امنیتی و تهدیدات سایبری.
(۲) قابلیت انتقال: امکان انتقال و به اشتراک‌گذاری اطلاعات مابین سیستم‌های مختلف امنیتی با استفاده از یک فرمت مشترک.
(۳) قابلیت تحلیل و پردازش: ایجاد یک فرمت که بتواند توسط ابزارهای مختلف تحلیلی و پردازشی مورد استفاده قرار گیرد.
(۴) کاربردهای گسترده: قابلیت استفاده در محیط‌های مختلف امنیتی برای تبادل اطلاعات امنیتی.

STIX از یک ساختار داده‌ای نظام‌مند استفاده می‌کند که شامل اجزای مختلفی نظیر حملات، تهدیدات، منابع، شواهد، اقدامات و ... است. این ساختار داده‌ای به صورت XML و JSON تعریف شده است و امکان تعریف اطلاعات بر اساس نیازهای مختلف امنیتی را فراهم می‌آورد.

۴.۵ استاندارد TAXII

استاندارد TAXII برای ارتباط بین سیستم‌های امنیتی مختلف جهت انتقال اطلاعات مربوط به تهدیدات سایبری کاربرد دارد. این استاندارد توسط کنسرسیوم OASIS توسعه داده شده است. TAXII از طریق تعریف پروتکل‌ها و پیغام‌های مختلف، اجازه می‌دهد تا اطلاعات امنیتی به صورت خودکار و امن بین سیستم‌های مختلف به اشتراک گذاشته شود [۲۷]. این پروتکل از مزایای زیر برخوردار است:

(۱) اطلاعات متنوع: TAXII اجازه می‌دهد تا اطلاعات متنوعی مانند شاخص‌های تهدید، الگوهای حمله، مشکوک بودن فایل‌ها و سایر موارد به اشتراک گذاشته شوند.
(۲) اتصال امن: TAXII از پروتکل‌های امنیتی ـ مانند HTTPS – برای ارتباطات از طریق شبکه اینترنت استفاده می‌کند. بنابراین اطلاعات به صورت رمزنگاری‌شده و امن منتقل می‌شوند.
(۳) استفاده از پیغام‌های معیار: TAXII از پیغام‌های استاندارد ـ مانند STIX– استفاده می‌کند که به صورت ساختارمند اطلاعات تهدیدات سایبری را توصیف می‌نمایند.
(۴) تعامل بین سیستم‌های مختلف: با استفاده از TAXII، سیستم‌های مختلف امنیتی می‌توانند به‌طور خودکار اطلاعات امنیتی را به اشتراک بگذارند. این تبادل اطلاعات امکان مواجهه سریع‌تر با تهدیدات سایبری را میسر می‌سازد.

کلیدی‌ترین هدف TAXII ایجاد یک محیط استاندارد و امن برای اشتراک اطلاعات امنیتی مابین سازمان‌ها و سیستم‌های مختلف است. این امر باعث افزایش کارایی و توانایی‌های سازمانی در مواجهه با تهدیدات امنیت سایبری می‌شود.

[1] Organization for the Advancement of Structured Information Standards

۵.۵ استاندارد CTISS

تهدیدات امنیتی به‌تبع رشد سریع فناوری‌ها و نیز توسعه فضای سایبری بسیار پیچیده و متنوع شده‌اند. تبادل اطلاعات مرتبط با تهدیدات سایبری بین سازمان‌ها و نهادها در مواجهه با این تهدیدات، نقش بسیار مهمی را ایفا می‌کند. در چنین شرایطی، به‌کارگیری استانداردها و پروتکل‌های مشترک به سازمان‌ها کمک می‌کند تا با تهدیدات سایبری به شکل مؤثرتری مقابله نمایند [۲۸].

استاندارد تبادل شواهد تهدید[1] (CTISS) معرف یک مجموعه استانداردها و پروتکل‌هایی است که به‌منظور تسهیل اشتراک اطلاعات تهدیدات سایبری بین سازمان‌ها و مؤسسات ایجاد شده است [۲۹]. این استانداردها و پروتکل‌ها ازجمله سازوکارهای اصلی برای تبادل اطلاعات امنیتی بین سازمان‌ها و نهادها به‌منظور شناسایی، پیش‌بینی و مدیریت تهدیدات سایبری هستند. CTISS هدف اصلی خود را در تسهیل تبادل اطلاعات امنیتی بین سازمان‌ها قرار داده است. این استانداردها شامل مؤلفه‌های زیر است:

(۱) استانداردهای فرمت داده: برای اطلاعاتی که بین سازمان‌ها به اشتراک گذاشته می‌شود، فرمت‌های استانداردی باید تعیین شود تا بتوان اطلاعات را به صورت یکسان و قابل تحلیل به اشتراک گذاشت.
(۲) پروتکل‌های ارتباطی: پروتکل‌هایی که سازمان‌ها برای ارسال و دریافت اطلاعات امنیتی استفاده می‌کنند باید امن و قابل اعتماد باشند تا حفاظت از اطلاعات حساس تضمین شود.
(۳) استانداردهای شناسایی و دسته‌بندی تهدیدات: برای توصیف و دسته‌بندی تهدیدات سایبری به یک شکل منسجم و قابل فهم باید استانداردهای خاصی تعریف شوند.
(۴) رویکردهای حریم خصوصی و امنیت: CTISS نیازمند تعیین رویکردها و سیاست‌هایی است که اطمینان حاصل کند تا اطلاعات اشتراکی در حالت امن قرار دارند و حریم خصوصی فردی حفظ می‌شود.
(۵) معماری و ساختار اطلاعات: تعیین معماری‌ها و ساختارهای استاندارد برای اطلاعاتی که به اشتراک گذاشته می‌شوند، به تدوین و تحلیل مؤثرتر اطلاعات کمک می‌کند.

CTISS با ایجاد استانداردهای مشترک و پروتکل‌های استاندارد برای اشتراک اطلاعات امنیتی به سازمان‌ها کمک می‌کند تا مواجهه سریع‌تر و مؤثرتری با تهدیدات سایبری داشته باشند و شرایط امنیتی حاکم بر فضای سایبری را بهبود بخشند.

۶.۵ تحلیل مقایسه‌ای استانداردها

در جدول ۴ به مقایسه کلان سه استاندارد معتبر شواهد تهدید –یعنی STIX، TAXII و CTISS– پرداخته شده است. این استانداردها هر کدام وظایف و کارکردهای خاص خود را در زمینه تبادل اطلاعات مربوط به تهدیدات، حملات و آسیب‌پذیری‌ها دارند. با استفاده از معیارهای استاندارد و پروتکل‌های تبادل اطلاعات امنیتی و با مقایسه و تحلیل معیارها و اصول بکارگیری هر یک از این استانداردها، می‌توان بهترین رویکرد و استاندارد را متناسب با نیازهای سازمان انتخاب نمود [۲۹].

استفاده از استانداردها از سوی سازمان‌ها می‌تواند بهبود قابل توجهی در مدیریت و پاسخ به تهدیدات سایبری ایجاد کند. این استانداردها، با فراهم آوردن یک زبان مشترک برای تبادل اطلاعات تهدیدات، امکان انتقال سریع، مؤثر و امن داده‌های امنیتی را بین سازمان‌ها فراهم می‌آورند. این اقدام نه‌تنها کارایی عملیاتی را افزایش می‌دهد بلکه همچنین کاهش زمان واکنش در مواجهه با حملات را تسریع می‌بخشد. با استفاده از این استانداردها، سازمان‌ها قادر خواهند بود تا بهترین استراتژی‌ها و تکنولوژی‌ها را برای مدیریت تهدیدات سایبری به کار گیرند و در نهایت، امنیت و قابلیت اطمینان سیستم‌های خود را بهبود بخشند.

۶ ائتلاف‌های شناخته‌شده شواهد تهدید در جهان

چارچوب‌های همکاری، آئین‌نامه‌های تبادل اطلاعات امنیتی و اتحادیه‌های شواهد تهدید در سراسر جهان نقش مهمی را در ارتقاء امنیت سایبری و مقابله با تهدیدات ایفا می‌نمایند. این ائتلاف‌ها –شامل سازمان‌های دولتی، صنعتی و تحقیقاتی– باهدف تبادل اطلاعات شواهد تهدید، تحلیل تهدیدها و ایجاد همکاری‌های مؤثر در زمینه رسیدگی به حوادث امنیت سایبری شکل گرفته‌اند. ازجمله این ائتلاف‌ها می‌توان به FS-ISAC (در حوزه خدمات مالی)، CTI League (به عنوان یک ائتلاف جامعه‌محور داوطلبانه) و AusCERT (فعال در منطقه استرالیا و نیوزیلند) اشاره کرد. این اتحادیه‌ها با ایجاد پلتفرم‌ها و استانداردهای مشترک، به سازمان‌ها کمک می‌کنند تا در مقابله با چالش‌های پیشروی امنیت سایبری به بهترین شکل ممکن عمل نمایند.

نقاط قوت تشکیل ائتلاف‌های شواهد تهدید مابین کشورهای مختلف شامل موارد زیر است [۳۰]:

(۱) تقویت همکاری بین‌المللی: این ائتلاف‌ها به کشورها امکان می‌دهند تا در مقابله با تهدیدات سایبری، همکاری و هماهنگی حداکثری داشته باشند. این تقویت همکاری می‌تواند به اشتراک‌گذاری اطلاعات، تجربیات و روش‌های مؤثر برای مقابله با تهدیدات سایبری منجر شود.
(۲) افزایش قدرت تصمیم‌گیری: با ایجاد این ائتلاف‌ها، کشورها می‌توانند قدرت تصمیم‌گیری خود را در مواجهه با تهدیدات سایبری افزایش دهند. این امر به دلیل دسترسی به منابع بیشتر، تحلیل‌های مشترک و توانایی اجرایی قوی‌تر را فراهم می‌آورد.
(۳) کاهش آسیب‌پذیری‌ها: با همکاری و مشارکت در ائتلاف‌های شواهد تهدید، کشورها می‌توانند از تجربیات یکدیگر استفاده نمایند و روش‌های مؤثرتری را برای جلوگیری از حملات سایبری و کاهش

[1] Cyber Threat Intelligence Sharing Standards

ویژگی / مزیت	STIX	TAXII	CTISS
نوع استاندارد	استاندارد داده‌ای	استاندارد ارتباطی	چارچوب تحلیل امنیتی
قابلیت انتقال اطلاعات (Information dissemination)	بسیار بالا	متوسط	متوسط
نحوه توصیف حمله‌ها	با دقت و جزئیات	متوسط	کم
امکان اشتراک‌گذاری داده‌ها و اطلاعات	بله	بله	بله
قابلیت انتقال داده‌ها	بله	بله	بله
امکان انتقال بر أساس ملاحظات سرعت	خیر	بله	بله
امکان انتقال بر اساس ملاحظات امنیت	بله	بله	بله
امکان ارتقاء و توسعه	بله	بله	بله
کاربردهای اصلی	تبادل اطلاعات مربوط به تهدیدات، حملات و آسیب‌پذیری‌ها	تبادل داده‌های مربوط به تهدیدات، حملات و آسیب‌پذیری‌ها	تجزیه و تحلیل اطلاعات مربوط به تهدیدات و حملات سایبری

جدول ۴. مقایسه کلان استانداردهای شواهد تهدید

آسیب‌های احتمالی به‌کار گیرند.

(۴) استقرار استانداردها و قوانین مشترک: این ائتلاف‌ها می‌توانند به توسعه و اجرای استانداردها و قوانین مشترک در زمینه امنیت سایبری کمک نمایند که این مهم به بهبود شرایط امنیت سایبری در سطح جهانی منجر می‌شود.

(۵) افزایش قدرت ارتباطات سیاسی: با عضویت در ائتلاف‌های شواهد تهدید، کشورها می‌توانند روابط سیاسی خود را با کشورهای دیگر تقویت کنند و به ارتقای جایگاه خود در جامعه بین‌المللی کمک نمایند.

بنابراین، تشکیل ائتلاف‌های شواهد تهدید بین کشورها می‌تواند بهبودهای چشمگیری در شرایط امنیت سایبری جهانی ایجاد کند و به کاهش تهدیدات سایبری و کاهش آسیب‌های ناشی از آن‌ها کمک نماید.

در مقیاس سازمان دولتی، تشکیل ائتلاف‌های شواهد تهدید می‌تواند از اهمیت ویژه‌ای برخوردار باشد. مهم‌ترین مزایای آن به شرح زیر است [۳۰]:

(۱) تقویت امنیت ملی: سازمان‌های دولتی مسئول حفظ امنیت کشور در برابر حملات سایبری هستند. با عضویت در ائتلاف‌های شواهد تهدید، این سازمان‌ها می‌توانند به اشتراک‌گذاری اطلاعات و تجربیات با کشورهای دیگر بپردازند و از تجربیات و توانمندی‌های همکارانشان استفاده کنند تا امنیت ملی را تقویت نمایند.

(۲) افزایش توانایی پاسخگویی: با عضویت در ائتلاف‌های شواهد تهدید، سازمان‌های دولتی می‌توانند توانایی پاسخگویی به حملات سایبری را بهبود بخشند. این ائتلاف‌ها می‌توانند به‌سرعت اطلاعات جدید در مورد تهدیدات سایبری را به اعضای خود منتقل نمایند و اقدامات مناسب برای مقابله با آن‌ها را هماهنگ کنند.

(۳) تقویت قوانین و سیاست‌ها: ائتلاف‌های شواهد تهدید می‌توانند به توسعه و اجرای قوانین و سیاست‌های مشترک در زمینه امنیت سایبری کمک کنند. این قوانین و سیاست‌ها بهبودهای لازم را در تدابیر امنیتی دولتی و عمومی ایجاد می‌نماید که در افزایش امنیت سایبری در سطح ملی و بین‌المللی حائز اهمیت است.

(۴) تسهیل در اشتراک‌گذاری اطلاعات: ائتلاف‌های شواهد تهدید در تسهیل اشتراک‌گذاری اطلاعات میان سازمان‌های دولتی مختلف مهم هستند. این اطلاعات شامل الگوهای حملات، روش‌های جدید تهدید و تجربیات در مقابله با حملات سایبری است.

به‌طورکلی، تشکیل ائتلاف‌های شواهد تهدید بین سازمان‌های دولتی می‌تواند بهبودهای چشمگیری را در امنیت سایبری ملی و بین‌المللی ایجاد نماید و در حفظ امنیت اطلاعات و سیستم‌های دولتی راهگشا باشد.

در ادامه به بررسی برخی از ائتلاف‌های شناخته‌شده شواهد تهدید پرداخته خواهد شد.

۱.۶ ائتلاف اشتراک‌گذاری و تحلیل اطلاعات

ائتلاف اشتراک‌گذاری و تحلیل اطلاعات[1] (ISAC) معرف مفهومی عمومی است که در زمینه‌های مختلف و در مکان‌های مختلف وجود دارد. هر ISAC به محل تجمع صنایع خاصی اختصاص دارد و عمدتاً برای تبادل اطلاعات شواهد تهدید و همکاری در حوزه امنیت سایبری شکل گرفته است. این ائتلاف‌ها توسط سازمان‌های دولتی، صنعتی و تحقیقاتی تشکیل شده‌اند و به عنوان مراکزی برای جمع‌آوری، تحلیل و تبادل اطلاعات مرتبط با تهدیدات سایبری عمل می‌کنند [۳۱، ۳۲].

برخی از ویژگی‌ها و فعالیت‌های ISAC به شرح زیر هستند:

(۱) جمع‌آوری اطلاعات شواهد تهدید: ISAC ها به عنوان نقاط کانونی جمع‌آوری اطلاعات شواهد تهدید از اعضای خود و سایر منابع متنوع اطلاعاتی عمل می‌کنند.

[1] Information Sharing and Analysis Center

(۲) تبادل اطلاعات: اعضای ISAC اطلاعات مربوط به تهدیدات سایبری و حوادث امنیتی را با یکدیگر به اشتراک می‌گذارند تا همگان از تجربیات یکدیگر بهره‌مند شوند.
(۳) تحلیل تهدیدات: ISAC ها توانایی تحلیل تهدیدات را دارند و اطلاعات جمع‌آوری‌شده را تجزیه و تحلیل کرده و نتایج را به اعضای خود ارائه دهند.
(۴) همکاری در مقابله با تهدیدات: اعضای ISAC با همکاری یکدیگر در راستای مقابله با تهدیدات سایبری مشترک اقداماتی را انجام می‌دهند.
(۵) سخت‌افزارهای امنیتی: برخی از ISAC ها ارائه گر تعدادی از سخت‌افزارها و ابزارهای امنیتی هستند تا اعضاء را در تقویت شرایط امنیت سایبری یاری نمایند.
(۶) آموزش و آگاهی‌رسانی امنیتی: ISAC ها ارائه‌گر برنامه‌های آموزشی و دانش‌افزایی هستند تا اعضاء را در مورد روش‌های جدید حفاظت و پیشگیری از تهدیدات سایبری آموزش دهند.

ISAC ها معرف زیرساخت‌های مهمی برای تعاملات بین صنعتی و تشکیل محیط‌های همکاری در زمینه امنیت سایبری هستند. البته هر ISAC با توجه به صنعت یا محیط توسعه با چالش‌ها و تهدیدات خاصی نیز روبرو است.

۲.۶ ائتلاف لیگ شواهد تهدید

لیگ شواهد تهدید [1] معرف یک ائتلاف پویا و جامعه‌محور از تحلیل‌گران شواهد تهدید و امنیت با تخصص در حوزه‌های مختلف سایبری است. این مجموعه باهدف مبارزه با تهدیدات سایبری و افزایش سطح امنیت در فضای سایبر به صورت داوطلبانه فعالیت می‌کند. اعضای CTI League از نقاط مختلف جهان به این ائتلاف پیوسته‌اند. آن‌ها در تحلیل تهدیدات سایبری، مقابله با حملات، آموزش و آگاهی‌رسانی امنیتی به جامعه، همکاری امنیتی با سازمان‌های مختلف و حفظ امنیت در حوزه زیرساخت‌های حیاتی ـ مانند صنعت بهداشت، امداد و نجات و ارتباطات عمومی ـ نقش مؤثری را ایفا می‌کنند. با توجه به ابعاد گسترده تهدیدات سایبری، CTI League با جمع‌آوری تجربیات متخصصان سایبری و فعالیت به عنوان یک نیروی داوطلبانه، به تقویت امنیت در فضای سایبری کمک می‌نماید [۳۰].

برخی از ویژگی‌ها و فعالیت‌های لیگ شواهد تهدید به شرح زیر هستند:

(۱) تحلیل تهدیدات: اعضای این لیگ به تحلیل تهدیدات سایبری می‌پردازند و ارائه گر بینش و درک عمیقی از روش‌ها و ابزارهای حملات سایبری هستند.
(۲) مشارکت در مقابله با حملات: این ائتلاف به سازمان‌ها در مقابله با حملات سایبری کمک می‌کند و رهنمودهایی را پیرامون اقدامات امنیت سایبری ارائه می‌دهد.
(۳) آموزش و آگاهی‌رسانی: CTI League ارائه گر خدمات آموزش و آگاهی‌رسانی به جامعه در زمینه امنیت سایبری است تا افراد بتوانند خود و منابع اطلاعاتی خود را در برابر تهدیدات حفظ نمایند.
(۴) همکاری با سازمان‌های مختلف: این ائتلاف با سازمان‌های دولتی، خصوصی و غیرانتفاعی همکاری می‌کند تا تجربیات و دانش خود در زمینه امنیت سایبری را به اشتراک بگذارد.
(۵) تأمین امنیت در حوزه زیرساخت‌های حیاتی: این لیگ در حوزه زیرساخت‌های حیاتی مانند صنعت بهداشت، امداد و نجات و نیز ارتباطات عمومی مشارکت دارد تا شرایط امنیت سایبری در این حوزه‌ها را ارتقاء دهد.

مواجهه‌های سایبری با ابعاد گسترده‌ای روبه‌رو شده‌اند و لیگ شواهد تهدید با جمع‌آوری نیروهای داوطلب و استفاده از تجربیات متخصصان سایبری تا حد امکان به مقابله با این تهدیدات کمک می‌نماید.

۳.۶ ائتلاف مرکز تعالی دفاع سایبری مشترک ناتو

مرکز تعالی دفاع سایبری مشترک ناتو [2] (NATO CCDCOE) معرف یک نهاد معتبر تحقیقاتی و آموزشی در حوزه دفاع سایبری است که تحت پوشش سازمان آتلانتیک شمالی (NATO) به فعالیت می‌پردازد. این مرکز در سال ۲۰۰۸ در استونی تأسیس شده است. این مجموعه باهدف ارتقاء قابلیت‌ها و توانمندی‌های دفاع سایبری کشورهای عضو ناتو و شرکای غیر ناتو به تحقیقات و آموزش در زمینه سایبری می‌پردازد. فعالیت‌های CCDCOE شامل تحقیقات پیشرفته در زمینه حفاظت در برابر تهدیدات سایبری، برگزاری دوره‌های آموزشی برای متخصصان حوزه سایبری، همکاری با اعضای ائتلاف و شرکای خارجی و مشارکت در برگزاری مانورهای سایبری است. این مرکز تلاش مضاعفی برای توسعه فنّاوری‌های دفاع سایبری، ایجاد استانداردهای امنیتی و نیز ارتقاء توانمندی‌های علمی و فناورانه در زمینه دفاع سایبری انجام می‌دهد [۳۳].

برخی از ویژگی‌ها و فعالیت‌های NATO CCDCOE به شرح زیر هستند:

(۱) اهداف: CCDCOE به‌منظور ارتقاء قابلیت‌ها و توانمندی‌های دفاع سایبری کشورهای عضو ناتو و همچنین شرکای غیر ناتو تأسیس شده است. این مرکز به تحقیقات علمی و فناوارنه در حوزه دفاع سایبری می‌پردازد و آموزش‌های تخصصی مختلفی را برگزار می‌کند.
(۲) فعالیت‌ها و پروژه‌ها: CCDCOE بر تولید دانش و تحقیقات پیشرفته در زمینه حفاظت در برابر تهدیدات سایبری، امنیت اطلاعات و نیز توسعه فنّاوری‌های دفاع سایبری متمرکز است. این مرکز پروژه‌های متعددی را با همکاری اعضای ائتلاف و شرکای خارجی برنامه‌ریزی و اجرا می‌کند.
(۳) آموزش و تربیت: CCDCOE ارائه گر دوره‌های آموزشی متعددی در زمینه دفاع سایبری است. این دوره‌ها برای نیروهای نظامی،

[1] CTI League

[2] Nato Cooperative Cyber Defence Centre of Excellence

متخصصان حوزه سایبری و سایر افراد مرتبط با امنیت سایبری ارائه می‌شوند.

(۴) همکاری با اعضای ائتلاف و شرکای خارجی: CCDCOE با همکاری اعضای ائتلاف و همچنین کشورهای شریک خود، به تبادل دانش، اطلاعات و تجربیات در حوزه دفاع سایبری می‌پردازد.

(۵) مشارکت در برگزاری مانورهای سایبری: این مرکز در راستای افزایش توانایی دفاع سایبری، در برگزاری مانورهای سایبری مختلف نظامی و غیرنظامی شرکت می‌کند.

(۶) پشتیبانی از استانداردهای امنیتی: CCDCOE به ترویج و پیشبرد استانداردهای امنیت سایبری مانند استانداردهای STIX و TAXII می‌پردازد.

۴.۶ ائتلاف تیم واکنش به حوادث اضطراری رایانه‌ای استرالیا

به‌منظور مقابله با تهدیدات پیچیده سایبری، تشکیل ائتلاف‌ها و تیم‌های واکنش به حوادث سایبری امری ضروری شده است. تیم واکنش به حوادث اضطراری رایانه‌ای استرالیا [1] (AusCERT) به عنوان یکی از معتبرترین تیم‌های واکنش به حوادث اضطراری رایانه‌ای (CERT) در منطقه استرالیا و نیوزیلند تأسیس گردید. این مجموعه مسئولیت ارائه خدمات امنیت سایبری، تجزیه و تحلیل تهدیدات و پشتیبانی از سازمان‌ها در مقابله با حوادث سایبری را داشته و نقش بسیار مهمی در افزایش سطح امنیت سایبری را در این منطقه ایفا می‌کند. عمده خدمات و فعالیت‌های AusCERT باهدف تقویت آگاهی و توانمندی سازمان‌ها در حوزه امنیت سایبری به شرح زیر هستند [۳۴]:

(۱) جمع‌آوری و ارائه اطلاعات شواهد تهدید: AusCERT به عنوان یک مرجع اصلی در منطقه، اطلاعات شواهد تهدید را از منابع مختلف جمع‌آوری کرده و به سازمان‌ها ارائه می‌دهد.

(۲) پشتیبانی و مشاوره امنیتی: این سازمان ارائه گر خدمات متنوع پشتیبانی و مشاوره امنیتی برای سازمان‌ها و افراد است تا آن‌ها بتوانند به بهترین شکل ممکن از زیرساخت‌ها و سیاست‌های امنیتی خود استفاده نمایند.

(۳) آموزش و آگاهی‌رسانی: AusCERT به ارائه دوره‌های آموزشی و منابع آموزشی در زمینه امنیت سایبری می‌پردازد تا توانمندی سازمان‌ها و افراد در مقابله با تهدیدات سایبری را افزایش دهد.

(۴) همکاری با صنعت و مراکز تحقیقاتی: این مجموعه با صنعت و محققان در زمینه امنیت سایبری همکاری دارد تا به تحلیل و پیش‌بینی تهدیدات سایبری کمک نمایند.

(۵) واکنش به حوادث سایبری: AusCERT توانمندی واکنش به رخدادهای امنیتی را دارد و در صورت لزوم، به سازمان‌ها کمک می‌کند تا به‌سرعت و به بهترین نحو ممکن به حوادث سایبری واکنش نشان دهند.

(۶) عضویت و اشتراک‌گذاری خدمات: سازمان‌ها و افراد می‌توانند با عضویت در AusCERT به خدمات و منابع این سازمان دسترسی پیدا کنند و از خدمات و اطلاعات ارزشمند آن بهره‌مند شوند.

۵.۶ تحلیل مقایسه‌ای ائتلاف‌ها

مطالعه تطبیقی ائتلاف‌های امنیت سایبری از اهمیت بسزایی برخوردار است، زیرا درک از عملکرد و ویژگی‌های مختلف این ائتلاف‌ها، به ما کمک می‌کند تا بهترین راهکارها و راهبردهای امنیت سایبری را برای محافظت از اطلاعات انتخاب کنیم. این مطالعه تطبیقی به بررسی چهار ائتلاف مهم و اثرگذار امنیت سایبری می‌پردازد. در جدول ۵ مقایسه کلان ائتلاف‌های معتبر شواهد تهدید ارائه شده است. با توجه به نیازهای متفاوت سازمان‌ها و گستردگی تهدیدات سایبری، انتخاب بهترین ائتلاف امنیت سایبری بستگی به اهداف و نیازهای خاص هر سازمان دارد. در جدول ۵ و با توجه به مقایسه‌های کلان انجام شده، سازمان‌ها می‌توانند از ظرفیت‌های مختلف این ائتلاف‌ها بهره‌برداری کنند و با پیروی از دستورالعمل‌های ارائه‌شده، امنیت سایبری خود را بهبود بخشند. برای مقایسه ائتلاف‌های امنیت سایبری، معیارهای (اهداف و ماموریت‌ها، نوع فعالیت‌ها و خدمات ارائه‌شده، مدل همکاری و عضویت، پوشش جغرافیایی و صنایع هدف، ابزارها و منابع و مزایا و نقاط قوت) در نظر گرفته شده‌اند [۳۵].

۶.۶ تحلیل مقایسه‌ای ائتلاف‌ها

مطالعه تطبیقی ائتلاف‌های امنیت سایبری از اهمیت بسزایی برخوردار است، زیرا درک از عملکرد و ویژگی‌های مختلف این ائتلاف‌ها، به ما کمک می‌کند تا بهترین راهکارها و راهبردهای امنیت سایبری را برای محافظت از اطلاعات انتخاب کنیم. این مطالعه تطبیقی به بررسی چهار ائتلاف مهم و اثرگذار امنیت سایبری می‌پردازد. در جدول ۵ مقایسه کلان ائتلاف‌های معتبر شواهد تهدید ارائه شده است. با توجه به نیازهای متفاوت سازمان‌ها و گستردگی تهدیدات سایبری، انتخاب بهترین ائتلاف امنیت سایبری بستگی به اهداف و نیازهای خاص هر سازمان دارد. در جدول ۵ و با توجه به مقایسه‌های کلان انجام شده، سازمان‌ها می‌توانند از ظرفیت‌های مختلف این ائتلاف‌ها بهره‌برداری کنند و با پیروی از دستورالعمل‌های ارائه‌شده، امنیت سایبری خود را بهبود بخشند. برای مقایسه ائتلاف‌های امنیت سایبری، معیارهای (اهداف و ماموریت‌ها، نوع فعالیت‌ها و خدمات ارائه‌شده، مدل همکاری و عضویت، پوشش جغرافیایی و صنایع هدف، ابزارها و منابع و مزایا و نقاط قوت) در نظر گرفته شده‌اند [۳۵].

۷ یافته‌های تحقیق

بر اساس چارچوب مندرج در روش تحقیق (بند ۲-۴)، در این بخش تحلیل مقایسه‌ای کاربردی چارچوب‌ها، پلتفرم‌ها، استانداردها و ائتلاف‌های پشتیبان شواهد تهدید ارائه شده است. در این راستا دو گام مستقل اما

[1] Australasian Computer Emergency Response Team

شاخص / ائتلاف	ISAC	CTI League	NATO CCDCOE	AusCERT
اهداف	اشتراک دانش، اطلاعات و تجربیات مرتبط با امنیت سایبری بین اعضای یک صنعت	شناسایی و پیگیری فعالیت‌های مخرب در فضای سایبری	ارائه آموزش، آگاهی و مطالعات در زمینه امنیت سایبری به اعضای ناتو	ارائه اطلاعات و خدمات امنیتی به سازمان‌ها و افراد استرالیایی
محدوده اعضاء	اعضای یک صنعت یا حوزه خاص	افراد خودآموز و کارشناسان امنیت سایبری	کشورهای عضو ناتو	سازمان‌ها و افراد استرالیایی
منابع اطلاعاتی	اطلاعات مربوط به تهدیدهای سایبری مشترک و اطلاعات امنیتی مرتبط	اطلاعات جمع‌آوری شده از اعضا، ابزارهای تحلیلی و داده‌های عمومی	اطلاعات به‌دست آمده از کشورهای عضو، سازمان‌های بین‌المللی و مؤسسات مرتبط	اطلاعات جمع‌آوری شده از اعضا، ابزارهای تحلیلی و داده‌های عمومی
روش‌های همکاری	به اشتراک گذاری داده‌های امنیتی، ایجاد گروه‌های کاری، برگزاری رویدادها و آموزش‌ها	همکاری در برنامه‌های پیشگیری و پاسخگویی به حملات، تحلیل تهدیدات و اشتراک‌گذاری اطلاعات مرتبط	ارتباطات دوستانه بین کشورهای عضو، مشارکت در تمرین‌ها و ارائه آموزش‌های متقابل	ایجاد ارتباطات مؤثر با اعضا، ارائه خدمات آموزشی و مشارکت در تمرین‌ها و رویدادهای امنیتی
مزایا	اشتراک دانش و تجربیات مشترک، افزایش آگاهی در برابر تهدیدات، ایجاد شبکه‌های حمایتی	شناسایی و پیگیری فعالیت‌های مخرب در فضای سایبری، تشخیص الگوهای حمله، ارائه آموزش و اطلاعات مفید	تقویت همکاری بین کشورها، به‌اشتراک گذاری تجربیات و اطلاعات امنیتی	ارائه خدمات امنیتی و آموزشی به سطح ملی، افزایش آگاهی امنیتی
چالش‌ها	مشکلات مربوط به حفظ حریم خصوصی و اطلاعات محرمانه، کاهش میزان مشارکت، مدیریت اطلاعات حساس	کمبود منابع و توانایی‌های فنی، کمبود هماهنگی در عملیات، مشکلات مربوط به حفظ حریم خصوصی	مشکلات زبانی و فرهنگی، ناپایداری سیاسی، محدودیت‌های مربوط به امنیت و اطلاعات حساس	کمبود منابع و توانایی‌های فنی، مدیریت اطلاعات حساس و حفظ حریم خصوصی

جدول ۵. مقایسه کلان ائتلاف‌های شواهد تهدید

معیار	دور اول (میانگین امتیاز)	دور دوم (میانگین امتیاز)	وضعیت نهایی
هدف	۴/۵	۴/۷	انتخاب شده
اجزا	۴/۲	۴/۴	انتخاب شده
مزایا	۴/۸	۴/۹	انتخاب شده
معایب	۴/۰	۴/۳	انتخاب شده
هزینه پیاده‌سازی	۳/۲	–	انتخاب نشده
موارد استفاده	۴/۱	۴/۳	انتخاب شده
پذیرش بین‌المللی	۳/۹	۳/۴	انتخاب نشده
قابلیت تطبیق	۴/۳	۴/۵	انتخاب شده
پشتیبانی و نگهداری	۳/۸	۳/۴	انتخاب نشده

جدول ۶. اعتباردهی به معیارهای مؤثر بر انتخاب چارچوب‌های شواهد تهدید بر پایه روش دلفی فازی

به‌هم پیوسته پیگیری و عملیاتی شده است. در مرحله اول، اعتبارسنجی معیارهای مؤثر در انتخاب موضوعات چهارگانه تحقیق حاضر مبتنی بر روش دلفی فازی انجام شده است. برای انتخاب این معیارها (نتایج ارائه شده در جداول ۶، ۹، ۱۲، ۱۵)، کارشناسان معیارهای اصلی که حد نصاب لازم را کسب کرده‌اند و برخی معیارهایی که حد نصاب را دریافت نکرده‌اند را تعیین نموده‌اند. معیارهایی که حد نصاب لازم را کسب کرده‌اند (میانگین امتیاز بالای ۵.۳) در ستون «وضعیت نهایی» به عنوان «انتخاب‌شده» مشخص شده‌اند. امتیازات معیارها در مقیاس ۱ تا ۵ تخصیص داده شده‌اند که ۵ به معنای بالاترین اهمیت و ۱ به معنای کمترین اهمیت است. این جدول کمک می‌کند تا به‌طور شفاف مشخص شود که کدام معیارها از دیدگاه کارشناسان اهمیت بیشتری داشته‌اند و چرا به عنوان معیارهای اصلی انتخاب شده‌اند. در مرحله دوم و برای مقایسه چارچوب‌ها، پلتفرم‌ها، استانداردها و ائتلاف‌ها بر اساس معیارهای تعیین‌شده در جداول ۸،۱۱،۱۴،۱۷ ارائه شده است. امتیازهای مندرج در جداول اخیرالذکر مبتنی بر پنل خبرگی و اجماع از طریق روش دلفی محاسبه و تعیین گردیده است. شایان ذکر است وزن دهی مندرج در جداول ۷،۱۰،۱۳،۱۶ این معیارها مبتنی بر روش تحلیل سلسله‌مراتبی

معیار	میانگین هندسی	وزن نهایی (نرمال‌شده)	وزن نهایی (%)
هدف	۰/۹۱۸	۰/۱۵۰	۱۵٪
اجزا	۰/۹۱۸	۰/۱۵۰	۱۵٪
مزایا	۱/۵۳۱	۰/۲۵۰	۲۵٪
معایب	۰/۹۱۸	۰/۱۵۰	۱۵٪
موارد استفاده	۰/۹۱۸	۰/۱۵۰	۱۵٪
قابلیت تطبیق	۰/۹۱۸	۰/۱۵۰	۱۵٪

جدول ۷. وزن‌دهی معیارهای منتخب پیرامون چارچوب‌های شواهد تهدید بر پایه روش تحلیل سلسله‌مراتبی

معیار	وزن	NIST	MITRE ATT&CK	Kill Cyber Chain	Loop OODA	MISP	مدل الماس
هدف	۱۵٪	۹	۸	۷	۶	۸	۷
اجزا	۱۵٪	۸	۹	۷	۶	۷	۸
مزایا	۲۵٪	۹	۸	۷	۶	۸	۷
معایب	۱۵٪	۷	۶	۶	۶	۸	۷
موارد استفاده	۱۵٪	۸	۷	۷	۶	۷	۷
قابلیت تطبیق	۱۵٪	۹	۸	۷	۶	۸	۷
امتیاز کل	۱۰۰٪	۸٫۴	۷٫۸۵	۶٫۸۵	۶	۷٫۷۵	۷٫۱۵

جدول ۸. مقایسه تحلیلی-کاربردی چارچوب‌های شواهد تهدید

معیار	دور اول (میانگین امتیاز)	دور دوم (میانگین امتیاز)	وضعیت نهایی
جمع‌آوری اطلاعات شواهد تهدید	۴٫۵	۴٫۶	انتخاب شده
تجزیه و تحلیل اطلاعات	۴٫۳	۴٫۴	انتخاب شده
خودکارسازی فرآیندها	۴٫۲	۴٫۱	انتخاب شده
اشتراک‌گذاری اطلاعات	۴٫۴	۴٫۳	انتخاب شده
ادغام با سایر ابزارها	۴٫۱	۴٫۲	انتخاب شده
پشتیبانی از استانداردها	۴٫۰	۴٫۱	انتخاب شده
پشتیبانی مشتریان	۳٫۳	-	انتخاب نشده
گزارش‌گیری و نمودارسازی	۴٫۲	۴٫۳	انتخاب شده
رابط کاربری کاربرپسند	۳٫۵	۳٫۴	انتخاب نشده
قیمت و هزینه‌ها	۳٫۸	۳٫۲	انتخاب نشده

جدول ۹. اعتباردهی به معیارهای مؤثر بر انتخاب پلتفرم‌های شواهد تهدید بر پایه روش دلفی فازی

معیار	میانگین هندسی	وزن نهایی (نرمال‌شده)	وزن نهایی
جمع‌آوری اطلاعات شواهد تهدید	۱٫۴۶۱۲	۰٫۲۰	۲۰٪
تجزیه و تحلیل اطلاعات	۱٫۴۶۱۲	۰٫۲۰	۲۰٪
خودکارسازی فرآیندها	۱٫۰۹۵۹	۰٫۱۵	۱۵٪
اشتراک‌گذاری اطلاعات	۰٫۷۳۰۶	۰٫۱۰	۱۰٪
ادغام با سایر ابزارها	۰٫۷۳۰۶	۰٫۱۰	۱۰٪
پشتیبانی از استانداردها	۰٫۷۳۰۶	۰٫۱۰	۱۰٪
گزارش‌گیری و نمودارسازی	۱٫۰۹۵۹	۰٫۱۵	۱۵٪

جدول ۱۰. وزن‌دهی معیارهای منتخب پیرامون پلتفرم‌های شواهد تهدید بر پایه روش تحلیل سلسله‌مراتبی

(AHP) انجام شده است [۳۶]. در این روش برای معیارها ابتدا باید مقایسه زوجی انجام شود. سپس میانگین هندسی از مقادیر موجود در هر ردیف ماتریس مقایسه زوجی محاسبه می‌شود و در انتها وزن نهایی با نرمال‌سازی میانگین هندسی هر معیار به دست می‌آید (جمع همه وزن‌ها باید برابر ۱ باشد).

۱.۷ یافته‌های تحقیق در زمینه تحلیل چارچوب‌های پشتیبان شواهد تهدید

با توجه به اهمیت روزافزون امنیت سایبری، مطالعه این چارچوب‌ها و مقایسه آن‌ها، گامی مهم و اساسی در جهت بهبود راهبردها و فرآیندهای امنیتی سازمان‌ها محسوب می‌شود. مطالعه تطبیقی و مقایسه‌ای به سازمان‌ها این امکان را می‌دهد تا بر اساس نیازها و شرایط خاص خود، بهترین چارچوب را برای مدیریت مخاطرات سایبری انتخاب کنند. با مقایسه دقیق ویژگی‌ها و عملکرد هر چارچوب، می‌توان تصمیمات بهتری در زمینه امنیت سایبری گرفت و از منابع موجود بهینه‌تر استفاده نمود. در [۳۷] توضیح داده می‌شود که چگونه باید معیارهای مختلفی از جمله هدف، اجزا، مزایا، معایب، موارد استفاده و قابلیت تطبیق را در ارزیابی چارچوب‌های امنیت سایبری در نظر گرفت.

برای مقایسه چارچوب‌های شواهد تهدید بر اساس معیارهای تعیین‌شده، جدول ۸ ارائه می‌شود. امتیازات هر چارچوب بر اساس نظرات ۱۸ کارشناس (۶ استاد دانشگاه و مدرس دارای مقاله یا تالیف مرتبط، ۹ پژوهشگر فعال در این زمینه و ۳ مجری پروژه‌های مرتبط با چارچوب‌های شواهد تهدید) با روش دلفی فازی به دست آمده است.

در انتخاب چارچوب‌های شواهد تهدید، سازمان‌ها باید به طور دقیق اهداف خود را مشخص و این اهداف را با نیازهای خاص در حوزه شواهد تهدید خود تطبیق دهند. اولویت انتخاب چارچوب مناسب در وهله اول براساس همراستایی اهداف امنیتی سازمان با اهداف و کارکردهای چارچوب‌های فوق‌الاشاره تعیین خواهد شد. علاوه‌براین، سازمان‌ها باید توجه ویژه‌ای به محدودیت‌ها و معایب هر چارچوب داشته باشند و توانایی خود را در مدیریت و کاهش این محدودیت‌ها ارزیابی نمایند. براین اساس

معیار	وزن	Splunk Phantom	MISP	ThreatConnect	Anomali ThreatStream	EclecticIQ
جمع‌آوری اطلاعات شواهد تهدید	۲۰٪	۸	۷	۹	۸	۷
تجزیه و تحلیل اطلاعات	۲۰٪	۹	۶	۸	۹	۸
خودکارسازی فرآیندها	۱۵٪	۹	۵	۷	۸	۷
اشتراک‌گذاری اطلاعات	۱۰٪	۸	۹	۸	۷	۷
ادغام با سایر ابزارها	۱۰٪	۷	۵	۸	۸	۷
پشتیبانی از استانداردها	۱۰٪	۸	۷	۸	۹	۸
گزارش‌گیری و نمودارسازی	۱۵٪	۹	۶	۸	۸	۷
امتیاز کل	۱۰۰٪	۸٫۵	۶٫۵	۸٫۰	۸٫۱	۷٫۳

جدول ۱۱. مقایسه تحلیلی-کاربردی پلتفرم‌های شواهد تهدید

معیار	دور اول	دور دوم	دور سوم	وضعیت نهایی
هدف اصلی	۴٫۵	۴٫۶	۴٫۷	انتخاب شده
توسعه‌دهنده	۴٫۲	۴٫۳	۴٫۴	انتخاب شده
هزینه پیاده‌سازی	۳٫۵	۳٫۰	-	انتخاب نشده
فرمت داده	۴٫۱	۴٫۲	۴٫۲	انتخاب شده
پروتکل ارتباطی	۴٫۰	۴٫۱	۴٫۰	انتخاب شده
استانداردهای شناسایی تهدید	۴٫۴	۴٫۵	۴٫۶	انتخاب شده
قابلیت انعطاف‌پذیری	۳٫۵	۳٫۴	-	انتخاب نشده
تعامل بین سیستم‌ها	۴٫۳	۴٫۴	۴٫۵	انتخاب شده
سهولت استفاده	۳٫۴	-	-	انتخاب نشده
رویکردهای حریم خصوصی	۳٫۹	۴٫۱	۴٫۰	انتخاب شده
قابلیت‌های شخصی‌سازی	۳٫۳	-	-	انتخاب نشده
پشتیبانی از استانداردها	۴٫۶	۴٫۷	۴٫۸	انتخاب شده
توسعه ابزارها	۴٫۳	۴٫۴	۴٫۵	انتخاب شده
میزان پذیرش	۴٫۲	۴٫۳	۴٫۴	انتخاب شده

جدول ۱۲. اعتباردهی به معیارهای مؤثر بر انتخاب استانداردهای شواهد تهدید بر پایه روش دلفی فازی

و در صورت آدرس‌دهی درست به دو مورد فوق‌الاشاره، سازمان‌ها بر اساس امتیازاتی که هر چارچوب در معیارهای مختلف کسب کرده است، می‌توانند به یک انتخاب کارآمد دست یابند و به بهترین شکل ممکن ظرفیت‌های شواهد تهدید را در مجموعه خود ارتقاء دهند.

۲.۷ یافته‌های تحقیق در زمینه تحلیل پلتفرم‌های پشتیبان شواهد تهدید

مطالعه تطبیقی پلتفرم‌های شواهد تهدید به سازمان‌ها این امکان را می‌دهد تا بر اساس نیازها و شرایط خاص خود، بهترین پلتفرم را برای مدیریت مخاطرات سایبری انتخاب کنند. در انتخاب پلتفرم‌های شواهد تهدید، سازمان‌ها باید متناسب با اولویت‌ها و محدودیت‌های خود و ویژگی‌های

معیار	میانگین هندسی	وزن نهایی (نرمال‌شده)	وزن نهایی
هدف اصلی	۲٫۲۰۵۶	۰٫۱۹۹۹	۲۰٪
توسعه‌دهنده	۱٫۶۵۴۶	۰٫۱۵۰۰	۱۵٪
فرمت داده	۱٫۱۰۳۶	۰٫۱۰۰۰	۱۰٪
پروتکل ارتباطی	۱٫۱۰۳۶	۰٫۱۰۰۰	۱۰٪
استانداردهای شناسایی تهدید	۱٫۱۰۳۶	۰٫۱۰۰۰	۱۰٪
تعامل بین سیستم‌ها	۱٫۱۰۳۶	۰٫۱۰۰۰	۱۰٪
رویکردهای حریم خصوصی	۱٫۱۰۳۶	۰٫۱۰۰۰	۱۰٪
پشتیبانی از استانداردها	۰٫۵۵۱۰	۰٫۰۴۹۹	۵٪
توسعه ابزارها	۰٫۵۵۱۰	۰٫۰۴۹۹	۵٪
میزان پذیرش	۰٫۵۵۱۰	۰٫۰۴۹۹	۵٪

جدول ۱۳. وزن‌دهی معیارهای منتخب پیرامون استانداردهای شواهد تهدید بر پایه روش تحلیل سلسله‌مراتبی

معیار	وزن	STIX	TAXII	CTISS
هدف اصلی	۲۰٪	۹	۸	۷
توسعه‌دهنده	۱۵٪	۸	۷	۶
فرمت داده	۱۰٪	۹	۷	۵
پروتکل ارتباطی	۱۰٪	۸	۹	۶
استانداردهای شناسایی تهدید	۱۰٪	۷	۸	۷
تعامل بین سیستم‌ها	۱۰٪	۸	۷	۶
رویکردهای حریم خصوصی	۱۰٪	۷	۶	۸
پشتیبانی از استانداردها	۵٪	۸	۷	۵
توسعه ابزارها	۵٪	۷	۶	۶
میزان پذیرش	۵٪	۸	۷	۶
امتیاز کل	۱۰۰٪	۸٫۲	۷٫۴	۶٫۳

جدول ۱۴. مقایسه تحلیلی-کاربردی استانداردهای شواهد تهدید

معیار	دور اول (میانگین امتیاز)	دور دوم (میانگین امتیاز)	وضعیت نهایی
اهداف و ماموریت‌ها	۴/۶	۴/۸	انتخاب شده
نوع فعالیت‌ها	۴/۵	۴/۷	انتخاب شده
مدل همکاری و عضویت	۴/۴	۴/۶	انتخاب شده
پوشش جغرافیایی	۴/۳	۴/۵	انتخاب شده
نرخ رشد عضویت	۳/۶	۳/۴	انتخاب نشده
ابزارها و منابع	۴/۲	۴/۴	انتخاب شده
تعداد مشارکت‌ها	۳/۵	۳/۳	انتخاب نشده
نوع فعالیت‌ها	۳/۶	۳/۴	انتخاب نشده
مدل همکاری و عضویت	۳/۲	-	انتخاب نشده
تعداد اعضا	۳/۸	۳/۰	انتخاب نشده
مدل کسب و کار	۳/۵	۳/۳	انتخاب نشده

جدول ۱۵. اعتباردهی به معیارهای مؤثر بر انتخاب ائتلاف‌های شواهد تهدید بر پایه روش دلفی فازی

معیار	میانگین هندسی	وزن نهایی (نرمال‌شده)	وزن نهایی
اهداف و ماموریت‌ها	۱/۵۳۱	۰/۲۵۰	۲۵٪
نوع فعالیت‌ها	۱/۴۶۱۲	۰/۲۰	۲۰٪
مدل همکاری و عضویت	۱/۰۹۵۹	۰/۱۵	۱۵٪
پوشش جغرافیایی	۱/۰۹۵۹	۰/۱۵	۱۵٪
ابزارها و منابع	۱/۵۳۱	۰/۲۵۰	۲۵٪

جدول ۱۶. وزن‌دهی معیارهای منتخب پیرامون ائتلاف‌های شواهد تهدید بر پایه روش تحلیل سلسله‌مراتبی

معیار / ائتلاف	وزن	ISAC	CTI League	NATO CCDCOE	AusCERT
اهداف و ماموریت‌ها	۲۵٪	۸	۷	۹	۶
نوع فعالیت‌ها	۲۰٪	۷	۸	۸	۷
مدل همکاری و عضویت	۱۵٪	۶	۷	۹	۶
پوشش جغرافیایی	۱۵٪	۸	۵	۹	۷
ابزارها و منابع	۲۵٪	۹	۶	۸	۷
امتیاز کل	۱۰۰٪	۸/۰	۶/۸	۸/۵	۶/۶

جدول ۱۷. مقایسه تحلیلی-کاربردی ائتلاف‌های شواهد تهدید

هر پلتفرم، از اطلاعات مقایسه تحلیلی آن‌ها برای انتخاب بهترین و منطبق‌ترین پلتفرم استفاده کنند. معیارهای جمع‌آوری اطلاعات شواهد تهدید، تجزیه و تحلیل اطلاعات، خودکارسازی فرآیندها، اشتراک‌گذاری اطلاعات، ادغام با سایر ابزارها، پشتیبانی از استانداردها، و گزارش‌گیری و نمودارسازی نیز باید در این فرآیند مدنظر قرار گیرند. با مقایسه دقیق ویژگی‌ها و عملکرد هر پلتفرم، می‌توان تصمیمات بهتری در زمینه امنیت سایبری گرفت و از منابع موجود بهینه‌تر استفاده نمود. در جدول ۱۱ پلتفرم‌ها از منظر تحلیل کاربردی مورد ارزیابی قرار می‌گیرند. همچنین دستورالعمل بکارگیری پلتفرم‌ها مطابق با معیارها و اصولی نظیر گارتنِر [۳۸] و فارِستِر [۳۹] که معمولاً شامل تجزیه و تحلیل عمیق و مقایسه‌ای از ابزارها و پلتفرم‌های امنیت سایبری مختلف هستند احصا شده است. امتیازات هر چارچوب بر اساس نظرات ۱۵ کارشناس (۳ استاد دانشگاه و مدرس دارای مقاله یا تالیف مرتبط، ۷ پژوهشگر فعال در این زمینه و ۵ مجری پروژه‌های مرتبط با پلتفرم‌های شواهد تهدید) و تحلیل‌های پنل خبرگان با روش دلفی فازی به دست آمده است.

در انتخاب پلتفرم‌های شواهد تهدید، چنانچه نیازهای اصلی سازمان در حوزه شواهد تهدید با قابلیت ارائه شده توسط پلتفرم‌های مختلف همخوانی داشته باشد، چارچوب امتیازدهی فوق می‌تواند به عنوان یک راهکار مناسب برای انتخاب پلتفرم هدف مدنظر قرار گیرد. در نهایت، انتخاب پلتفرم مناسب باید بر اساس ترکیبی از اهداف و اولویت‌های سازمان باشد تا بتوانند به بهترین نحو امنیت سایبری خود را تقویت نمایند.

۳.۷ یافته‌های تحقیق در زمینه تحلیل استانداردهای پشتیبان شواهد تهدید

مطالعه و مقایسه استانداردهای مختلف شواهد تهدید می‌تواند به بهبود راهبردها و فرآیندهای امنیتی در سازمان‌ها کمک کند. در انتخاب استانداردهای شواهد تهدید، سازمان‌ها باید متناسب با اولویت‌ها و محدودیت‌های خود و ویژگی‌های هر استاندارد، از اطلاعات مقایسه تحلیلی آن‌ها برای انتخاب بهترین و منطبق‌ترین استاندارد استفاده کنند. در [۴۰] معیارهای هدف اصلی، توسعه‌دهنده، فرمت داده، پروتکل ارتباطی، استانداردهای شناسایی تهدید، تعامل بین سیستم‌ها، رویکردهای حریم خصوصی، پشتیبانی از استانداردها، توسعه ابزارها و میزان پذیرش نیز باید در این فرآیند مدنظر قرار گیرند. در این مطالعه تطبیقی، با استفاده از نظرات ۱۷ کارشناس (شامل ۴ تحلیلگر امنیت، ۵ پژوهشگر امنیتی، و ۸ فرد با سابقه کار در حوزه استانداردگذاری پروژه‌های مرتبط با شواهد تهدید)، به ارزیابی و مقایسه استانداردها پرداخته شده است. این نظرات با استفاده از روش دلفی فازی جمع‌آوری و تحلیل شده‌اند. بر اساس نتایج این تحقیق، سازمان‌ها می‌توانند با توجه به نیازها و شرایط خاص خود، بهترین استاندارد را برای مدیریت مخاطرات سایبری انتخاب کنند. جدول ۱۴، امتیازات به‌دست‌آمده برای هر استاندارد را بر اساس معیارهای تعیین‌شده ارائه می‌دهد. این امتیازات نشان‌دهنده همراستایی اهداف امنیتی سازمان‌ها با اهداف و کارکردهای استانداردهای مختلف است و به عنوان اولویت انتخاب استاندارد مناسب می‌تواند مورد استفاده قرار گیرد.

۴.۷ یافته‌های تحقیق در زمینه تحلیل ائتلاف‌های پشتیبان شواهد تهدید

ائتلاف‌های شواهد تهدید به سازمان‌ها این امکان را می‌دهند تا با استفاده از اشتراک‌گذاری اطلاعات و منابع، بهبود چشم‌گیری در شناسایی و پاسخ به تهدیدات بالقوه داشته باشند. در انتخاب ائتلاف‌های شواهد تهدید، سازمان‌ها باید متناسب با اولویت‌ها و محدودیت‌های خود و ویژگی‌های هر ائتلاف، از اطلاعات مقایسه تحلیلی آن‌ها برای انتخاب بهترین و منطبق‌ترین ائتلاف استفاده کنند. در [۴۱] معیارهای اهداف و مأموریت‌ها، نوع فعالیت‌ها، مدل همکاری و عضویت، پوشش جغرافیایی ابزارها و منابع نیز باید در این فرآیند مدنظر قرار گیرند. این مطالعه تطبیقی با استفاده از نظرات ۱۸ کارشناس (شامل ۸ تولید کننده و تحلیلگر فید امنیت/فید شواهد تهدید، ۱۰ فرد شاخص و شناخته شده عضو ائتلاف‌ها/مجامع تخصصی امنیت)، به بررسی و مقایسه ویژگی‌ها و مزایای مختلف ائتلاف‌های شواهد تهدید پرداخته است. نتایج نشان می‌دهد که سازمان‌ها می‌توانند با انتخاب و مشارکت در ائتلاف‌های مناسب، به منابعی از داده‌های تهدیدات سایبری دست یابند که به تنهایی ممکن است قادر به جمع‌آوری آن نباشند. این امر به آن‌ها امکان می‌دهد تا با رویکردهای پیشگیرانه و واکنشی، استراتژی‌های امنیتی مؤثرتری برای مقابله با تهدیدات بالقوه تدوین کنند. جدول ۱۷ امتیازات و مقایسه ائتلاف‌ها را بر اساس معیارهای تعیین‌شده ارائه می‌دهد که نشان‌دهنده مزایا و کارکردهای مختلف هر ائتلاف است. این نتایج به سازمان‌ها کمک می‌کند تا با توجه به نیازهای خاص خود، بهترین ائتلاف را برای بهره‌گیری از مزایا و رویکردهای آن در مقابله با تهدیدات انتخاب کنند.

۸ نتیجه‌گیری

استفاده از چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید برای سازمان‌ها باعث بهبود قابلیت‌ها و عملکردهای امنیتی آنان می‌شود. در این مقاله، ابتدا مهم‌ترین چارچوب‌ها به‌طور خلاصه معرفی و ویژگی‌های کلیدی آن‌ها بررسی و تحلیل شدند. این چارچوب‌ها امکان فراهم کردن یک محیط اطمینان‌بخش و مقاوم در برابر تهدیدات سایبری را فراهم می‌آورند.

عدم پیشرفت در پیاده‌سازی شواهد تهدید در یک سازمان به عوامل مختلفی وابسته است. در برخی موارد، سازمان‌ها ممکن است منابع مالی، انسانی و فناورانه لازم برای پیاده‌سازی و توسعه شواهد تهدید را به صورت کافی تخصیص ندهند. این مشکل می‌تواند باعث محدودیت در توانایی سازمان برای جمع‌آوری، تحلیل و استفاده از اطلاعات شواهد تهدید شود. علاوه‌براین، عدم وجود یک راهبرد مشخص و منطقی برای پیاده‌سازی شواهد تهدید می‌تواند باعث ناتوانی در تعیین اهداف، اولویت‌بندی فعالیت‌ها و انتخاب منابع مناسب شود.

در این راستا و در مقاله حاضر، برای کمک به سازمان‌ها جهت مواجهه کارآمد با شرایط فوق‌الاشاره دو نوع تحلیل انجام شد:

(۱) در مرحله اول و با تحلیل مقایسه‌ای کلان چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید، موضوع تصویرسازی پیرامون قلمرو کاربرد و شرایط بکارگیری هریک از موضوعات چهارگانه فوق مدنظر قرار گرفت. در این راه، قابلیت‌ها، مزایا، معایب و محدودیت‌های پیش‌روی استفاده از چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید آدرس‌دهی گردید. این امر فضای پیش‌روی سازمان‌ها جهت ورود/ عدم ورود به استفاده از هریک از این عرصه‌ها را شفاف و تا حدودی عدم قطعیت را پیرامون موضوعات چهارگانه کاهش داده است.

(۲) در مرحله دوم و با تحلیل مقایسه‌ای کاربردی چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید –در قالب یافته‌های تحقیق–، دو موضوع توسط محقق آدرس‌دهی شده است.

- اول، معرفی، اعتباردهی و وزن‌دهی به معیارها و متغیرهای تصمیمی است که در انتخاب و بکارگیری هریک از موضوعات تحقیق حاضر (یعنی چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌ها) ایفای نقش می‌کنند. در این راه و جهت شناسایی معیارهای مؤثر بر انتخاب از منابع معتبر تخصصی و برای اعتباردهی (انتخاب) و وزن‌دهی به آن‌ها از روش‌شناسی آماری معین و پنل تخصصی مرتبط با آن موضوع استفاده شده است.
- دوم، ارزیابی و ارزش‌گذاری چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید براساس چارچوب ارزیابی و معیارهای شناسایی و وزن‌دهی شده در مرحله قبل است. در این راه، از رهنمودهای مدون توسعه‌دهنده یا متولی چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌ها در کنار نظرات خبرگان حوزه تخصصی –با روش تعریف‌شده در تحقیق حاضر– بهره‌برداری شده است.

سازمان‌های بهره‌بردار از چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید در صورت رعایت دو مورد زیر می‌توانند از نتایج ارزیابی و ارزش‌گذاری ارائه‌شده در بخش تحلیل مقایسه‌ای کاربردی جهت انتخاب هریک از موضوعات چهارگانه استفاده نمایند:

(۱) تأمین همراستایی راهبردی: همراستایی راهبردی به معنی آن است که استفاده از چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید در راستای تأمین اهداف تجاری و امنیتی سازمان‌ها باشد. از این‌رو، پیش از انتخاب چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید باید هدف از بکارگیری، مؤلفه‌های سازنده و کارکردهای اصلی آن‌ها با نیازهای اصلی سازمان هدف تطبیق داده شود.

(۲) حل‌وفصل محدودیت‌ها: یکی از پیش‌نیازهای انتخاب چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید توجه به معایب و محدودیت‌ها یا پیش‌نیازهای ویژه عضویت یا بکارگیری آن‌ها است. در صورت عدم توجه به محدودیت‌ها و پیش‌بینی راهکارهای مؤثر مواجهه با آن‌ها، بکارگیری صرف چارچوب‌ها، استانداردها، پلتفرم‌ها

و ائتلاف‌های شواهد تهدید می‌تواند منجر به تحمیل جدی هزینه‌ها و شکست در اجرای پروژه‌های مربوطه شود.

مبتنی بر یافته‌های تحقیق حاضر، سازمان‌ها با استفاده آگاهانه و مبتنی بر تحلیل از این چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌ها برای پیاده‌سازی شواهد تهدید می‌توانند به نتایج زیر دست یابند:

- افزایش آگاهی و توانمندی: چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید، به سازمان‌ها کمک می‌کنند تا بهبود آگاهی و توانمندی‌های خود در مواجهه با تهدیدات سایبری را افزایش دهند. این سازوکارها امکان شناسایی، ارزیابی و مدیریت بهتر مخاطرات را فراهم می‌آورد.
- ارتقاء امنیت سایبری: استفاده از چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید، منجر به ارتقاء سطح امنیت سایبری سازمان می‌شود. این سازوکارها از اصول و رویکردهای مشخصی برای شناسایی و مدیریت تهدیدات استفاده می‌کنند. این مهم به سازمان‌ها کمک می‌کند تا در مقابله با حملات سایبری به‌شکلی مؤثرتر عمل نمایند.
- افزایش توانایی تصمیم‌گیری: استفاده از این چارچوب‌ها و پلتفرم‌های شواهد تهدید به مدیران سازمان‌ها کمک می‌کند تا تصمیم‌گیری‌های بهتری را در زمینه امنیت سایبری اتخاذ نمایند و منابع خود را به صورت بهینه‌تری مدیریت نمایند.
- ایجاد هماهنگی و همگرایی: چارچوب‌ها، استانداردها، پلتفرم‌ها و ائتلاف‌های شواهد تهدید با ارائه روش‌ها و فرآیندهای استاندارد شده، به سازمان‌ها کمک می‌کنند تا فرهنگ امنیتی را در سازمان تقویت کرده و هماهنگی بین بخش‌های مختلف را تسهیل نمایند.
- اشتراک‌گذاری دانش و تجربیات: با پیوستن به ائتلاف‌های شواهد تهدید، سازمان‌ها به ظرفیت اشتراک گذاشتن اطلاعات و تجربیات با دیگران و نیز بهره‌برداری از دانش جمعی و ابزارهای مشترک دست پیدا می‌کنند. این همکاری‌ها منجر به افزایش قدرت تشخیص و پاسخ به تهدیدات سایبری می‌شود.

۹ سپاسگزاری

بدین‌وسیله از پژوهشکده امنیت ارتباطات و فناوری اطلاعات پژوهشگاه ارتباطات و فناوری اطلاعات که در قالب پروژه جایزه تعالی امنیت سایبری حمایت معنوی خود را از این فعالیت پژوهشی بعمل آورده، کمال تشکر را دارد.

مراجع

[1] MITRE ATT&CK. Threat intelligence program, 2024. Accessed: 2024.

[2] Johnson, Christopher S. and F., L. Cyber threat intelligence and information sharing. tech. rep., NIST, 2016.

[3] Security Intelligence. Understanding cyber threat intelligence, 2024. Accessed: 2024.

[4] Saadatmand, F. A. S. Configurations of platform organizations: Implications for complementor engagement. 2019.

[5] Ghorra-Gobin, C. The comparative social science approach. 2008.

[6] Linstone, H. A. and Turoff, M., eds. . *The Delphi Method: Techniques and Applications*. Addison-Wesley Publishing Company, 2002.

[7] Mukherjee, S. S. and Chatterjee, S. Application of delphi method in cyber security framework selection: A review. *Journal of Cyber Security Technology*, 3(4):203–216, 2019.

[8] Lingel, S., Rhodes, C., Cordova, A., Hagen, J., Kvitky, J., and Menthe, L. Methodology for improving the planning, execution, and assessment of intelligence, surveillance, and reconnaissance operations. tech. rep., RAND Project Airforce, 2008.

[9] Military decision-making process, 2014. Accessed: 2014.

[10] Afenu, Divine S. Industrial control systems security validation based on mitre adversarial tactics, techniques, and common knowledge framework. *Electronics*, 13(5):917, 2024.

[11] Troia, Vinny. *Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques*. Wiley, 2020.

[12] Fujita, Junya. A structured cyber attack representation model based on the diamond model and adversary states. in *IEEE*, 2023.

[13] Lockheed Martin. Cyber kill chain, 2024. Accessed: 2024.

[14] Shehu, Asma'u, Umar, Mahmood, and Aliyu, Abdulmalik. Cyber kill chain analysis using artificial intelligence. *Asian Journal of Research in Computer Science*, 2023.

[15] National Institute of Standards and Technology (NIST). Nist cybersecurity framework, 2024. Accessed: 2024.

[16] Ford, Daniel. *A Vision So Noble: John Boyd, the OODA Loop, and America's War on Terror*. Warbird Books, 2013.

[17] Zager, Robert. Ooda loops in cyberspace: A new cyber defense model. *SMALL WARS*, 2017.

[18] MISP. Misp threat sharing, 2024. Accessed: 2024.

[19] Wagner, Cynthia. Misp: The design and implementation of a collaborative threat intelligence sharing platform. in *ACM*, 2016.

[20] Blokdyk, Gerardus. *Threat Intelligence Platform: A Complete Guide*. 5STARCooks, 2020.

[21] Splunk Phantom. Splunk phantom threat intelligence, 2024. Accessed: 2024.

[22] ThreatConnect. Threat intelligence operations and cyber risk quantification, 2024. Accessed: 2024.

[23] Anomali ThreatStream. Threat intelligence platform, 2024. Accessed: 2024.

[24] EclecticIQ. Eclecticiq platform, 2024. Accessed: 2024.

[25] Shostack, Adam. *Threat Modeling: Designing for Security*. Wiley, 2014.

[26] OASIS. Structured threat information expression (stix™), 2024. Accessed: 2024.

[27] OASIS. Trusted automated exchange of intelligence information (taxii™), 2024. Accessed: 2024.

[28] CTIC. Cyber threat intelligence consortium, 2024. Accessed: 2024.

[29] OASIS. Organization for the advancement of structured information standards, 2021. Accessed: 2021.

[30] CTI League. Threat intelligence, 2024. Accessed: 2024.

[31] ISAC. Threat intelligence, 2024. Accessed: 2024.

[32] FS-ISAC. Safeguarding the global financial system by reducing cyber risk, 2024. Accessed: 2024.

[33] NATO CCDCOE. The nato cooperative cyber defence centre of excellence, 2024. Accessed: 2024.

[34] AusCERT. Australasian computer emergency response team, 2024. Accessed: 2024.

[35] Awad, Lina M., Al-Kaseem, Bilal S., and Al-Shaer, Said F. The role of information sharing in cybersecurity: A survey. 2021.

[36] Saaty, T. L. *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*. McGraw-Hill, 1980.

[37] National Institute of Standards and Technology (NIST). Nist special publication 800-37 revision 2: Risk management framework for information systems and organizations: A system life cycle approach for security and privacy. tech. rep., 2018. Accessed: 2018.

[38] Gartner. Magic quadrant for security information and event management (siem), 2020. Accessed: 2020.

[39] Forrester. The forrester wave: Security analytics platforms, 2020. Accessed: 2020.

[40] National Institute of Standards and Technology (NIST). Guide to cyber threat information sharing (nist special publication 800-150). tech. rep., 2016. Accessed: 2016.

[41] ENISA. Cooperative models, 2020. Accessed: 2020.

[42] Lee, Martin. *Cyber Threat Intelligence*. Wiley, 2023.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2025, Volume 23, Number 1 (pp. 19–44)
https://monadi.isc.org.ir

Analysis of frameworks, standards, platforms, and coalitions supporting the development of cyber threat intelligence in organizations

Amin chahardoli [1] and Abouzar Arabsorkhi [2,*]

[1] *Faculty of Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran*
[2] *Iran Telecommunication Research Center, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: May 16, 2024
Accepted: January 4, 2025
Published Online: May 14, 2025

Keywords:
Cyber Threat Intelligence, Frameworks, Platforms, Reference Standards, Leagues

Type: Research paper

In today's modern world, with the emergence of technological advancements, cybersecurity has become one of the most critical issues. Every day, millions of data items are exchanged across the internet, exposing organizations and individuals to threats such as cyber intrusions, unauthorized access to information, and more. In this dynamic environment, Threat Intelligence has emerged as a prominent and effective tool to combat these threats—without overlooking necessary sensitivities. This modern approach enables organizations to analyze threat intelligence data meticulously, respond proactively to cyberattacks, and ensure the desired level of information security.

Given the increasing trend of cyberattacks, governments and organizations worldwide are pursuing strategies to strengthen institutional capacities for threat intelligence. In this article, through a comparative study of frameworks, standards, platforms, and coalitions (as key tools for enhancing cybersecurity and preventing attacks), the researcher provides a detailed analytical examination of these tools and their role in reinforcing cybersecurity systems. By focusing on the structural strengths and implementation components of threat intelligence in organizations—and leveraging the experiences of governments and international coalitions—this research aims to illustrate the essential role of these components in the production, dissemination, and utilization of threat intelligence. It also highlights the importance of effectively integrating these solutions into an organization's information security cycle.

Achieving threat intelligence through frameworks, standards, platforms, and related coalitions requires attention to diverse requirements and actions. Based on the findings of this research, decision-makers and stakeholders can anticipate and operationalize necessary measures to implement threat intelligence approaches at an organizational level. Furthermore, adopting these frameworks, standards, platforms, and coalitions not only helps organizations utilize threat intelligence more effectively but also plays a critical role in decision-making and countering cyberattacks.

Frameworks, standards, platforms, and coalitions supporting threat intelligence development represent the most vital components, tools, and approaches used in the collection, analysis, and application of threat intelligence. These tools and standards have advanced significantly over time to assist organizations in effectively combating cyber threats. They enable organizations to better produce, disseminate, and implement threat intelligence strategies to ad-

* Corresponding author
Email addresses: amin.chahardoli@iau.ac.ir (Amin chahardoli), abouzar_arab@itrc.ac.ir (Abouzar Arabsorkhi)
© 2025 ISC. All rights reserved.

dress diverse attacks and threats.

This article is based on an extensive and in-depth study of major international frameworks for implementing and developing threat intelligence, as well as adopting standards and structures aligned with organizational needs—including principles, processes, responsibilities, and roles—within the threat intelligence lifecycle. By analyzing published best practices and insights from this research, practical recommendations are provided to organizations for managing threat intelligence. The production, dissemination, analysis, and application of threat intelligence are critically important for organizations due to the following reasons:

- Threat Identification and Prediction: Threat intelligence helps organizations identify and analyze patterns and trends in cyberattacks. This information guides organizations in predicting future attack types and planning appropriate countermeasures.
- Enhancing Incident Response: By leveraging threat intelligence, organizations can respond swiftly and effectively to cyberattacks. This minimizes potential damages and reduces the costs associated with attacks.
- Strengthening Cybersecurity: Organizations can implement necessary improvements to their systems and networks using threat intelligence, thereby better protecting their resources. These measures include researching and developing security technologies, enforcing efficient security policies, and enhancing employee awareness and trainin.

The development and implementation of frameworks, standards, platforms, and coalitions not only empower organizations to leverage threat intelligence more effectively but are also pivotal in strategic decision-making and countering cyberattacks. In the pervasive world of information technology, threat intelligence serves as a vital and undeniable tool in addressing organizations' security challenges. The use of threat intelligence in cybersecurity management—encompassing concepts such as threat identification, data-driven security decision-making, protection of sensitive information, defensive strategies, early detection and rapid response, and risk prediction and mitigation—emerges as a key factor in elevating security standards. By emphasizing the importance of these issues and the unparalleled role of threat intelligence in preventing and countering cyber threats, organizations are encouraged to leverage this powerful tool in the realm of cybersecurity.

Based on the outlined considerations, the primary research question of this study is:

- What are the functional roles of frameworks, standards, platforms, and alliances supporting threat intelligence in organizations? Addressing this main question requires answering the following sub-questions:
- What are the constituent components and elements of frameworks, standards, platforms, and alliances supporting threat intelligence in organizations?
- What are the factors influencing the selection and implementation of frameworks, standards, platforms, and alliances supporting threat intelligence in organizations?
- What are the criteria influencing the selection and implementation of frameworks, standards, platforms, and alliances supporting threat intelligence in organizations?
- What is the status of these influential criteria concerning each selected framework, standard, platform, or alliance supporting threat intelligence in organizations?
- How will the evaluation and assessment of selected frameworks, standards, platforms, and alliances supporting threat intelligence be conducted based on these criteria?