بسم الله الرحمن الرحیم

مرکز ماهر
مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

دانشگاه فردوسی مشهد
آزمایشگاه تخصصی آپا

مدیریت رخدادهای امنیت رایانه‌ای و تشکیل تیم‌های CERT سازمانی

احسان طیرانی راد
مدیر آموزش و روابط‌عمومی آزمایشگاه تخصصی آپا
دانشگاه فردوسی مشهد

سمینار آموزشی مدیران و کارشناسان فناوری اطلاعات و ارتباطات استان آذربایجان غربی – ۲۶ مرداد ۱۳۹۵

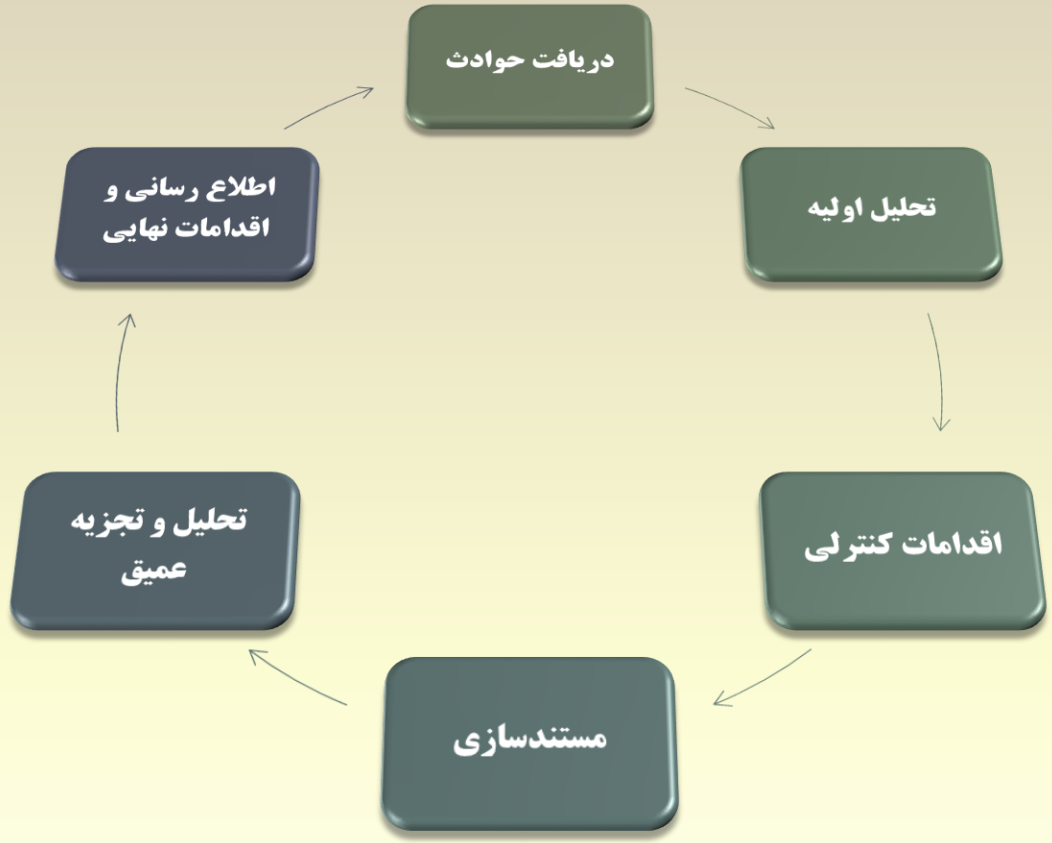
مدیریت رخدادهای امنیت رایانه‌ای

مفاهیم

امنیت فاوا

- به‌طور کلی امنیت رایانه‌ای مجموعه‌ای از راه‌حل‌های فنی برای مشکلات غیرفنی است.
- وظیفهٔ 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 پائین گسترش یابد.

تکامل چرخه دانش امنیت



- دریافت حوادث
- تحلیل اولیه
- اقدامات کنترلی
- مستندسازی
- تجزیه و تحلیل عمیق
- اطلاع رسانی و اقدامات نهایی

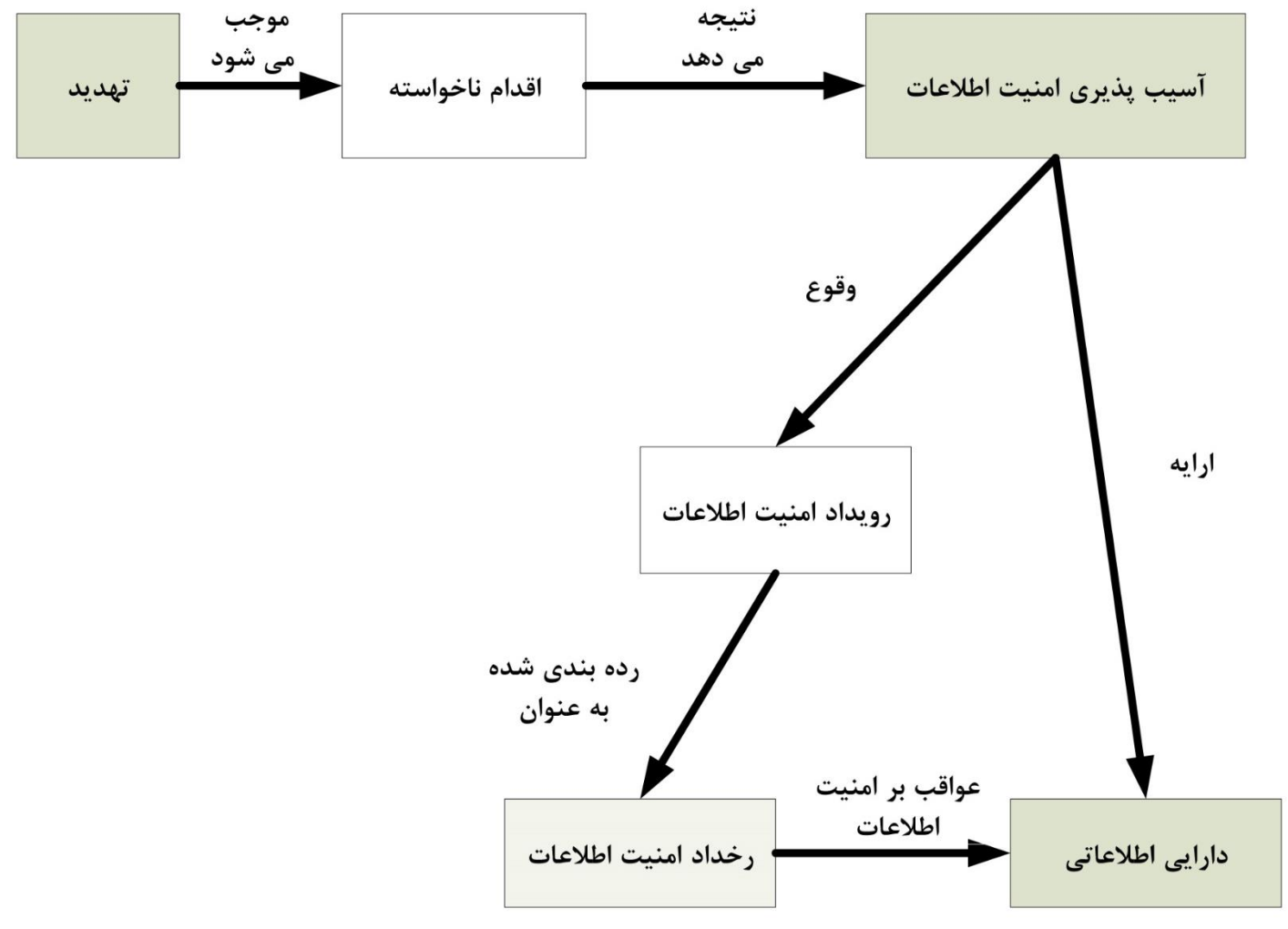
برنامه‌ریزی مبتنی بر نیازهای امنیتی

- برنامه‌ریزی برای تعیین نیازهای امنیتی
- ارزیابی مخاطره و انتخاب بهترین شیوه‌ها
- ایجاد سیاست‌هایی برای انعکاس نیازها
- پیاده‌سازی امنیت
- بررسی و واکنش به وقایع

اهداف مدیریت رخداد امنیت اطلاعات

- آشکارسازی، گزارش و ارزیابی رخدادهای امنیت اطلاعات
- پاسخ به رخدادهای امنیت اطلاعات که شامل فعال‌سازی کنترل‌های مناسب پیشگیری، کاهش و بازیابی تاثیرات می‌باشد
- گزارش آسیب‌پذیری‌های امنیت اطلاعات که هنوز به عنوان عامل آسیب‌ها بهره‌برداری نشده‌اند و ارزیابی و برخورد صحیح با آن‌ها
- درس گرفتن از رخداد امنیت اطلاعات و آسیب‌پذیری‌ها، پی‌ریزی کنترل‌های پیشگیرانه، و بهبود رویکرد کلی مدیریت رخداد امنیت اطلاعات

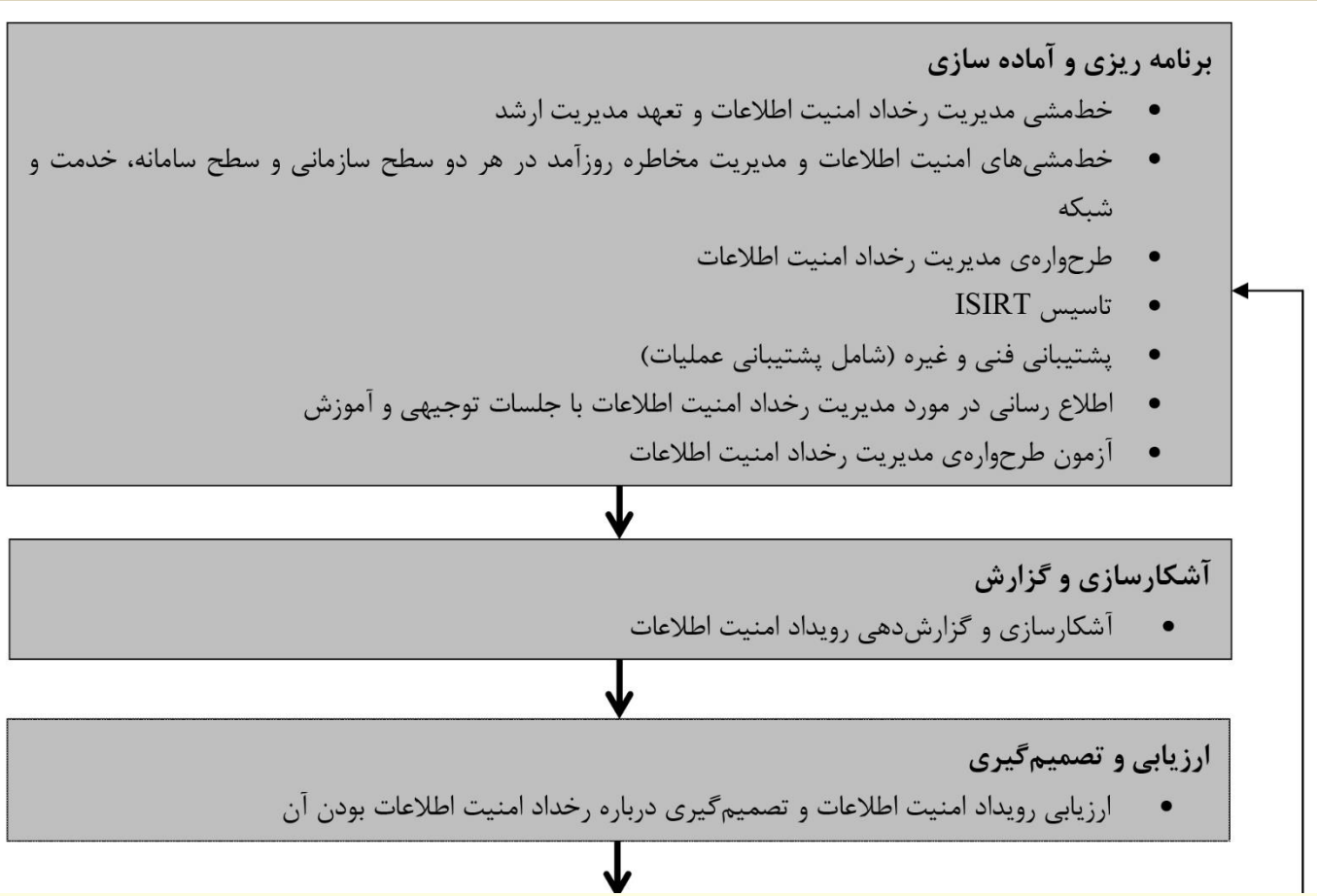
مدیریت رخداد امنیت اطلاعات



گام‌های اصلی برای کاهش اثر رخداد امنیت اطلاعات

- توقف و محدودیت
- ریشه‌کنی
- تحلیل و گزارش
- پیگیری

مراحل مدیریت رخداد امنیت اطلاعات

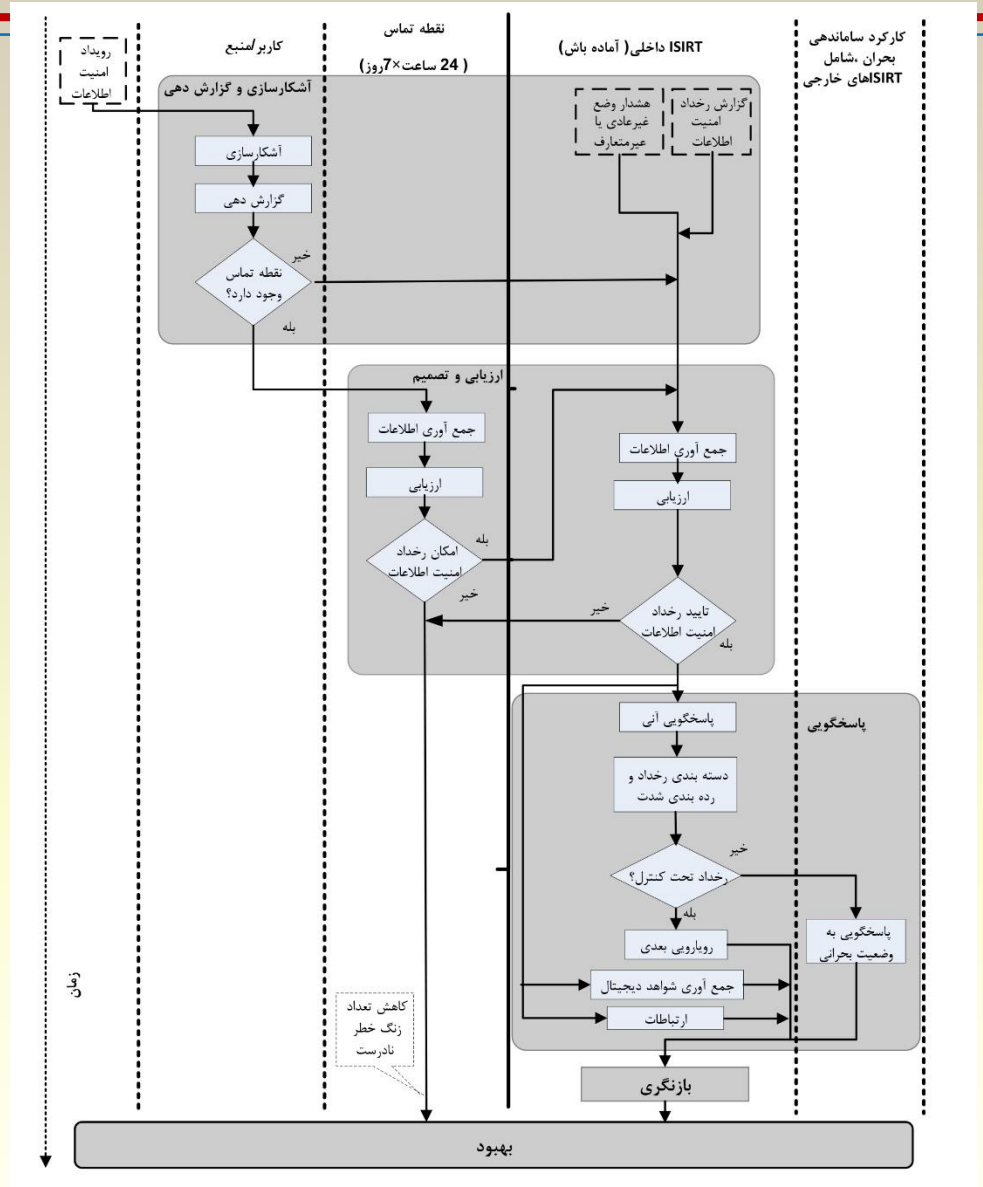


- برنامه‌ریزی و آماده‌سازی
- آشکارسازی و گزارش
- ارزیابی و تصمیم‌گیری
- پاسخ‌گویی
- درس‌های آموخته شده

مراحل مدیریت رخداد امنیت اطلاعات

- برنامه‌ریزی و آماده‌سازی
- آشکارسازی و گزارش
- ارزیابی و تصمیم‌گیری
- پاسخ‌گویی
- درس‌های آموخته شده

نمودار جریان رویداد و رخداد امنیت اطلاعات



COMPUTER EMERGENCY RESPONSE TEAM (CERT)

گروه پاسخ‌گویی به فوریت‌های رایانه‌ای

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.

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

- 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

انواع گروه‌های پاسخگویی به حوادث رایانه‌ای

- **رسمی**
  - گزارش‌دهی
  - بررسی
  - پاسخگویی
- **موردی**
  - گردهم‌آیی در زمان نیاز
  - وظایف غیر رسمی

مدل‌های ساختاری گروه‌های پاسخگویی به حوادث رایانه‌ای

- **تیم امنیت**
  - به شکل رسمی وظیفه پاسخگویی ندارد
  - گروه پاسخگویی به حوادث رایانه‌ای ایجاد نشده است
  - گروه موردی
- **گروه پاسخگویی به حوادث رایانه‌ای داخلی**
- **گروه پاسخگویی به حوادث رایانه‌ای هماهنگ**

اهداف اصلی

- کمینه و کنترل‌کردن خسارت
- فراهم‌آوردن 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 فناوری اطلاعات و ارتباطات

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 و ارتباطات سازمان از قبیل راهبردهای کاهش‌دهنده مخاطرات و اقدام‌های پیش‌گیرانه در مورد رویدادها و رخدادها
- 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

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.

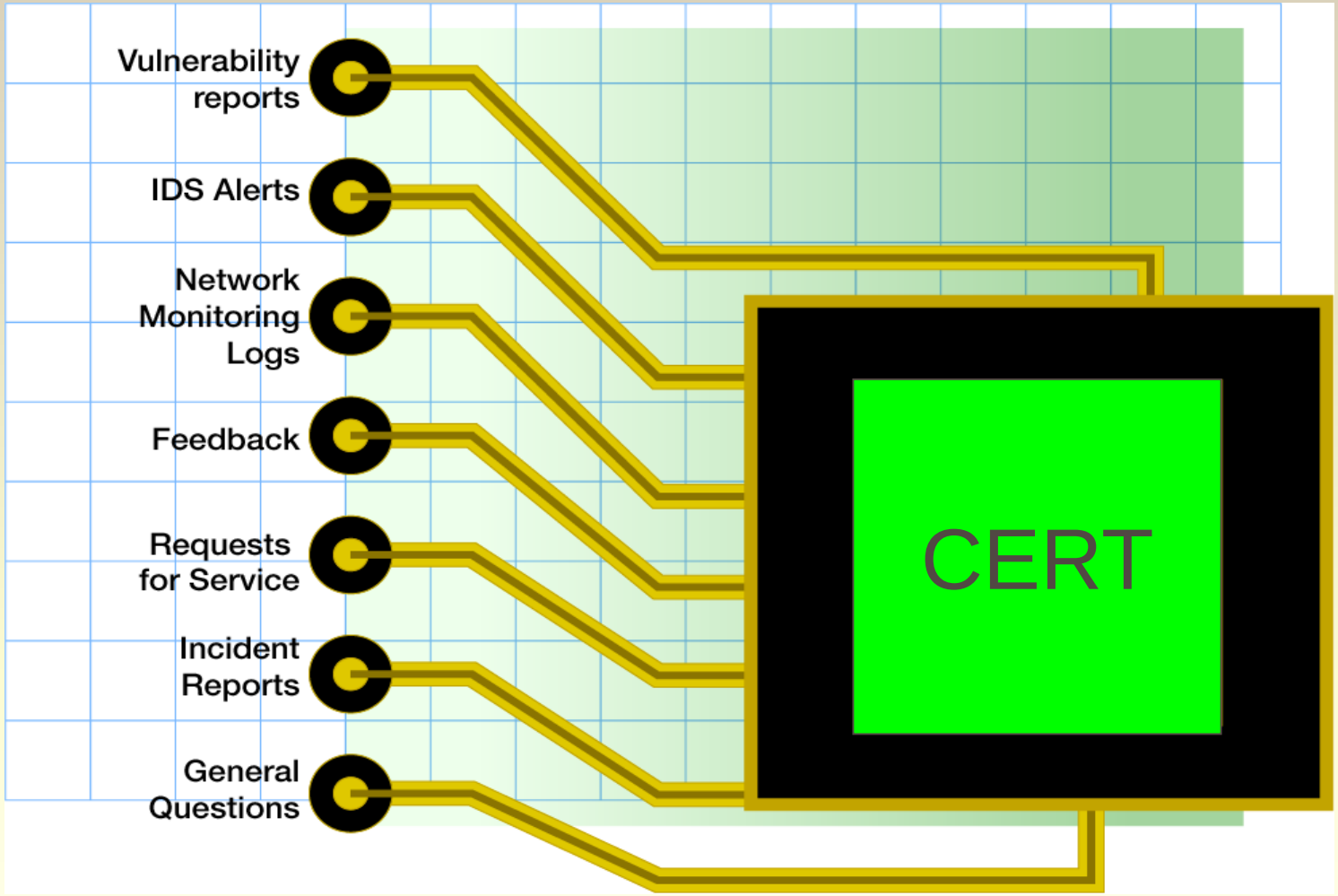
انواع سرویس‌ها

- سرویس‌ها بر اساس نیاز تعریف می‌شوند
- سازمان سرویس‌ها را تعیین می‌کند
- سه سرویس عمومی
  - سرویس‌های پیشگیرانه
  - سرویس‌های واکنشی
  - سرویس‌های مدیریت کیفیت امنیت

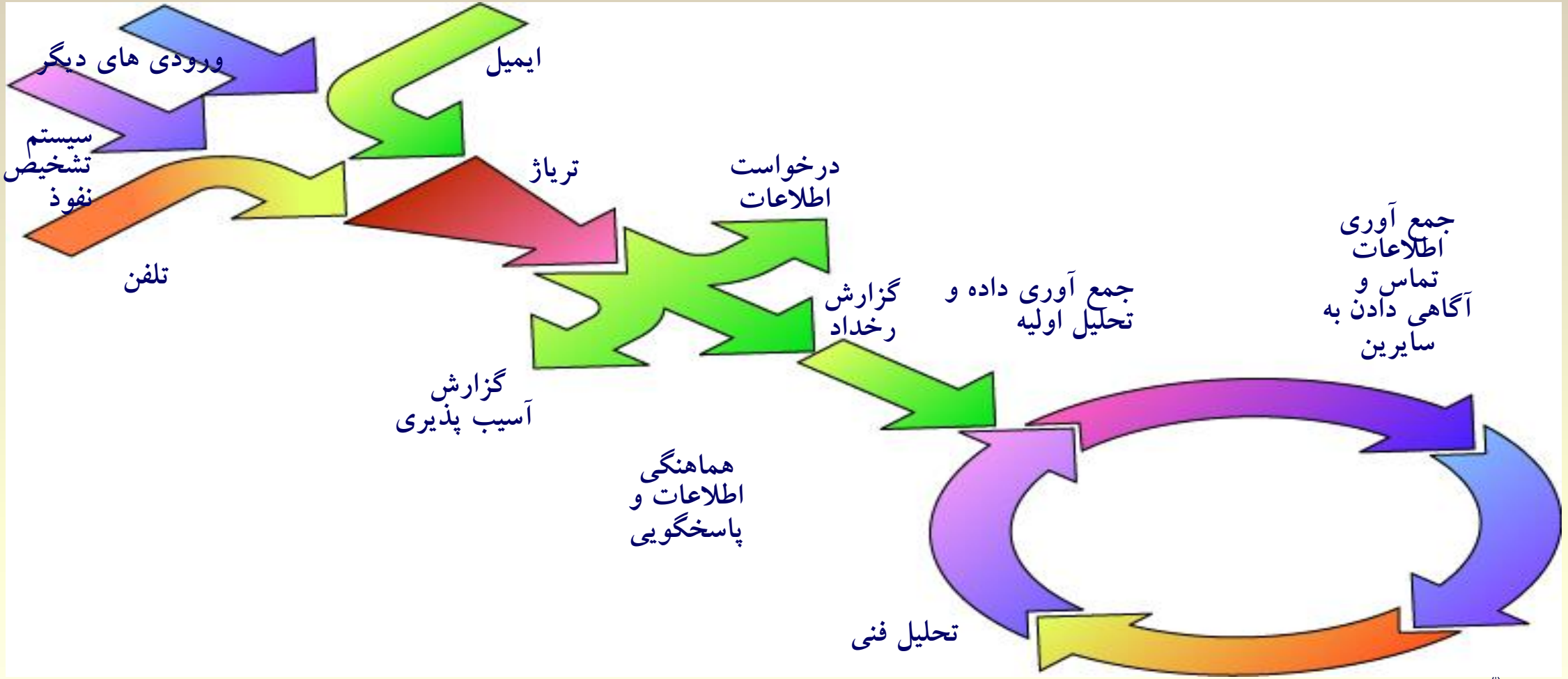
خدمات

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

ورودی‌های CERT



مراحل دریافت گزارش رخداد و پاسخگویی به آن در CERT



سرویس‌های واکنشی

- پاسخ به درخواست گزارش آسیب‌پذیری
- آنالیز رویداد
- بیان علت رویداد
- تصمیم‌گیری و پیاده‌سازی روش‌های ترمیم
- سیاست‌گذاری برای جلوگیری
- جمع‌آوری گزارشات
- بررسی مجموعه گزارش‌ها
- به اشتراک‌گذاری نتایج
- هشدار به سایر تیم‌ها

سرویس‌های واکنشی

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

سرویس‌های واکنشی

- **اخطارها 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 پیشگیرانه

- بهبود قبل از وقوع حادثه
- کاهش اثرات حادثه
- کاهش حادثه در بلند مدت

سرویس‌های پیشگیرانه

- اعلان‌ها
- بررسی و نظارت بر فن‌آوری‌های جدید در سازمان
- بررسی و ارزیابی مداوم امنیت
- تنظیم امنیتی سرویس‌ها
- طراحی و ایجاد ابزارهای امنیتی
- آزمون نفوذپذیری متناوب
- نشر مطالب امنیتی

سرویس‌های مدیریت کیفیت امنیت

- مطالعه مستندات جمع‌آوری شده در حملات قبلی
- تحلیل ریسک‌ها
- دریافت و ارایه مشاوره‌های امنیتی
- آموزش
- ارزیابی و تست محصولات
- ارزیابی گواهی‌نامه‌های دریافت شده

مدیریت حوادث

- **مدیریت کلیه‌ی فعالیت‌های امنیتی سایبری**
  - پیشگیری
  - بررسی ریسک‌ها
  - ترمیم و بازیابی
  - ...
- **مدیریت مداوم و تمام وقت**

مدیریت حوادث

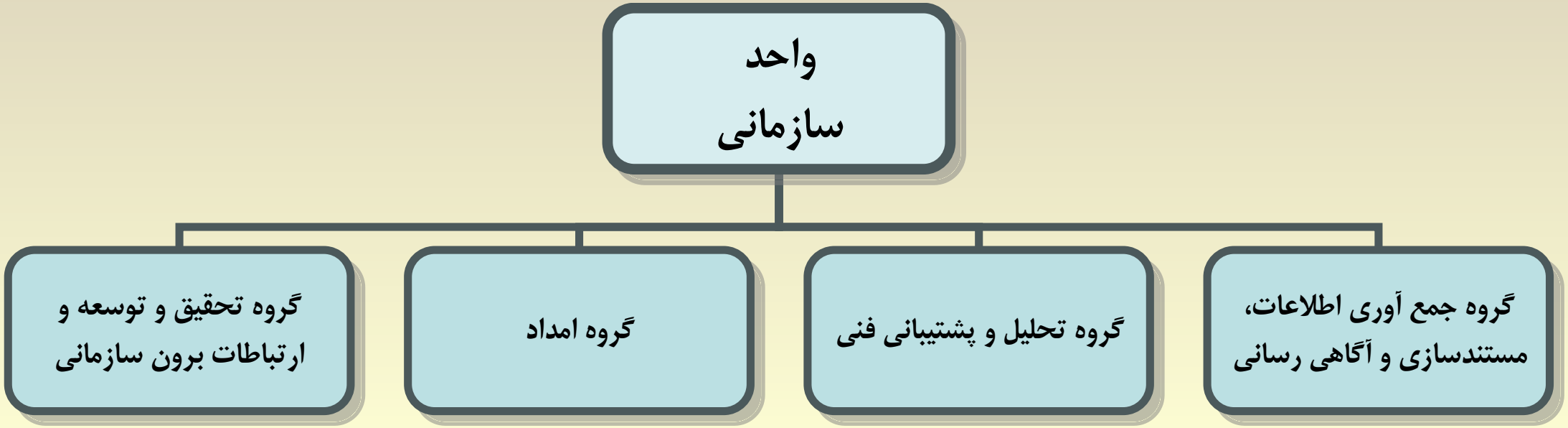
- تشخیص و گزارش‌دهی
- طبقه‌بندی
- تحلیل و بررسی
- پاسخگویی

مدل فرآیند مدیریت حوادث

- ایجاد معماری چند لایه
  - کادر تخصصی
  - مدیران
- آماده سازی بستر تقویت و پیشرفت
- حفاظت از زیرساخت
- تشخیص حادثه
- طبقه بندی حوادث
- پاسخ دهی

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 به‌منظور 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.

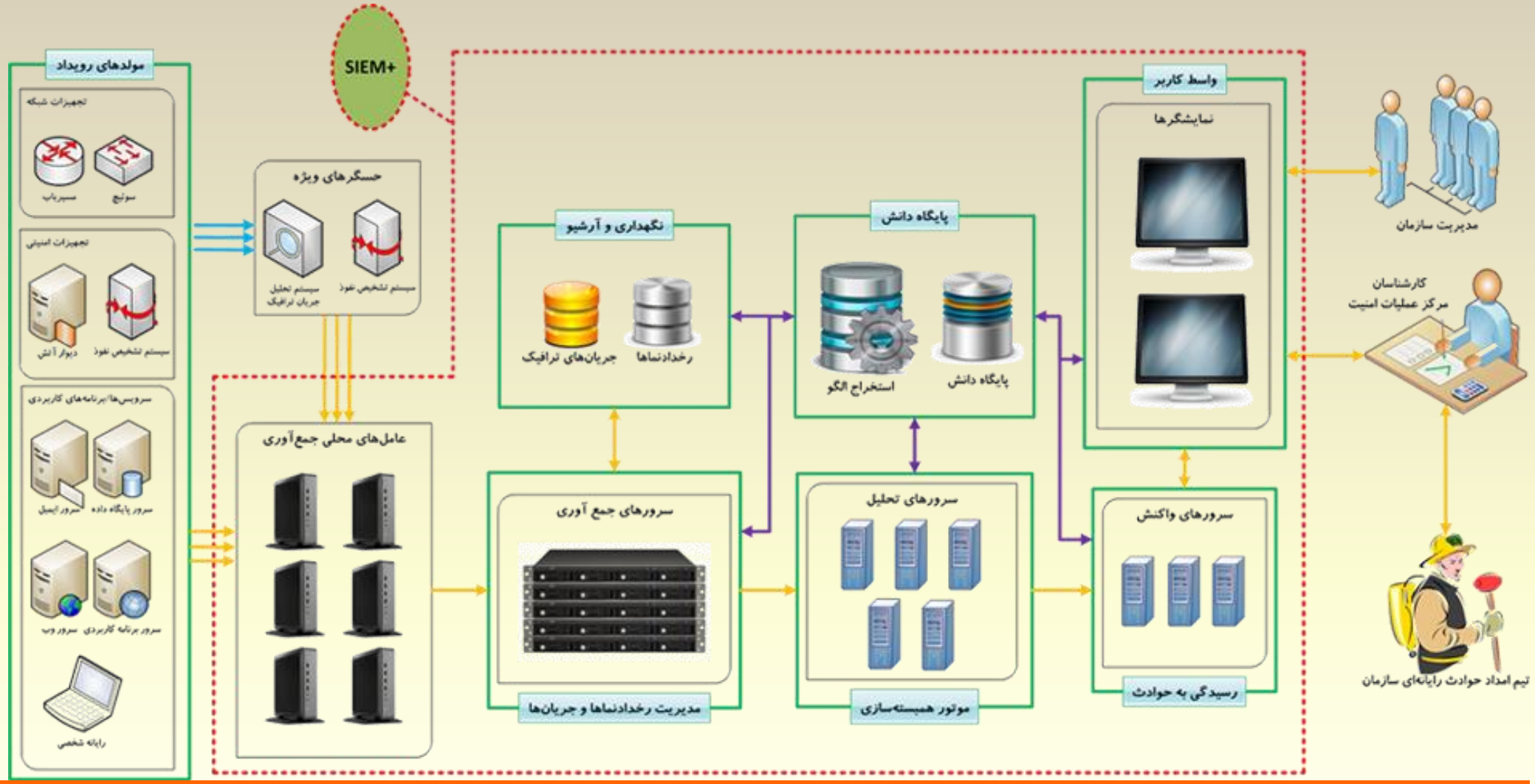
گروه امداد

- 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 ارائه‌شده را برعهده دارد.
- نظارت بر فناوری‌ها و ارائه راهکارهای جدید برای ارائه خدمات و ارتباطات برون سازمانی هم با تامین‌کنندگان و هم با دیگر مراکز مشابه از وظایف این گروه می‌باشد.

مرکز عملیات امنیت



از بذل توجهتان متشکرم

http://cert.um.ac.ir

tayarani@um.ac.ir