



مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای



وزارت ارتباطات و فناوری اطلاعات  
سازمان فناوری اطلاعات ایران



دانشگاه فردوسی مشهد

آزمایشگاه تخصصی آفا

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

# مدیریت رخدادهای امنیت رایانه‌ای و تشکیل تیم‌های CERT سازمانی

احسان طیرانی راد

مدیر آموزش و روابط عمومی آزمایشگاه تخصصی آفا

دانشگاه فردوسی مشهد

سمینار آموزشی مدیران و کارشناسان فناوری اطلاعات و ارتباطات استان بوشهر - ۱۰ شهریور ۱۳۹۵



# مدیریت رخدادهای امنیت رایانه‌ای

مفاهیم

# امنیت فاوا

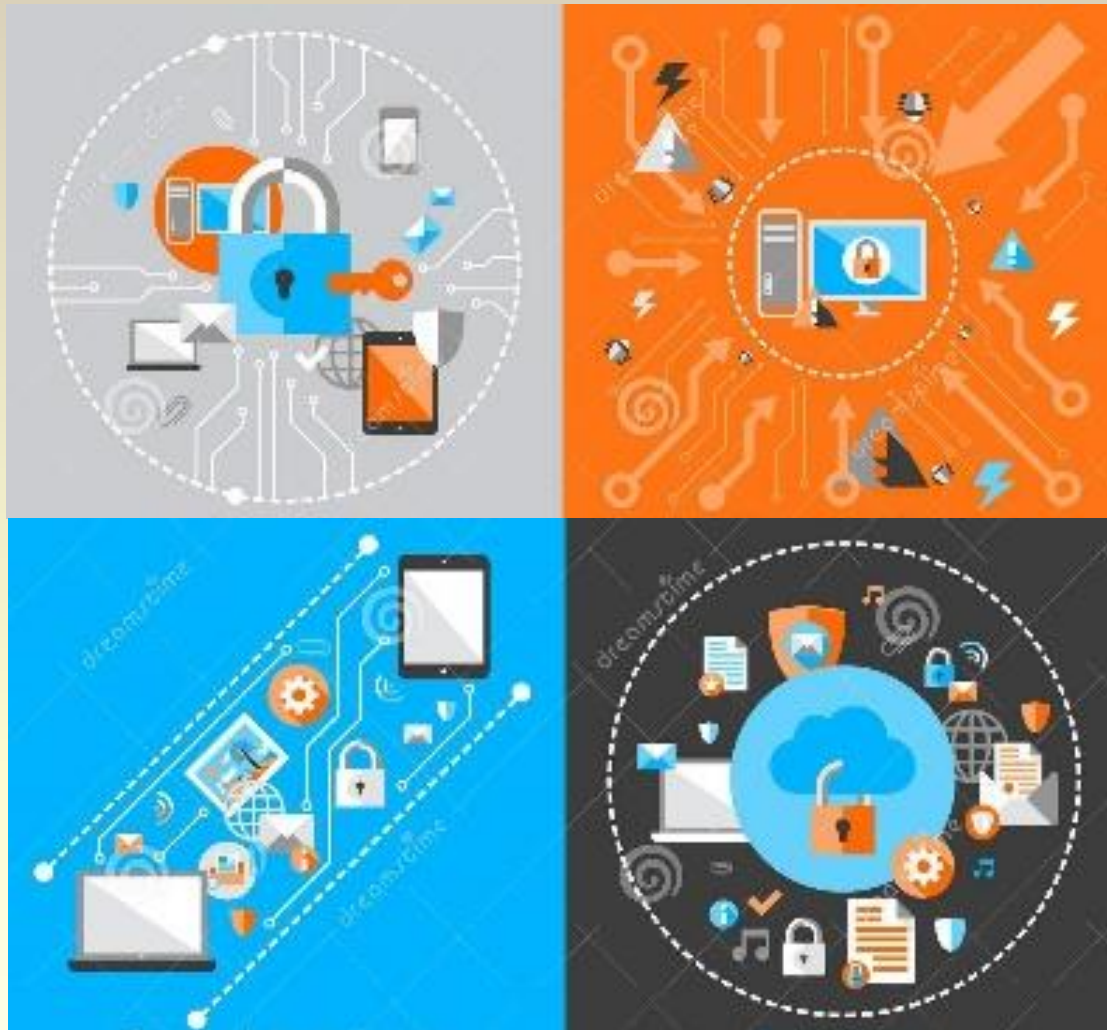
- به طور کلی امنیت رایانه‌ای مجموعه‌ای از راه‌حل‌های فنی برای مشکلات غیرفنی است.
- وظیفه متخصصان امنیتی کمک به سازمان در تصمیم‌گیری در مورد زمان و هزینه‌ای است که می‌خواهد برای مساله امنیت اختصاص دهند.
- در سازمان‌ها آگاهی از امنیت و سیاست امنیتی باید از بالا به پایین گسترش یابد.



# اهداف مدیریت رخدادهای امنیت اطلاعات

- آشکارسازی، گزارش و ارزیابی رخدادهای امنیت اطلاعات
- پاسخ به رخدادهای امنیت اطلاعات که شامل فعال سازی کنترل های مناسب پیشگیری، کاهش و بازبازی تاثیرات می باشد
- گزارش آسیب پذیری های امنیت اطلاعات که هنوز به عنوان عامل آسیب ها بهره برداری نشده اند و ارزیابی و برخورد صحیح با آنها
- درس گرفتن از رخداد امنیت اطلاعات و آسیب پذیری ها، پی ریزی کنترل های پیشگیرانه، و بهبود رویکرد کلی مدیریت رخدادهای امنیت اطلاعات

# گام‌های اصلی برای کاهش اثر رخدادهای امنیتی اطلاعات



■ توقف و محدودیت

■ ریشه‌کشی

■ تحلیل و گزارش

■ پیگیری

# برنامه‌ریزی مبتنی بر نیازهای امنیتی



■ برنامه‌ریزی برای تعیین نیازهای امنیتی

■ ارزیابی مخاطره و انتخاب بهترین شیوه‌ها

■ ایجاد سیاست‌هایی برای انعکاس نیازها

■ پیاده‌سازی امنیت

■ بررسی و واکنش به وقایع

# تکامل چرخه دانش امنیت



■ دریافت حوادث

■ تحلیل اولیه

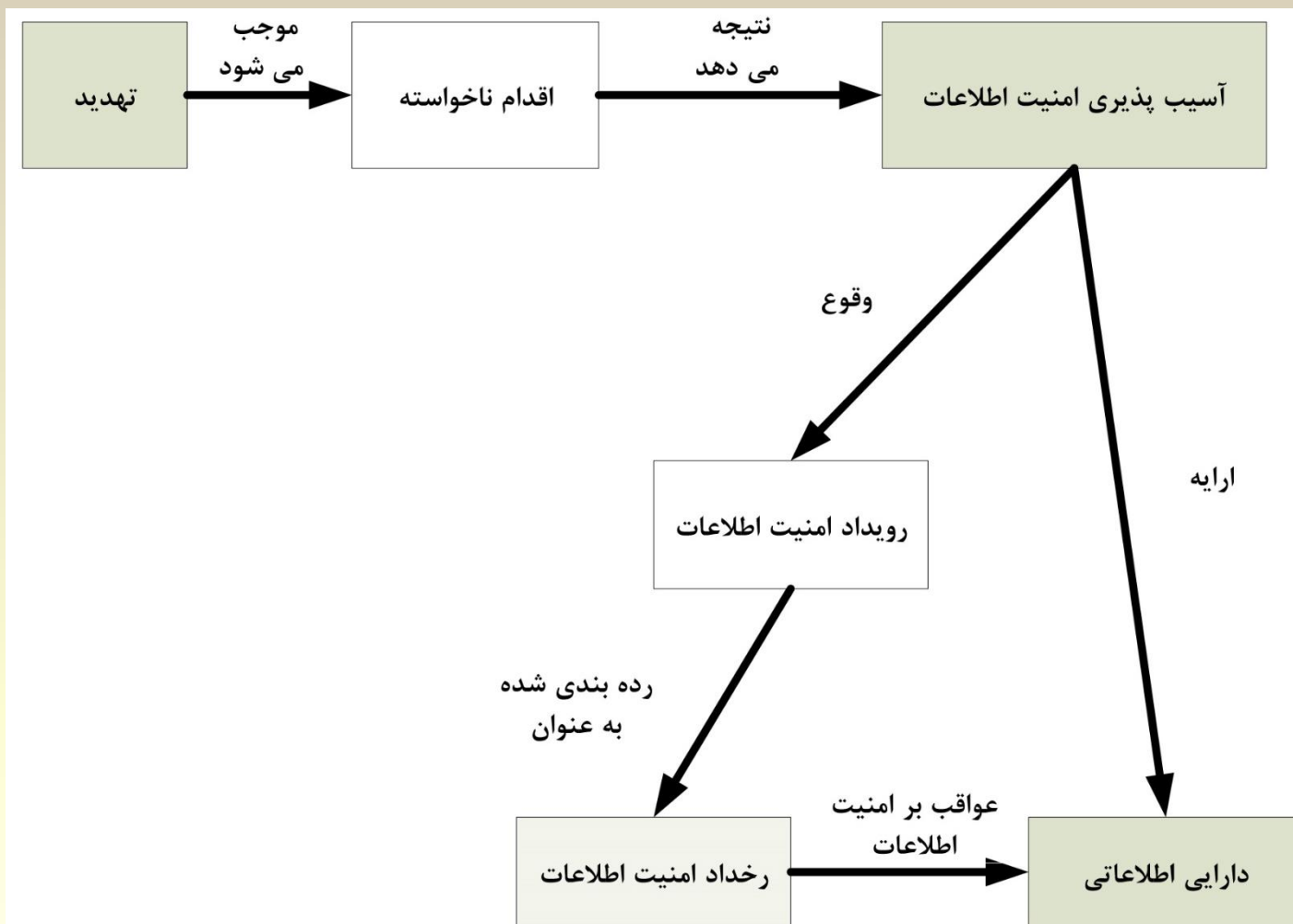
■ اقدامات کنترلی

■ مستندسازی

■ تجزیه و تحلیل عمیق

■ اطلاع رسانی و اقدامات نهایی

# مدیریت رخدادهای امنیت اطلاعات





# مراحل مدیریت رخدادهای امنیت اطلاعات

■ برنامه ریزی و آماده سازی

■ آشکارسازی و گزارش

■ ارزیابی و تصمیم گیری

■ پاسخ گویی

■ درس های آموخته شده

## برنامه ریزی و آماده سازی

- خط مشی مدیریت رخداد امنیت اطلاعات و تعهد مدیریت ارشد
- خط مشی های امنیت اطلاعات و مدیریت مخاطره روزآمد در هر دو سطح سازمانی و سطح سامانه، خدمت و شبکه
- طرحواره ی مدیریت رخداد امنیت اطلاعات
- تاسیس ISIRT
- پشتیبانی فنی و غیره (شامل پشتیبانی عملیات)
- اطلاع رسانی در مورد مدیریت رخداد امنیت اطلاعات با جلسات توجیهی و آموزش
- آزمون طرحواره ی مدیریت رخداد امنیت اطلاعات

## آشکارسازی و گزارش

- آشکارسازی و گزارش دهی رویداد امنیت اطلاعات

## ارزیابی و تصمیم گیری

- ارزیابی رویداد امنیت اطلاعات و تصمیم گیری درباره رخداد امنیت اطلاعات بودن آن

# مراحل مدیریت رخدادهای امنیت اطلاعات

■ برنامه ریزی و آماده سازی

■ آشکار سازی و گزارش

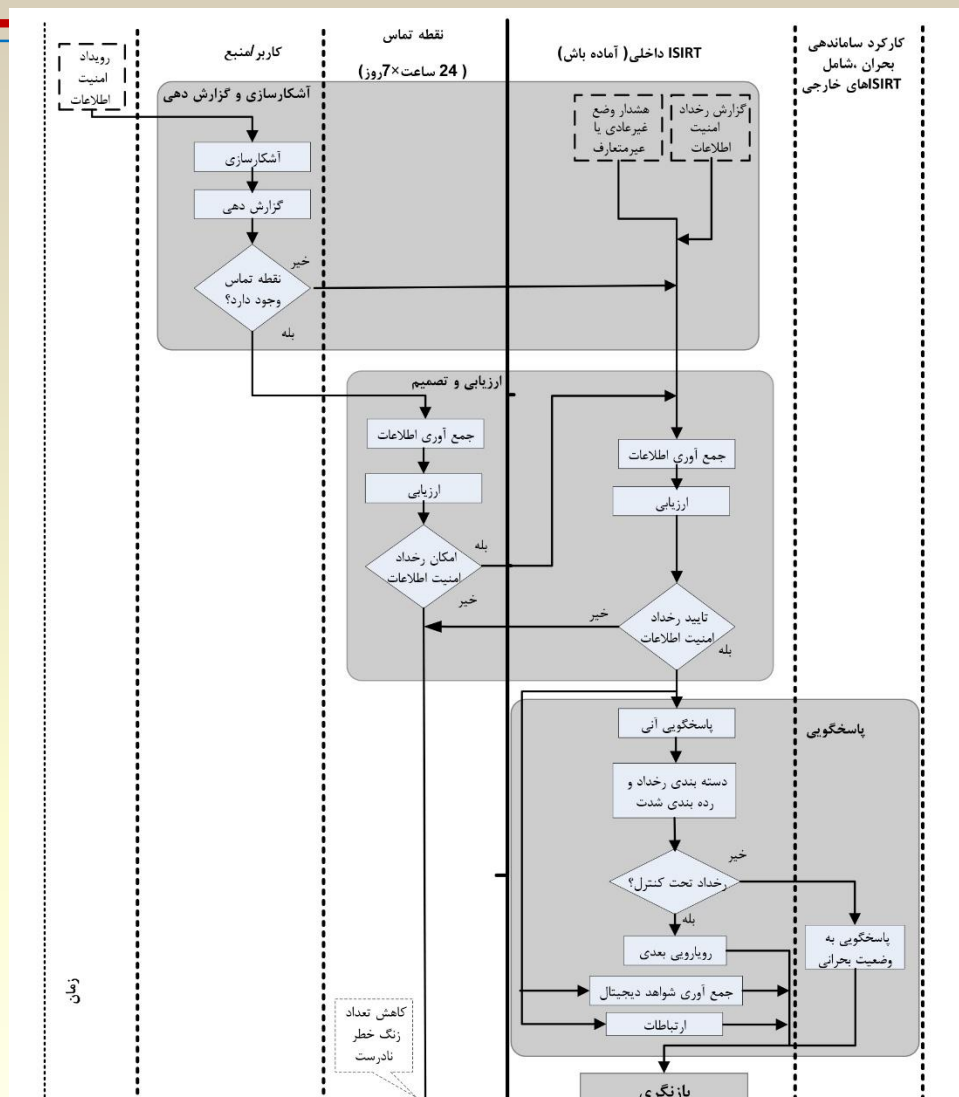
■ ارزیابی و تصمیم گیری

■ پاسخ گویی

■ درس های آموخته شده



# نمودار جریان رویداد و رخداد امنیت اطلاعات



# COMPUTER EMERGENCY RESPONSE TEAM (CERT)

گروه پاسخ گویی به فوریت های رایانه ای

# گروه پاسخ‌گویی به فوریت‌های رایانه‌ای



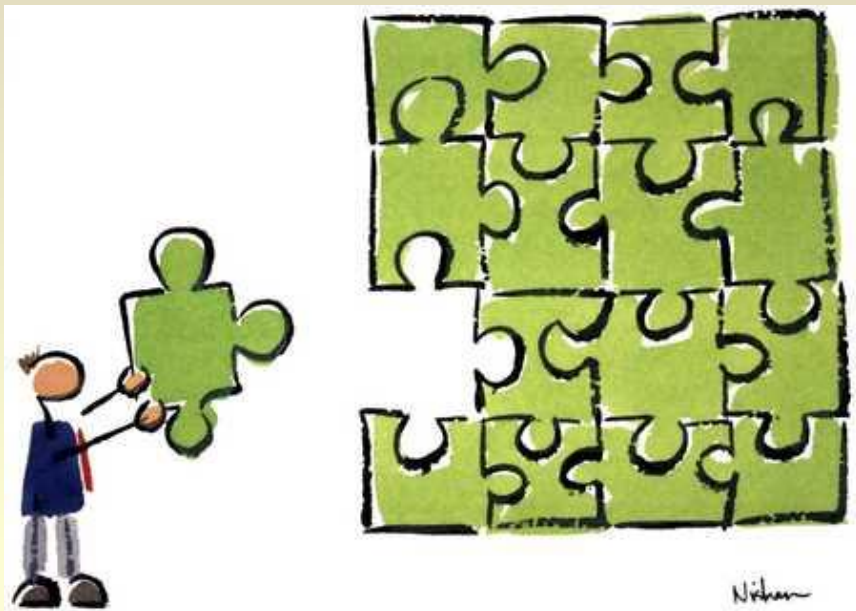
- یک واحد خدماتی که مسوول دریافت، مرور و پاسخ‌گویی به گزارشات ارسالی، مشکلات و رخدادهای کامپیوتری است.
- سرعت در تشخیص، تحلیل و پاسخ‌گویی به مشکل امنیتی، میزان خطر، شدت تنش، گستردگی حوزه تاثیر و هزینه ترمیم آن را کاهش می‌دهد.

# اهداف اصلی

■ کمینه و کنترل کردن خسارت

■ فراهم آوردن پاسخ و روش ترمیم مناسب

■ یافتن روش‌هایی برای جلوگیری از رخداد بعدی



# مزایا

- ایجاد واحدی متمرکز برای مدیریت موارد امنیتی فناوری اطلاعات و ارتباطات
- ایجاد یک مرکز تماس امنیت رایانه‌ای و دسترسی سریع و بدون واسطه کاربران
- پاسخ‌گویی متمرکز و تخصصی به مسائل امنیتی
- کمک‌رسانی و امداد به موقع توسط متخصصان سازمان، در زمان‌های بحرانی
- آگاهی به مسائل حقوقی مرتبط در هنگام دادخواهی‌های حقوقی
- پیگیری، توسعه و پیشرفت سیاست‌های امنیتی سازمان
- همکاری و آگاهی‌رسانی هم‌زمان به کاربران در زمینه امنیت فاوا

# ماموریت‌ها و وظایف

- مدیریت رویدادهای امنیت فناوری اطلاعات و ارتباطات سازمان (جمع‌آوری اطلاعات، تحلیل، پاسخ‌گویی و پشتیبانی)
- مدیریت رخدادهای امنیت فناوری اطلاعات و ارتباطات سازمان (جمع‌آوری اطلاعات، تحلیل، پاسخ‌گویی، امداد و پشتیبانی)
- آگاهی‌رسانی، توان‌مندسازی و انتشار دانش
- طراحی و تدوین سیاست‌ها و راهبردهای ارتقای امنیت فناوری اطلاعات سازمان از قبیل راهبردهای کاهش‌دهنده مخاطرات و اقدام‌های پیش‌گیرانه
- تدوین آئین‌نامه‌ها، دستورالعمل‌ها و پروتکل‌های امنیتی سازمان
- اجرا و پیاده‌سازی سامانه مدیریت امنیت اطلاعات (ISMS) در سازمان
- کمک و همکاری در توسعه کمی و کیفی و ارتقای امنیت فناوری اطلاعات و ارتباطات با همکاران و تامین‌کنندگان



# اسامی مختلف CERT

CSIRT	Computer Security Incident Response Team	تیم پاسخگویی به رخداد امنیتی کامپیوتری
CSIRC	Computer Security Incident Response Capability	توانایی پاسخگویی به رخداد امنیتی کامپیوتری
CIRC	Computer Incident Response Capability	توانایی پاسخگویی به رخداد کامپیوتری
CIRT	Computer Incident Response Team	تیم پاسخگویی به رخداد کامپیوتری
IHT	Incident Handling Team	تیم رسیدگی به رویداد
IRC	Incident Response Center or Incident Response Capability	مرکز پاسخگویی به رخداد یا توانایی پاسخگویی به رخداد
IRT	Incident Response Team	تیم پاسخگویی به رخداد
SERT	Security Emergency Response Team	تیم پاسخگویی به فوریت های امنیتی
CERT	Computer Emergency Response Team	تیم پاسخگویی به فوریت های کامپیوتری
SIRT	Security Incident Response Team	تیم پاسخگویی به رخداد امنیتی

# اسامی مختلف CERT در داخل کشور



مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای

■ ماهر: مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای

■ گوهر: گروه واکنش هماهنگ رخداد

■ مهار: مرکز هماهنگی امداد رایانه‌ای

■ آپا: آگاهی رسانی، پشتیبانی و امداد



# نکات مهم در ایجاد CERT



- ایجاد CERT، پروژه ای زمان بر است.
- جمع آوری اطلاعات برای این پروژه از اهمیت به سزایی برخوردار است.
- ایجاد و بهره برداری از CERT هزینه زیادی می طلبد.
- نیاز به جابجایی و انتقال نیروها جهت استقرار در تیم وجود خواهد داشت.
- کسب مقبولیت یک تیم در حوزه فعالیت خود با کیفیت محصولات و خدماتی که ارائه می کند، ممکن می شود اما نیازمند زمان است.
- قابلیت اعتماد مهمترین عامل موفقیت است.

# انواع گروه‌های پاسخگویی به حوادث رایانه‌ای



## ■ موردی

- گردهم‌آیی در زمان نیاز
- وظایف غیر رسمی
- به شکل رسمی وظیفه پاسخگویی ندارد

## ■ رسمی

- گزارش‌دهی
- بررسی
- پاسخگویی

# انواع سرویس‌ها

■ سرویس‌ها بر اساس نیاز تعریف می‌شوند

■ سازمان سرویس‌ها را تعیین می‌کند

■ سرویس‌های عمومی

■ سرویس‌های پیشگیرانه

■ سرویس‌های واکنشی

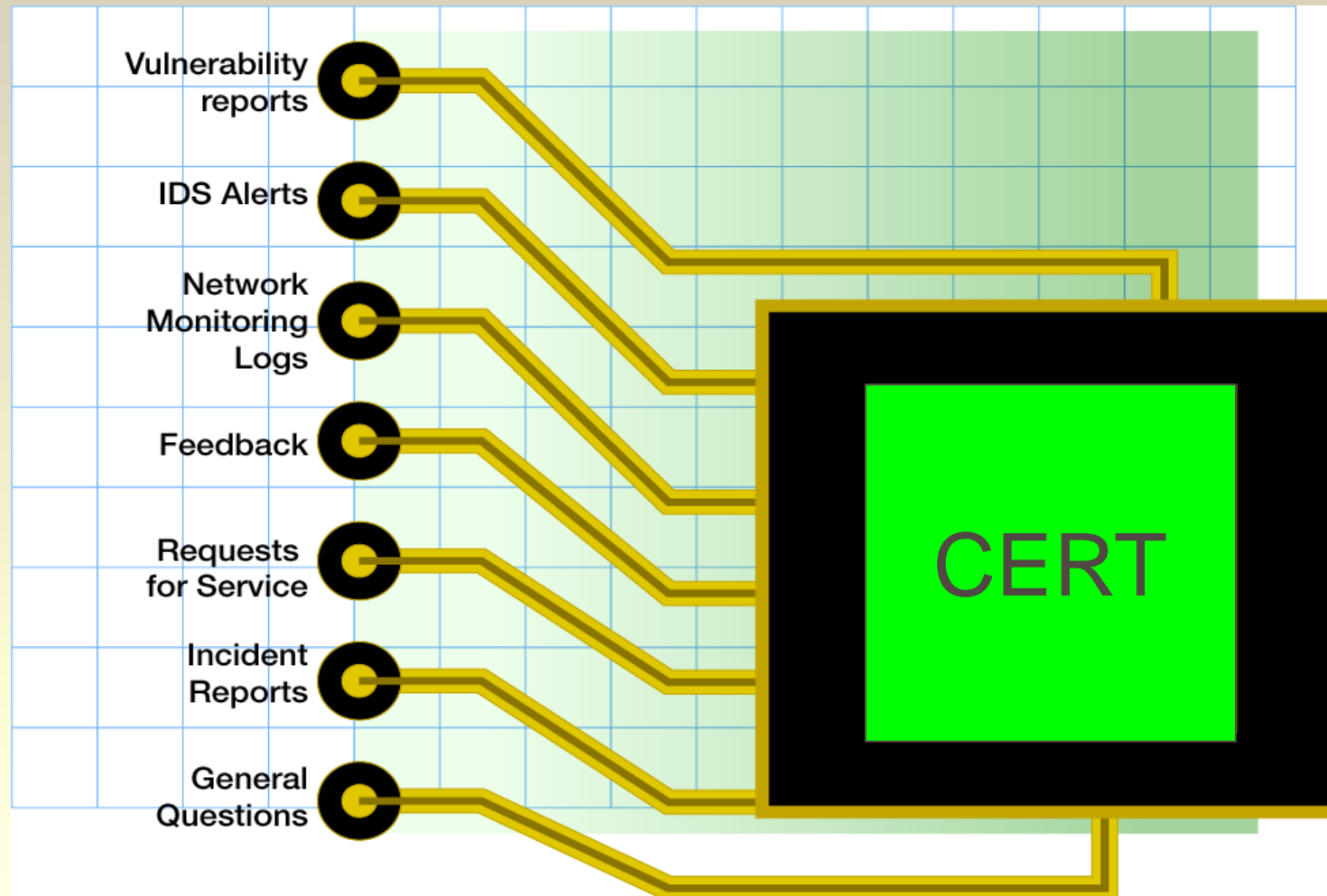
■ سرویس‌های مدیریت کیفیت امنیت



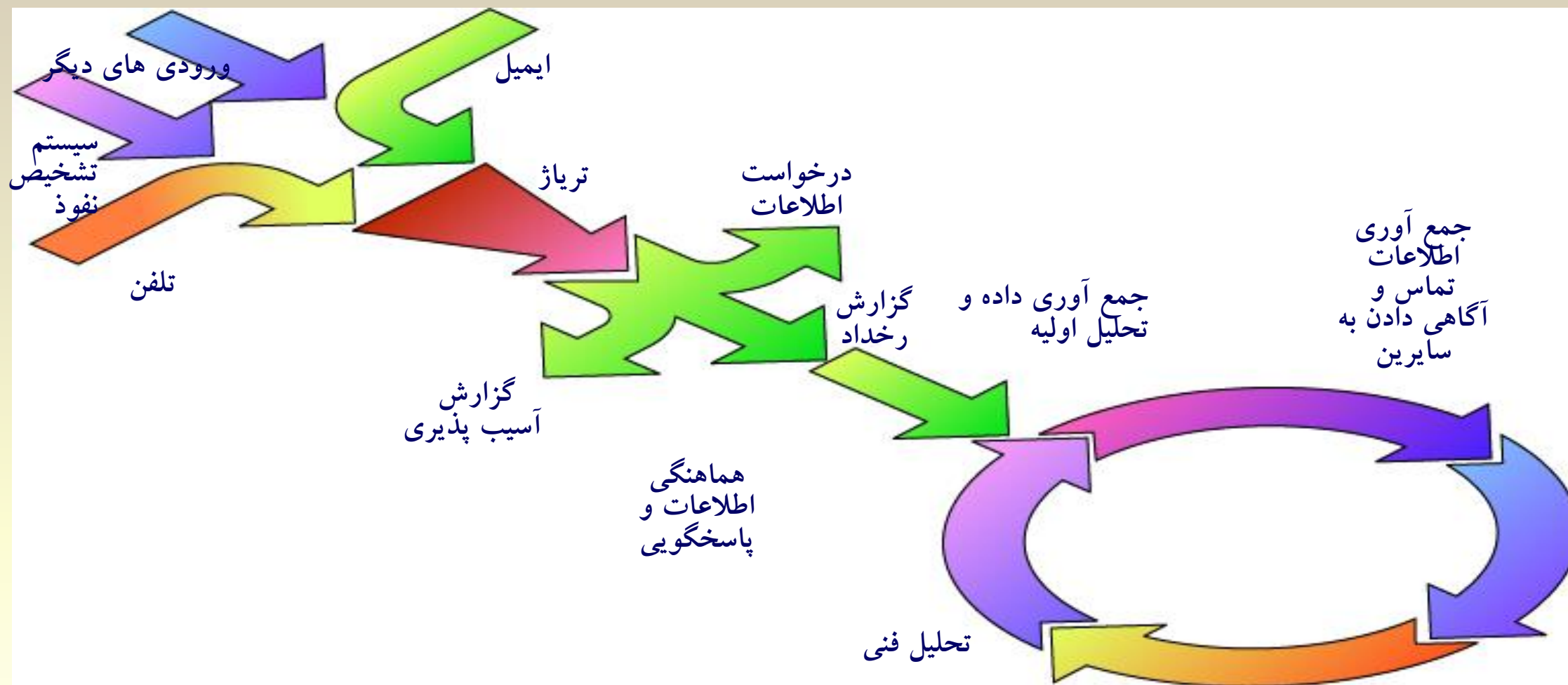
# سرویس‌های عمومی

سرویس‌های مدیریت کیفیت امنیت	سرویس‌های واکنشی	سرویس‌های پیشگیرانه
تحلیل ریسک	اعلام اخطار و هشدار	اعلان‌ها
طرح ترمیم خرابی و تداوم کار	رسیدگی به رخداد (تحلیل، پاسخگویی در محل، پشتیبانی پاسخگویی، هماهنگی در پاسخگویی)	پایش فناوری
		بررسی و ارزیابی امنیتی
		توسعه ابزارهای امنیتی
مشاوره امنیتی	مدیریت آسیب پذیری (تحلیل، پاسخگویی، هماهنگی پاسخگویی)	سرویس‌های تشخیص نفوذ
آگاه سازی		انتشار اطلاعات مربوط به امنیت
آموزش	مدیریت آثار باقیمانده از حمله (تحلیل، پاسخگویی، هماهنگی پاسخگویی)	پیکربندی و نگهداری ابزارها، برنامه‌های کاربردی، زیرساخت‌ها و سرویس‌های امنیتی
ارزیابی و تایید محصول		

# ورودی‌های CERT



# مراحل دریافت گزارش رخداد و پاسخگویی به آن در CERT



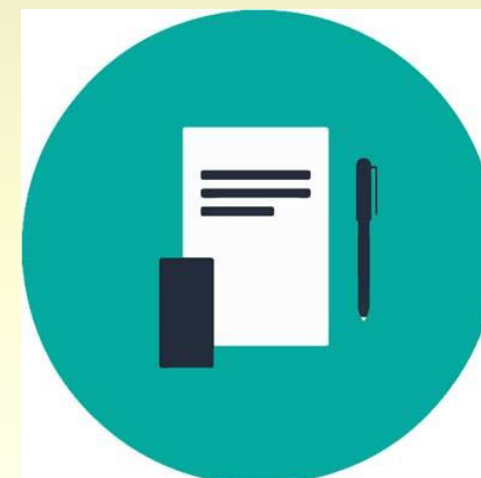
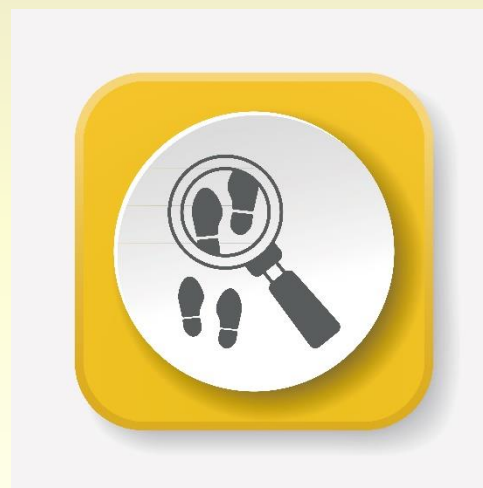
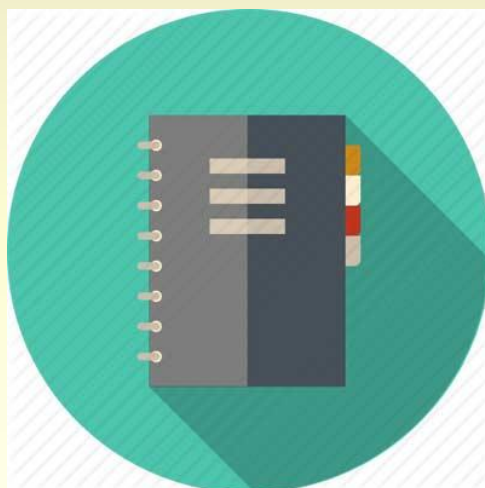


# اهداف کاربری سرویس‌های پیشگیرانه

■ بهبود قبل از وقوع حادثه

■ کاهش اثرات حادثه

■ کاهش حادثه در بلند مدت



# سرویس‌های پیشگیرانه

■ اعلان‌ها

■ بررسی و نظارت بر فناوری‌های جدید در سازمان

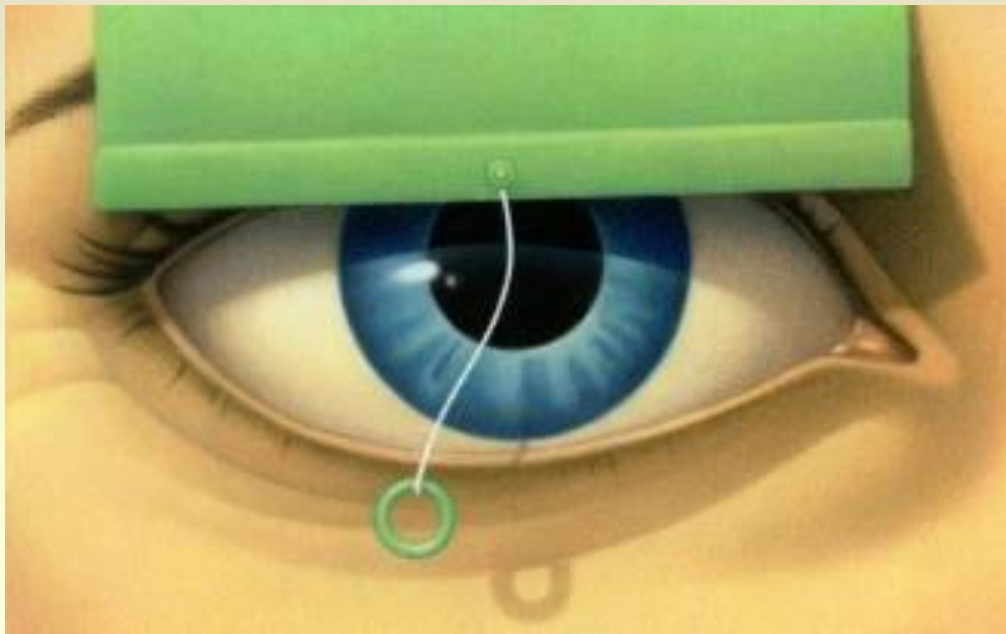
■ بررسی و ارزیابی مداوم امنیت

■ تنظیم امنیتی سرویس‌ها

■ طراحی و ایجاد ابزارهای امنیتی

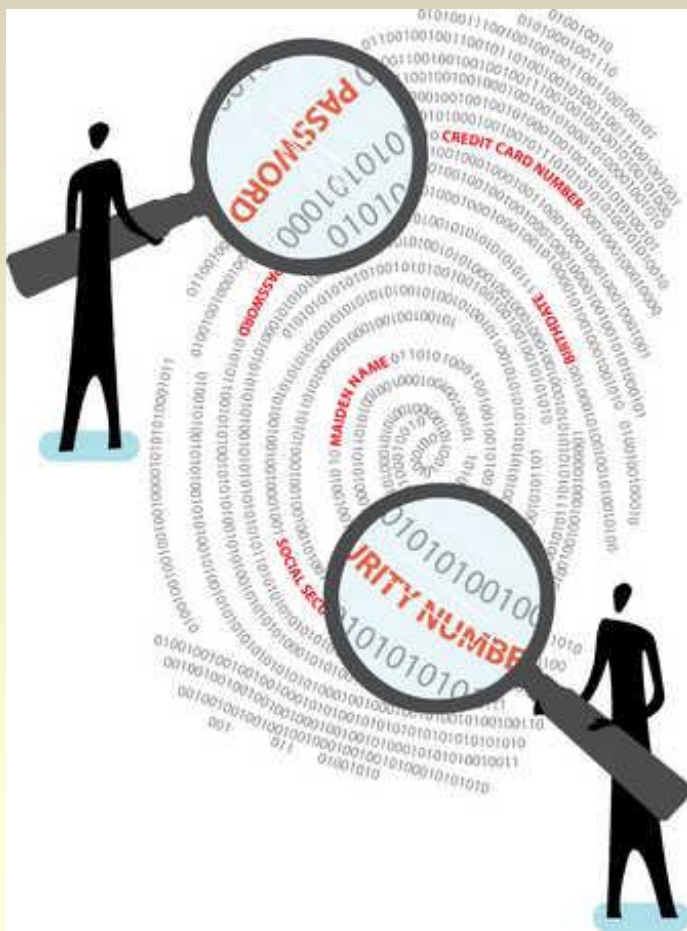
■ آزمون نفوذپذیری متناوب

■ نشر مطالب امنیتی



# اهداف کاربر بست سرویس های واکنشی

- پاسخ به درخواست گزارش آسیب پذیری
- آنالیز رویداد
- بیان علت رویداد
- تصمیم گیری و پیاده سازی روش های ترمیم
- سیاست گذاری برای جلوگیری
- جمع آوری گزارشات
- بررسی مجموعه گزارش ها
- به اشتراک گذاری نتایج
- هشدار به سایر تیم ها



# سرویس‌های واکنشی

---

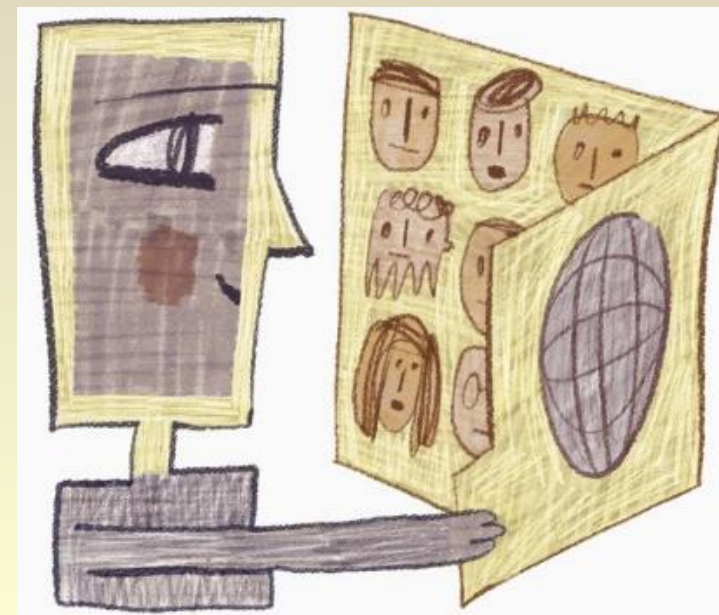
- اخطارها و هشدارها
- بررسی حوادث
- بررسی آسیب‌پذیری‌ها
- بررسی کدهای مخرب

# سرویس‌های واکنشی

## ■ اختارها و هشدارها

■ انتشار اطلاعات

■ تهیه راهنمای حفاظتی - امنیتی



# سرویس‌های واکنشی

## ■ بررسی حوادث

■ تحلیل حادثه

■ جمع‌آوری مدارک قانونی

■ ردیابی و جستجوی سرچشمه مشکلات

■ پاسخگویی در محل

■ پشتیبانی

■ هماهنگی بین گروه‌های زیرمجموعه



# سرویس‌های واکنشی

## ■ بررسی آسیب‌پذیری‌ها

■ تحلیل آسیب‌پذیری‌ها

■ ایجاد راهکارهای مناسب

■ هماهنگی





# سرویس‌های واکنشی

## ■ بررسی کدهای مخرب

■ تحلیل کدهای مخرب

■ ایجاد راهکارهای مناسب

■ هماهنگی





# سرویس‌های مدیریت کیفیت امنیت

- مطالعه مستندات جمع‌آوری شده در حملات قبلی

- تحلیل ریسک‌ها

- دریافت و ارائه مشاوره‌های امنیتی

- آموزش

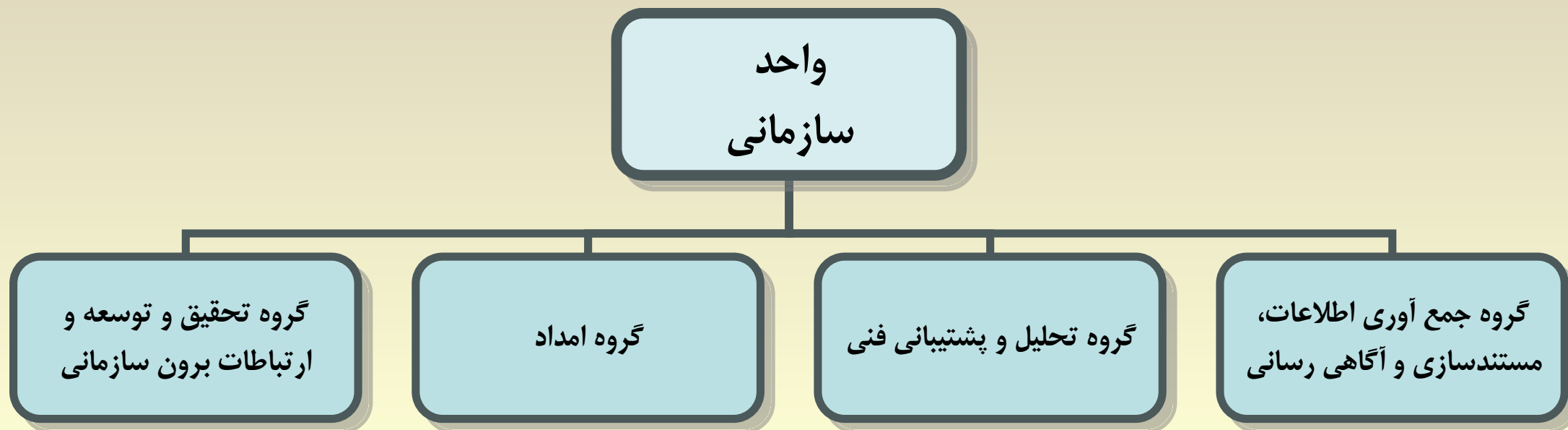
- ارزیابی و تست محصولات

- ارزیابی گواهی‌نامه‌های دریافت شده



# ساختار پیشنهادی

# ساختار پیشنهادی



# گروه جمع‌آوری اطلاعات، مستندسازی و آگاهی‌رسانی

- این گروه وظیفه جمع‌آوری اطلاعات، اخبار امنیتی، ابزارها و سایر موارد مرتبط و مورد نیاز را بر عهده دارد.
- تنظیم مستندات جهت انتشار به منظور آگاهی‌رسانی نیز از جمله وظایف این گروه می‌باشد.

# گروه تحلیل و پشتیبانی فنی

■ این گروه وظیفه ارائه راهنمایی‌های امنیتی، پاسخگویی به سؤال‌ها و تحلیل رویدادها را برعهده دارد.

■ کنترل و پیگیری آسیب‌پذیری‌ها، توسعه ابزار امنیتی، پیکربندی و پشتیبانی سامانه‌ها و شبکه‌های رایانه‌ای، بررسی و ممیزی‌های مربوط به امنیت از دیگر وظایف این گروه است.

# گروه امداد

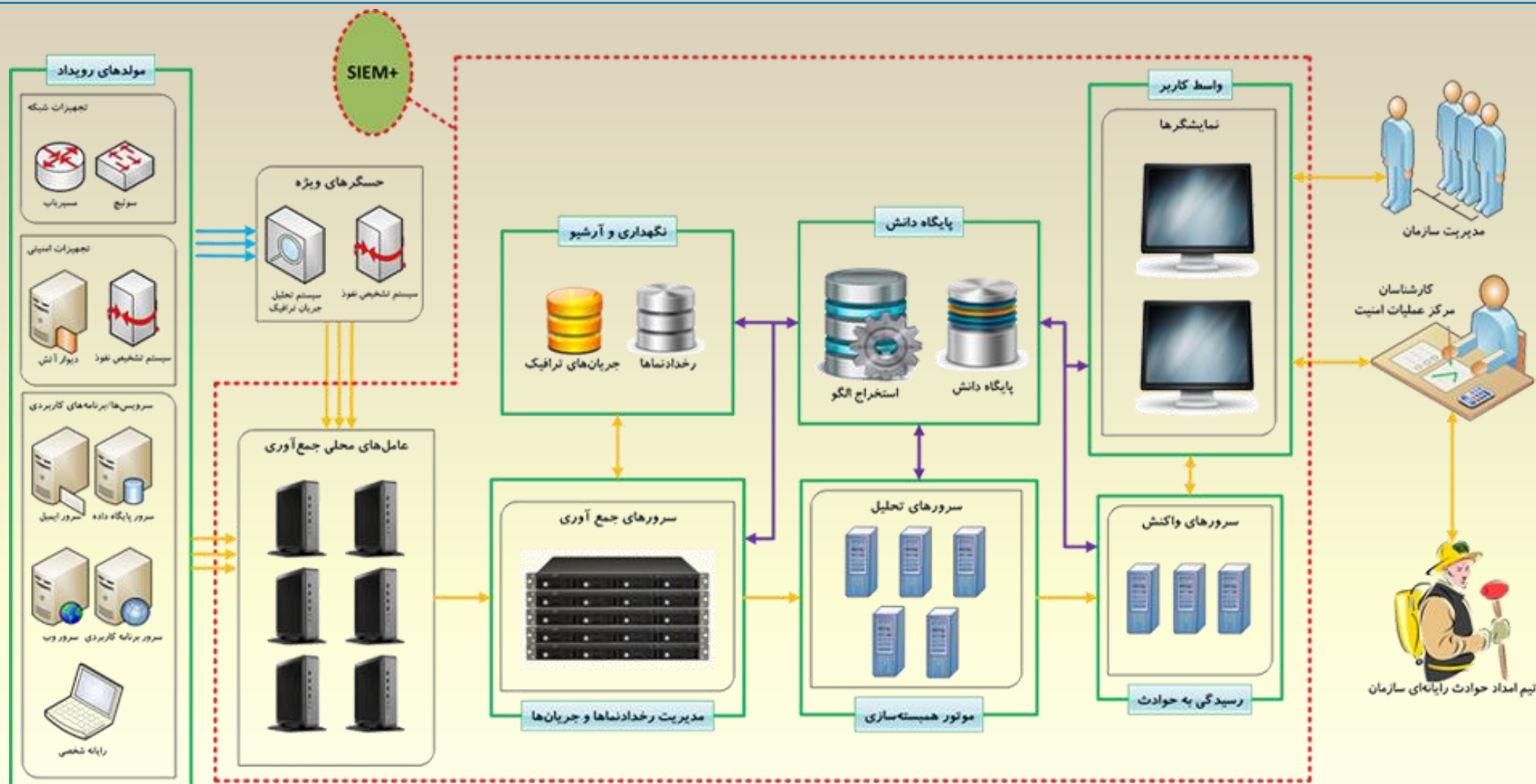
- وظیفه پاسخ‌گویی به حوادث در محل و امداد در هنگام وقوع حادثه امنیتی و پیگیری‌ها و پشتیبانی‌های مورد نیاز پس از حادثه نیز بر عهده این گروه است.

# گروه تحقیق و توسعه و ارتباطات برون سازمانی

---

- این گروه وظیفه تضمین کیفیت در خدمات ارائه شده را برعهده دارد.
- نظارت بر فناوری ها و ارائه راهکارهای جدید برای ارائه خدمات و ارتباطات برون سازمانی هم با تامین کنندگان و هم با دیگر مراکز مشابه از وظایف این گروه می باشد.

# مرکز عملیات امنیت





# از بذل توجهتان متشکرم

<http://cert.um.ac.ir>

[tayarani@um.ac.ir](mailto:tayarani@um.ac.ir)