جمهوری اسلامی ایران
ریاست جمهوری
مرکز مدیریت راهبردی افتا

ملاحظات و دستورالعمل‌های نگهداری و آرشیو لاگ

تیر ۱۴۰۳
نسخه ۱.۱

فهرست مطالب

۱. مقدمه

در زمینه فناوری اطلاعات و امنیت سایبری، لاگ[1] به فایل یا مجموعه‌ای از رکوردها گفته می‌شود که وقایع و فعالیت‌های مختلف سیستم، نرم‌افزار، یا شبکه را ثبت می‌کند. این اطلاعات می‌تواند شامل مواردی مانند ورود و خروج کاربران، فعالیت‌های شبکه، وقایع امنیتی (فعالیت‌های مشکوک یا حملات سایبری)، خطاها و هشدارها (خطاهای نرم‌افزاری و سخت‌افزاری) و تغییرات سیستمی باشد. لاگ‌ها به مدیران سیستم و متخصصان امنیت سایبری کمک می‌کند تا وضعیت عملکرد سیستم را بررسی و مشکلات را شناسایی و رفع کنند و از امنیت سیستم محافظت نمایند. با توجه به تنوع زیاد لاگ‌های امنیتی در شبکه، نیاز به وجود روالی جهت مدیریت آن‌ها بسیار حائز اهمیت می‌باشد. این روال باید شامل استانداردهای دقیق و جزئی شامل فرآیند تولید، انتقال، ذخیره سازی، تجزیه و تحلیل و حذف ایمن لاگ‌ها باشد. در این سند امنیتی تلاش شده تا چارچوب مشخصی از الزامات مدیریت لاگ برای سازمان‌های حیاتی کشور ارائه شود.

۲. اهداف

نگهداری و آرشیو لاگ به فرآیند جمع آوری، ذخیره سازی و مدیریت لاگ ها اشاره دارد که لازم است مطابق با سه اصل محافظت از محرمانه بودن، یکپارچگی و در دسترس بودن لاگ‌ها پیاده سازی شود. این روال برای اطمینان از اینکه لاگ های امنیتی با جزئیات کافی و برای مدت زمان مناسب ذخیره می شوند ضروری است. مدیریت صحیح لاگ ها از جنبه های مختلف امنیتی، قانونی، عملیاتی و مدیریتی اهمیت زیادی داشته و به سازمان ها در تشخیص و جلوگیری از حوادث امنیتی و ردیابی فعالیت کاربران، پاسخ به حوادث امنیتی، تطابق با مقررات و استانداردهای جهانی و عیب یابی و بهینه سازی سیستم کمک می‌کند.

۳. دسته بندی لاگ

بطورکلی لاگ‌ها در هفت دسته اصلی تقسیم‌بندی می‌شوند که هریک اطلاعات و رویدادهای مختلفی را ثبت می‌کنند لذا سازمان‌های حیاتی می‌بایست نسبت به ثبت و نگهداری تمامی موارد ذیل به همراه الزامات کلی که در بخش ۴ معرفی خواهند شد، اقدام نمایند.

نوع لاگ	دسته بندی	توضیحات
لاگ سیستم عامل	لاگ‌های سیستم[2]	شامل اطلاعات مربوط به عملکرد سیستم‌عامل، خطاها و تغییرات مهم در سیستم
	لاگ‌های امنیتی[3]	شامل اطلاعات مربوط به تلاش‌های ورود و خروج کاربران، دسترسی‌های موفق و ناموفق و تغییرات امنیتی در سیستم
	لاگ‌های رخداد[4]	ثبت رویدادهای مختلف در سیستم عامل مانند نصب نرم افزارها، به روزرسانی‌ها و خطاهای سیستم

[1] log
[2] System Logs
[3] Security Logs
[4] Event Logs

نوع لاگ	دسته بندی	توضیحات
لاگ نرم افزار کاربردی[1]	لاگ برنامه‌های وب[2]	شامل اطلاعات مربوط به درخواست‌های ورودی و خروجی، خطاهای برنامه و دسترسی به منابع وب
	لاگ پایگاه داده	شامل اطلاعات مربوط به اجرای دستورات SQL، تغییر در داده‌ها و دسترسی‌های کاربران به پایگاه‌داده
	لاگ سرور ایمیل	شامل اطلاعات مربوط به ارسال و دریافت ایمیل‌ها، خطاهای تحویل و دسترسی به صندوق‌های پست الکترونیک
لاگ شبکه	لاگ فایروال	شامل اطلاعات مربوط به ترافیک مجاز و غیرمجاز، قوانین فیلترینگ و حملات شناسایی شده
	لاگ روتر و سوئیچ	شامل اطلاعات مربوط به ترافیک شبکه، تغییرات پیکربندی و خطاهای شبکه
	لاگ سیستم‌های تشخیص و جلوگیری از نفوذ[3]	شامل اطلاعات مربوط به فعالیت‌های مشکوک، حملات شناسایی شده و پاسخ به تهدیدات
لاگ احراز هویت و دسترسی[4]	لاگ سرویس‌های احراز هویت	شامل اطلاعات مربوط به تلاش‌های ورود و خروج، تغییرات رمز عبور و دسترسی به منابع
	لاگ Active Directory و LDAP	شامل اطلاعات مربوط به تغییرات در حساب‌های کاربری، گروه‌ها و دسترسی به دایرکتوری‌ها
لاگ سرویس‌های ابری	لاگ پلتفرم‌های ابری	شامل اطلاعات مربوط به دسترسی به منابع ابری، تغییرات پیکربندی و فعالیت کاربران در محیط‌های ابری
لاگ امنیت فیزیکی	لاگ دسترسی فیزیکی	شامل اطلاعات مربوط به دسترسی به اتاق‌های سرور و استفاده از کارت‌های دسترسی
	لاگ سیستم‌های نظارتی	شامل اطلاعات مربوط به رویدادهای ثبت شده توسط دوربین‌های نظارتی و سیستم‌های امنیت فیزیکی
لاگ سیستم‌های مدیریت و مانیتورینگ	لاگ سامانه مدیریت رخداد[5]	شامل اطلاعات جمع‌آوری‌شده از منابع مختلف برای تحلیل و مدیریت امنیت
	لاگ نرم افزارهای مدیریت شبکه و سیستم	شامل اطلاعات مربوط به نظارت عملکرد و سلامت سیستم‌ها و شبکه‌ها

[1] Application Logs
[2] Web Application Logs
[3] IDS/IPS Logs
[4] Authentication and Access Logs
[5] Security Information And Event Management (SIEM)

۴. الزامات امن‌سازی لاگ

در وهله اول سازمان باید خط مشی و رویه‌هایی را برای مدیریت لاگ ایجاد کند. برای ایجاد و حفظ فعالیت‌های مدیریت لاگ، یک سازمان می‌بایست فرآیندهای استاندارد را برای انجام مدیریت لاگ توسعه دهد. به عنوان بخشی از این فرآیندها، سازمان باید الزامات و اهداف ثبت لاگ را تعریف کند و بر اساس آن‌ها، سیاست‌هایی را توسعه دهد که الزامات اجباری و توصیه‌های پیشنهادی در زمینه مدیریت لاگ، شامل **چرخه تولید، انتقال، ذخیره‌سازی، تجزیه و تحلیل** و **حذف** لاگ را به وضوح تعریف کند. پیش از بیان الزامات، لازم است به توضیح مفهوم Audit Log پرداخته شود.

لاگ ممیزی یا Audit Log که به عنوان Audit Trail نیز شناخته می‌شود، سابقه ی کلی از تمامی فعالیت‌ها، تغییرات و رویدادهای مهم در یک سیستم، نرم افزار یا شبکه را در خود جای می‌دهد. این لاگ‌ها به منظور مستندسازی و پیگیری فعالیت‌های کاربران، تغییرات سیستم و دسترسی‌ها استفاده می‌شود. هدف اصلی Audit Log این است که ردیابی دقیقی از تمامی اقدامات و فعالیت‌ها فراهم کند تا بتوان در صورت نیاز جهت تحلیل و پاسخ به حوادث امنیتی و نظارت و کنترل دسترسی به آن‌ها مراجعه کرد. یک Audit Log باید شامل اطلاعات کاربر (شناسه، نقش و سطح دسترسی کاربر)، زمان و تاریخ رویداد، نوع رویداد (نوع فعالیت انجام شده مانند ورود- خروج- دسترسی به فایل)، نتیجه رویداد (موفقیت آمیز بودن یا نبودن) و مبدأ و مقصد ارتباط (مثلا آدرس IP) باشد.

در جدول ۱ و

جدول ۲ الزامات مرتبط با این بخش ارائه شده است. سطوح پیاده سازی و عملکردهای امنیتی مشخص شده در جدول ۱، در ادامه توضیح داده شده است.

۴.۱ سطوح پیاده سازی

سطوح پیاده سازی در کنترل‌های امنیتی CIS[1]، برای کمک به سازمان ها در اولویت بندی و پیاده سازی کنترل های امنیتی بر اساس سطح پیچیدگی و منابع مورد نیاز طراحی شده اند. هر سطح نشان دهنده بلوغ و پیشرفت در پیاده سازی کنترل ها است. هدف اصلی این است که سازمان با ارزیابی روند پیاده سازی کنترل های امنیتی خود، به شکلی سازمان یافته تر و هدفمندتر، سطح امنیت سایبری خود را بهبود بخشیده و در برابر تهدیدات محافظت شود.

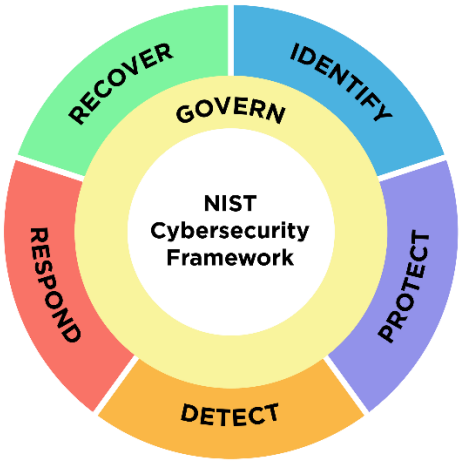
- **سطح ۱** (IG1[2]): به سازمان‌های کوچک تا متوسط با تخصیص محدود فناوری در حوزه امنیت سایبری برای حفاظت از دارایی‌ها و پرسنل فناوری اطلاعات اختصاص دارد. دغدغه اصلی این سازمان ها نگه‌داشت عملیاتی کسب و کار خود، به‌دلیل تحمل محدود خرابی است. حساسیت داده‌هایی که این نوع از سازمان‌ها سعی در محافظت از آن‌ها دارند کم و اصولاً تنها محدود به اطلاعات مالی و هویتی کارمندان است.
- **سطح ۲** (IG2): برای سازمان‌هایی است که از بخش‌های متعدد با ریسک‌های متفاوت بر اساس عملکرد و مأموریت شغلی خاصی تشکیل شده‌اند. این سازمان‌ها اغلب اطلاعات حساس مشتری یا سازمانی را ذخیره و پردازش می‌کنند و می‌توانند وقفه‌های کوتاه خدمات را تحمل کنند. نگرانی اصلی این سازمان‌ها از دست دادن اعتماد عمومی در صورت وقوع اخلال و نشت داده[3] است. این دسته از سازمان‌ها علاوه‌بر رعایت ملاحظات سطح ۱، ملاحظات این سطح را نیز پیاده سازی کرده اند.
- **سطح ۳** (IG3): برای سازمان‌هایی است که بخشی از پرسنل آن‌ها کارشناسان امنیتی هستند که در جنبه های مختلف امنیت سایبری (مانند مدیریت ریسک، تست نفوذ و امنیت سامانه) تخصص دارند. دارایی‌ها و داده‌های این سازمان شامل اطلاعات یا عملکردهای حساس و تحت نظارت است. سازمان‌هایی که در این سطح قرار دارند، باید در دسترس بودن خدمات، محرمانه بودن و یکپارچگی داده‌های حساس را بررسی کنند چراکه حملات موفقیت‌آمیز به این سازمان‌ها می‌تواند آسیب‌های قابل توجهی به رفاه اجتماعی وارد کند. این دسته از سازمان‌ها علاوه‌بر رعایت ملاحظات سطح ۱ و ۲، ملاحظات این سطح را نیز پیاده سازی کرده اند.

۴.۲ عملکرد امنیتی

عملکردهای امنیتی در چارچوب امنیت سایبری NIST Cybersecurity Framework v2.0 (CSF)، مجموعه ای از فعالیت‌ها و فرآیندهایی است که به سازمان‌ها کمک می‌کنند تا ریسک‌های امنیت سایبری خود را به طور جامع مدیریت کنند. این عملکردها به عنوان بخش اصلی چارچوب امنیت سایبری، هریک نقش مهمی در مدیریت و کاهش ریسک‌های امنیت سایبری

[1] Center of Internet Security
[2] Implementation Group
[3] Data breach

دارند. در نسخه 8.1 از سند CIS تلاش شده تا همخوانی بیشتری با استانداردها و چارچوب‌های امنیتی دیگر مانند ISO و NIST برقرار شود، لذا همانطور که در جدول ۱ مشخص است، این عملکردهای امنیتی برای هریک از الزامات بصورت جداگانه مشخص شده است. این همخوانی به سازمان‌ها کمک می کند تا تطابق بیشتری با الزامات و استانداردهای امنیتی داشته باشند.



شکل ۱ – عملکردهای چارچوب امنیت سایبری

۱. **Govern** (حاکمیت) : ایجاد ساختارهای مدیریتی و نظارتی برای اطمینان از هماهنگی و همخوانی تمامی فعالیت های امنیتی با اهداف و سیاست های سازمان و تضمین اینکه این فعالیت ها به طور موثر و مستمر انجام می شوند.

۲. **Identify** (شناسایی) : شناسایی دارایی ها، داده ها و نقاط ضعف امنیتی به منظور درک بهتر از وضعیت موجود و شناسایی تهدیدات بالقوه

۳. **Protect** (حفاظت) : پیاده سازی اقدامات و کنترل های امنیتی برای حفاظت از دارایی ها و اطلاعات سازمان در برابر تهدیدات

۴. **Detect** (تشخیص) : نظارت و شناسایی فعالیت های مشکوک و رخدادهای امنیتی به منظور تشخیص زودهنگام حملات و تهدیدات

۵. **Respond** (پاسخ دهی) : پاسخ دهی به رخدادهای امنیتی به منظور کاهش تاثیرات منفی و بازیابی سریع سیستم ها و اطلاعات.

۶. **Recover** (بازیابی) : بازیابی سیستم ها و اطلاعات پس از وقوع رخدادهای امنیتی و اطمینان از بازگشت به وضعیت عادی عملیات

جدول ۱ – مدیریت لاگ های ممیزی (سطح بندی شده براساس کنترل‌های امنیتی CIS)

سطوح	عملکرد امنیتی	الزامات و ملاحظات
سطح ۱	حاکمیت	ایجاد و حفظ فرآیند مدیریت لاگ‌های ممیزی
سطح ۱	تشخیص	جمع‌آوری لاگ‌های ممیزی
سطح ۱	حفاظت	حصول اطمینان از فضای ذخیره سازی کافی برای لاگ‌های ممیزی
سطح ۲	حفاظت	استاندارد نمودن همگام سازی زمانی

سطح ۲	تشخیص	جمع‌آوری لاگ‌های ممیزی با جزئیات بیشتر (شامل منبع رویداد، تاریخ، نام کاربری، مهرزمانی، آدرس مبدأ، آدرس مقصد و سایر عناصر مفیدی که در فورنزیک کمک کننده است.)
سطح ۲	تشخیص	جمع‌آوری لاگ‌های ممیزی پرس و جوی DNS[1]
سطح ۲	تشخیص	جمع‌آوری لاگ‌های ممیزی درخواست‌های URL
سطح ۲	تشخیص	جمع‌آوری لاگ‌های ممیزی خط فرمان[2]
سطح ۲	تشخیص	متمرکز نمودن لاگ‌های ممیزی
سطح ۲	حفاظت	نگهداری از لاگ‌های ممیزی
سطح ۲	تشخیص	بررسی و ارزیابی لاگ‌های ممیزی
سطح ۳	تشخیص	جمع‌آوری لاگ‌های ارائه‌دهنده خدمات[3]

[1] Query
[2] Command-Line
[3] Service Provider

جدول ۲- الزامات مربوط به نظارت و مدیریت لاگ بر اساس چارچوب امنیت سایبری نسخه NIST ۲.۰

الزامات	توضیحات	راهنمای اجرا
سیاست و رویه‌های نظارت و ثبت لاگ	ایجاد، مستندسازی، تأیید، ابلاغ، اعمال، ارزیابی و حفظ خط مشی‌ها و رویه‌ها برای ثبت و نظارت. حداقل سالیانه خط‌مشی‌ها و رویه‌ها بازبینی و به‌روزرسانی شوند.	خط مشی‌ها و رویه‌ها باید شامل موارد زیر باشد: • مشخص کردن هدف، دامنه، نقش‌ها، مسئولیت‌ها و هماهنگی بین نهادهای سازمانی و آموزش • چگونه حوادث در طول یک حادثه امنیتی رسیدگی می‌شوند؟ • چه اطلاعاتی باید ثبت و نظارت شوند و برای چه مدت؟ • در صورت بروز حادثه به چه کسی اطلاع داده می شود؟ رویدادهای زیر در رویه نظارت و ثبت لاگ بایستی ضبط[1] شوند: • دسترسی‌های فردی کاربر به سیستم‌ها • اقدامات انجام شده توسط هر فردی که دارای سطح دسترسی root یا ادمین است. • دسترسی به تمام لاگ‌های ممیزی باید بر اساس اصل need-to-know و اصل حداقل امتیاز محدود شود. • تلاش‌های نامعتبر دسترسی • هرگونه تغییر، افزودن و یا حذف حساب هایی با سطح دسترسی root یا ادمین. • راه‌اندازی، متوقف کردن یا ایجاد هرگونه وقفه لحظه‌ای در لاگ‌های ممیزی • ایجاد و حذف اشیاء در سطح سیستمی
حفاظت از لاگ‌های ممیزی	تعریف، پیاده سازی و ارزیابی فرآیندها، رویه‌ها و اقدامات فنی برای اطمینان از امنیت و نگهداری از لاگ‌های ممیزی	متدولوژی حفاظت از لاگ باید با رعایت هرگونه تعهدات قانونی یا نظارتی قابل اجرا اعمال شود. در غیاب این الزامات، سازمان باید به هرگونه استاندارد مناسب برای کسب و کار، پایبند باشد.

[1] capture

الزامات	توضیحات	راهنمای اجرا
قابلیت پاسخگویی[1] و دسترسی به لاگ‌های ممیزی	دسترسی به لاگ‌های ممیزی تنها محدود به کارمندان مجاز شده و سوابق دسترسی‌های منحصر به فرد آن‌ها نگهداری شود.	لاگ‌های ممیزی باید امکان ردیابی دسترسی‌ها پس از شناسایی فعالیت‌های مشکوک را فراهم کنند. همچنین این لاگ‌ها باید شامل داده‌های کافی برای پشتیبانی از نیازهای تحقیقاتی در زمینه نقض امنیتی شوند. دسترسی به تمام لاگ‌های ممیزی می‌بایست بر اساس اصل need-to-know و حداقل امتیاز محدود شود. همچنین درصورت اعمال ناخواسته یا غیرمجاز، هشدار مربوطه تولید شود.
نظارت و پاسخ به لاگ‌های ممیزی	لاگ‌های ممیزی باید برای شناسایی فعالیت‌های خارج از الگوی معمولی یا مورد انتظار نظارت شود. ایجاد و پیروی از یک فرآیند تعریف شده برای بررسی و انجام اقدامات مناسب و به‌موقع در مورد ناهنجاری‌های شناسایی شده الزامی است.	قابلیت پاسخ به خرابی و شکست باید وجود داشته باشد. همچنین لایه‌های زیرساختی نیز درنظر گرفته (به عنوان مثال شبکه، هایپروایزر، نقطه پایانی، صفحه کنترل[2] و صفحه داده[3]) و خرابی‌ها و هشدارها در صورت بروز، رصد شود.
همگام‌سازی زمانی	از یک منبع زمانی قابل اعتماد در تمام سیستم‌های پردازش اطلاعات استفاده شود.	همگام‌سازی زمان‌های سیستمی، هماهنگی مناسب بین سیستم ها را امکان پذیر می کند و ردیابی و بازسازی روند زمانی فعالیت‌ها را تسهیل می کند. همچنین مفاهیم زیر باید در نظر گرفته شوند : • سیستم‌های حساس و بحرانی، زمان صحیح و ثابتی داشته باشند. • زمان در تمام سیستم‌ها هماهنگ باشد. • داده‌های زمان محافظت شوند. • تنظیمات زمان، از منابع زمانی قابل اطمینان دریافت شود.

[1] Accountability
[2] Control plane
[3] Data Plane

الزامات	توضیحات	راهنمای اجرا
دامنه لاگ	ایجاد، مستندسازی و پیاده سازی اینکه کدام متادیتا اطلاعات سیستم باید ثبت شوند. بررسی و به‌روزرسانی دامنه حداقل بصورت سالیانه یا هر زمان که در محیط تهدید تغییری ایجاد شود.	نمونه‌هایی از رویدادهایی که باید ثبت شوند عبارتند از : • رویدادهای موفق یا ناموفق ورود به حساب کاربری • رویدادهای مدیریت حساب • دسترسی به دارایی‌ها • تغییر سیاست • توابع امتیاز[1] • ردیابی فرآیند و رویدادهای سیستم • تمام فعالیت های ادمین • بررسی‌های احراز هویت • بررسی‌های مجوز[2] • حذف داده‌ها • دسترسی به داده‌ها • تغییرات داده • تغییرات مجوز[3]
سوابق لاگ	ایجاد سوابق ممیزی شامل اطلاعات امنیتی مرتبط	اطلاعات لاگ امنیتی مرتبط باید شامل موارد زیر باشد، هرچند محدود به این موارد نیست: • نوع رویداد • زمان رویداد • مکان رویداد • مبدأ رویداد • نتیجه رویداد • هویت فرد یا سیستم مرتبط با رویداد
محافظت از لاگ	حصول اطمینان از اینکه سیستم اطلاعاتی، سوابق ممیزی را از دسترسی بدون مجوز، تغییرات و حذف محافظت می کند.	دسترسی به سوابق ممیزی باید بر اساس حداقل امتیاز و تنها به افراد مجاز اعطا شود. تغییرات در لاگ‌ها، شامل حذف، باید توسط افراد مجاز ردیابی و تایید شود. لاگ‌ها باید بر اساس سیاست‌های سازمان، پشتیبان گیری[4] شوند.

[1] priviledge
[2] Authorization
[3] Permision
[4] Backup

الزامات	توضیحات	راهنمای اجرا
لاگ تراکنش/فعالیت	ثبت[1] و نظارت بر رویدادهای مدیریت چرخه حیات کلید برای فعال کردن ممیزی و گزارش استفاده از کلیدهای رمزنگاری	ثبت رویدادهای چرخه حیات کلید باید شامل رویدادهای زیر باشد اما به آنها محدود نمی شود: • تولید کلید • استفاده از کلید • ذخیره سازی کلید (شامل پشتیبان‌گیری) • بایگانی یا حذف کلید • تنها کارمندان مجاز باید به اجزای کلید دسترسی داشته باشند و تمام تلاش‌های دسترسی باید ثبت و بررسی شوند. مستندسازی و پیاده‌سازی تمام فرآیندها و رویه‌های مدیریت کلید برای کلیدهای رمزنگاری از جمله : • تولید کلیدهای رمزنگاری قوی • توزیع امن کلید رمزنگاری • ذخیره‌سازی امن کلید رمزنگاری • ابطال کلید پس از انقضا • تقسیم دانش و کنترل دوگانه در صورت نیاز برای عملیات مدیریت کلید دستی • جلوگیری از تعویض غیرمجاز کلیدهای رمزنگاری
لاگ‌های کنترل دسترسی	با استفاده از سیستم کنترل دسترسی قابل ممیزی، دسترسی فیزیکی نظارت و ثبت شود.	سازمان باید تمام دسترسی‌های فیزیکی را از طریق روش های زیر نظارت و ثبت کند: • تایید دسترسی فیزیکی افراد هنگام ورود به مناطق امن • نگهداری از لاگ‌های دسترسی فیزیکی برای تاسیسات • بررسی منظم لاگ‌های کنترل دسترسی سازمان باید از دوربین‌های ویدیویی یا مکانیزم‌های کنترل دسترسی (یا هردو) برای نظارت بر دسترسی فیزیکی افراد به مناطق حساس استفاده کند. داده‌های جمع‌آوری شده بررسی شود و با ورودی‌های دیگر همبستگی[2] ایجاد شود و داده‌ها حداقل برای ۳ ماه ذخیره شود (مگر اینکه توسط قانون محدودیت دیگری وجود داشته باشد).

[1] log
[2] Correlate

۵. منابع

https://www.cisecurity.org/controls/v8.1

https://csf.tools/reference/cloud-controls-matrix/v4-0/log/

https://csrc.nist.gov/pubs/sp/800/92/final