

کد اصلی دسته	دسته اصلی	کد زیر دسته اول	زیر دسته اول	دسته دوم کد زیر	زیر دسته دوم	کد زیر دسته سوم	زیر دسته سوم	کد زیر دسته چهارم	زیر دسته چهارم	کد زیر دسته پنجم	زیر دسته پنجم
۰۶	فناوری اطلاعات و ارتباطات و نرم افزارهای رایانه‌ای	۰۴	امنیت فضای تبادل اطلاعات	۰۱	شناسایی	۰۱	راهکارهای افزایش شناخت نسبت به هدف (سازمان، سیستم و غیره)	۰۱	سیستم مدیریت دارایی (با در نظر گرفتن نیازمندی‌های امنیتی)	۰۰	زیر دسته پنجم
								۰۲	سیستم‌های ارزیابی ریسک	۰۰	
								۰۳	انواع سیستم‌های تحلیل شکاف و ممیزی امنیتی روی یک دارایی خاص	۰۰	
				۰۱	۰۱	سیستم‌های تصدیق اصالت، مجازشماری، حسابرسی (AAA)	۰۱	سیستم مدیریت هویت و شناسایی و دسترسی (IAM) و تصدیق اصالت و SSO	۰۰		
							۰۲	سیستم کنترل و نظارت بر استفاده مانند راهکارهای مدیریت تجهیزات موبایل (BYOD و غیره)، سیستم‌های اکانتینگ	۰۱	MDM	
				۰۲	محافظة	سیستم‌های محافظت از داده	۰۱	سیستم‌های مدیریت کلید، مدیریت گواهی، مدیریت امضا، مازول‌های امنیتی نرم / سخت‌افزاری	۰۱	توکن امنیتی هوشمند، SSM، PKI	
							۰۲	سیستم‌ها/ راه‌حل‌های محافظت از محرمانگی و حریم خصوصی داده‌ها (رمزنگاری، Masking، Tokenization و غیره)	۰۱	شبکه اجتماعی امن خاص منظوره	
							۰۳	سیستم‌های محافظت از نشت داده (DLP)	۰۰		
							۰۴	سیستم‌های یک‌طرفه ساز جریان داده (Data Diode)	۰۰		
							۰۵	سیستم‌های مدیریت دسترسی‌های راه دور (PAM)	۰۰		
							۰۶	سیستم‌های پنهان‌نگاری و پنهان‌کاوی	۰۰		
				۰۱	تشخیص	سیستم‌های تحلیل و کشف تقلب	۰۱	سیستم تخصصی تحلیل و محافظت در برابر تهدیدها (STAP)، جعبه شنی (SandBox)، سیستم تشخیص انواع کد بدخواه و بدافزار جدید	۰۱	تشخیص موبایل کد، آنتی‌ویروس	
							۰۲	سیستم‌های تحلیل رفتار کاربر و موجودیت‌ها (UEBA) و شکار تهدیدات (Cyber Threat Hunting)	۰۰		
							۰۳	ظرف و شبکه عسل (Honey Net و Honey Pot)، اتاق انفجار	۰۰		
							۰۱	انواع سیستم‌های تحلیل کد نرم‌افزار (ایستا، پویا و غیره)	۰۰		
				۰۲	ابزارهای پویا، تحلیل و ارزیابی آسیب‌پذیری	ابزارهای پویا، تحلیل و ارزیابی آسیب‌پذیری	۰۲	سیستم‌های پویا آسیب‌پذیری (Vulnerability Scanning)	۰۰		
۰۳	سیستم‌های ارزیابی آسیب‌پذیری (Vulnerability Assessment)	۰۰									
۰۴	سیستم‌های جامع پویا، تحلیل و ارزیابی آسیب‌پذیری: مانند Vulanerability Assement & Scanning	۰۰									

کد دسته اصلی	دسته اصلی	کد زیر دسته اول	زیر دسته اول	دسته دوم	کد زیر دسته سوم	زیر دسته سوم	کد زیر دسته چهارم	زیر دسته چهارم	کد زیر دسته پنجم	زیر دسته پنجم		
۰۶	فناوری اطلاعات و ارتباطات و نرم افزارهای رایانه‌ای	۰۴	امنیت فضای تبادل اطلاعات	۰۷	۰۱	راهکار جامع امنیت اطلاعات	۰۱	انواع ابزار آزمون نفوذ و شبیه‌سازی حملات روی انواع دارایی‌ها	۰۰	ابزارهای تست امنیتی پروتکل‌ها		
							۰۲	انواع ابزارهای آزمون نفوذ برنامه‌های کاربردی وب، ابزارهای آزمون نفوذ تجهیزات و همبندی شبکه	۰۱	حملات کانال‌های نهان		
							۰۳	کشف ادله حادثه	۰۱	انواع چارچوب‌ها، سیستم‌ها و ابزارهای پی‌جویی (Forensics) جرایم شامل: انواع چارچوب‌های انجام پیجویی، سیستم‌های پیجویی: حافظه، سیستم‌عامل، شبکه، فایل و غیره	۰۰	
							۰۴	تحلیل و به اشتراک‌گذاری	۰۲	سیستم‌ها و مراکز تحلیل و به اشتراک‌گذاری اطلاعات و هوشمندی تهدیدات (انواع ISACها) در حوزه‌های مختلف صنعت	۰۰	
							۰۳	مدیریت	۰۱	سیستم‌های مدیریت پاسخگویی به حوادث امنیتی (IRS یا IRMS)	۰۰	
							۰۲	سیستم‌های SOAR	۰۲	سیستم‌های SOAR	۰۰	
							۰۱	سیستم‌های مدیریت BCP و DRP	۰۱	سیستم‌های مدیریت BCP و DRP	۰۰	
							۰۱	بازیابی از حوادث و ادامه کسب‌وکار	۰۱	سیستم‌های امحا و بازیابی داده	۰۰	
							۰۶	مدیریت امنیت اطلاعات	۰۱	سیستم‌های مدیریت خط‌مشی‌های امنیت اطلاعات	۰۰	
							۰۲	حاکمیت و نگهداری اطلاعات	۰۲	سیستم‌های مدیریت ریسک	۰۰	
							۰۳	سیستم به‌روزرسانی و مدیریت وصله‌های امنیتی	۰۳	سیستم به‌روزرسانی و مدیریت وصله‌های امنیتی	۰۰	
							۰۴	راهکار جامع مدیریت امنیت اطلاعات مانند سیستم مدیریت حاکمیت، ریسک و تطابق، ISMS	۰۴	راهکار جامع مدیریت امنیت اطلاعات مانند سیستم مدیریت حاکمیت، ریسک و تطابق، ISMS	۰۰	
							۰۱	سیستم یکپارچه مدیریت تهدیدات (UTM)	۰۱	سیستم یکپارچه مدیریت تهدیدات (UTM)	۰۰	
							۰۲	انواع مازول‌های سیستم امنیتی نقطه پایانی (EPS یا EDR یا EPP) و سیستم‌های ضد بدافزار	۰۲	انواع مازول‌های سیستم امنیتی نقطه پایانی (EPS یا EDR یا EPP) و سیستم‌های ضد بدافزار	۰۱	مانند انواع آنتی‌ویروس، App White Listing و غیره
							۰۳	سیستم‌های تحلیل ترافیک پیشرفته امنیتی	۰۲	سیستم‌های تحلیل ترافیک پیشرفته امنیتی	۰۲	بازرسی عمیق بسته (DPI)
							۰۴	انواع سیستم‌های تشخیص/مقابله با نفوذ (شبکه، میزبان و غیره) مانند: HIDS, ... NIDPS	۰۳	سیستم‌های تحلیل ترافیک پیشرفته امنیتی	۰۳	NTA
							۰۵	انواع راه‌حل‌های دیوارها و دروازه‌های امنیتی شامل انواع دیوارهای آتش و دروازه‌های امنیتی مانند دروازه‌های ایمیل	۰۴	انواع سیستم‌های تشخیص/مقابله با نفوذ (شبکه، میزبان و غیره) مانند: HIDS, ... NIDPS	۰۱	APT و DDoS
							۰۶	سیستم‌های ترکیبی ممیزی و مقاوم‌سازی امنیتی روی انواع دارایی	۰۵	انواع راه‌حل‌های دیوارها و دروازه‌های امنیتی شامل انواع دیوارهای آتش و دروازه‌های امنیتی مانند دروازه‌های ایمیل	۰۱	دیوار آتش شبکه، دیوار آتش نرم‌افزار یا برنامه‌های کاربردی (WAF)، دیوار آتش پایگاه داده، دروازه‌های امن ایمیل
							۰۷	سیستم مدیریت و تحلیل اطلاعات، رویدادها و لاگ‌های امنیتی	۰۶	سیستم‌های ترکیبی ممیزی و مقاوم‌سازی امنیتی روی انواع دارایی	۰۱	سیستم‌های ممیزی و امن سازی تجهیزات شبکه و انواع سرویس‌های پایه‌ای (مانند امن سازی پایگاه داده، Active Directory، وب سرور، ایمیل و ...)
								مانند Managed Security و SoC SIEM Services، سیستم‌های مدیریت لاگ	۰۷	سیستم مدیریت و تحلیل اطلاعات، رویدادها و لاگ‌های امنیتی	۰۱	مانند Managed Security و SoC SIEM Services، سیستم‌های مدیریت لاگ