**آزمایشگاه آپا**

**آگاهی‌رسانی، پشتیبانی و امداد در**

**حوزه امنیت سیستم‌عامل**

**دانشگاه صنعتی امیرکبیر**

**(با حمایت مرکز تحقیقات مخابرات ایران)**

**گروه مدیریت**

# رویه های مورد نیاز برای ایجاد یک گروه پاسخگویی به حوادث کامپیوتری رسمی

**FC_۸۷_۰۶_۰۱**

**تاریخ: ۸۷/۰۶**

| مشخصات سند | | | |
|---|---|---|---|
| **نام سند:** رویه های مورد نیاز برای ایجاد یک گروه پاسخگویی به حوادث کامپیوتری رسمی | | | |
| **کد فایل** | **آخرین نسخه** | **تاریخ آخرین بازبینی** | **گروه** |
| FC_۸۷_۰۶_۰۱ | ۱،۱ | ۸۷/۰۹/۰۳ | مدیریت |

| سابقه سندها | | | |
|---|---|---|---|
| **نسخه** | **تاریخ تنظیم** | **تنظیم‌کننده** | **توضیحات** |
| ۱،۰ | ۸۷/۰۶/۰۱ | خدیجه محمدزاده | ایجاد |

# چکیده

برای پاسخگویی سریع به حملات، به سیاستها و روشهایی برای گزارش این حملات، تحلیل و پاسخگویی به آنها نیاز داریم. این کارها توسط گروهی که گروه پاسخگویی به حوادث کامپیوتری (CSIRT ) نامیده می شود انجام می‌گردد. در این گزارش سعی بر آن است که یک تعریف کلی از سرویسهای گروه پاسخگویی به حوادث کامپیوتری ارائه شود و رویه‌های گروه پاسخگویی به حوادث به اجمال معرفی گردند.

## فهرست مطالب


**۱ مقدمه ..... ۱**

**۲ انواع گروههای پاسخگویی به حوادث کامپیوتری..... ۱**

**۳ مدلهای ساختاری گروه پاسخگویی به حوادث کامپیوتری ..... ۱**

**۴ سرویسهای گروه پاسخگویی به حوادث کامپیوتری.....۲**

۴-۱ سرویسهای واکنشی..... ۳

*۴-۱-۱ اخطارها و هشدارها.....۳*

*۴-۱-۲ بررسی حوادث .....۴*

*۴-۱-۳ بررسی آسیب پذیریها.....۵*

*۴-۱-۴ بررسی کدهای آسیب‌رسان.....۶*

۴-۲ سرویسهای پیشگیرانه .....۶

*۴-۲-۱ اعلانها.....۷*

*۴-۲-۲ نظارت بر تکنولوژیها .....۷*

*۴-۲-۳ بررسی و ارزیابی امنیت.....۷*

*۴-۲-۴ پیکربندی و نگهداری از ابزارهای امنیتی ،کاربردها،زیرساختارها و سرویسها.....۷*

*۴-۲-۵ ایجاد ابزارهای امنیتی .....۸*

*۴-۲-۶ سرویسهای تشخیص نفوذ .....۸*

*۴-۲-۷ انتشار اطلاعات مربوط به امنیت.....۸*

۴-۳ سرویسهای مدیریت کیفیت امنیت..... ۸

*۴-۳-۱ آنالیز ریسک .....۹*

*۴-۳-۲ مشاوره در زمینه امنیت.....۹*

*۴-۳-۳ آموزش.....۹*

*۴-۳-۴ ارزیابی محصولات یا گواهیها .....۹*

**۵ مدیریت حوادث ..... ۱۰**

**۶ مدل فرآیند در مدیریت حوادث.....۱۱**

**۷ مروری بر رویه های مدیریت حوادث.....۱۲**

**۸ نگاشت فرآیند.....۱۵**

**۹ نمودار جریان کاری مدیریت حوادث.....۱۶**

**۱۰ منابع و مراجع .....۲۰**

## فهرست شکلها

شکل ۱-رابطه بین مدیریت،پاسخگویی و بررسی حوادث ..... ۱۱
شکل ۲-فرآیندهای مدیریت حوادث ..... ۱۳
شکل ۳- مقایسه مدیریت امنیت و مدیریت حوادث..... ۱۵
شکل ۴-نمودار جریان کاری مدیریت حوادث ..... ۱۹

## فهرست جداول

جدول۱-سرویسهای گروه پاسخگویی به حوادث کامپیوتری ..... ۲

## ۱ مقدمه

زمانی که یک سازمان با یک مشکل امنیتی کامپیوتری روبرو می‌شود باید به سرعت و به نحو موثری به این مشکل پاسخ دهد. هرچه سازمان بتواند سریعتر، حملات را تشخیص دهد و با موفقیت آن‌ها را آنالیز کند می‌تواند آسیب‌های ناشی از حمله و هم‌چنین هزینه‌های مربوط به ترمیم[۱] را کاهش دهد. تحلیل موفقیت‌آمیز ماهیت حملات و رویدادها منجر به روش‌های پیشگیرانه شده و از وقوع اتفاقات مشابه جلوگیری می‌شود. توانایی پاسخگویی سریع و موثر به حملات کامپیوتری، یک عنصر اساسی در ایجاد یک محیط امن برای کامپیوترها است.

برای پاسخگویی سریع به حملات به سیاست‌ها و روش‌هایی برای گزارش این حملات، تحلیل و پاسخگویی به آن‌ها نیاز داریم .این کارها توسط گروهی که *"گروه پاسخگویی به حوادث کامپیوتری"*(CSIRT)[۲] نامیده می‌شود انجام می‌گردد. اولین گروه پاسخگویی به حوادث کامپیوتری در سال ۱۹۸۸ بعد از این‌که کرم موریس[۳] ده درصد کامپیوترهایی را که به اینترنت متصل بودند را آلوده کرد در دانشگاه Carnegie Mellon به وجود آمد.

## ۲ انواع گروههای پاسخگویی به حوادث کامپیوتری

یک گروه پاسخگویی به حوادث کامپیوتری می‌تواند رسمی یا موردی[۴] باشد در تیمهای رسمی وظیفه اصلی اعضای تیم در جهت تامین اهداف گروه پاسخگویی به حوادث کامپیوتری است یعنی اعضا فقط به گزارش‌دهی و بررسی و پاسخگویی به حوادث می پردازند ولی در گروه‌های موردی اعضا فقط در زمان نیاز گرد هم می‌آیند و به غیر از وظایف مربوط به گروه پاسخگویی به حوادث کامپیوتری وظایف دیگری نیز بر عهده دارند. با بزرگ شدن سازمان نیاز به تیم رسمی افزایش می‌یابد.

## ۳ مدلهای ساختاری گروه پاسخگویی به حوادث کامپیوتری

- تیم امنیت[۵] : در این مدل هیچ گروه یا بخشی وظیفه پاسخگویی به حملات را به طور رسمی بر عهده ندارد. گروه پاسخگویی به حوادث کامپیوتری تاسیس نشده است و نیروهای موجود (عموما مدیران سیستم، شبکه و امنیت) به صورت یک گروه موردی این کار را به عنوان بخشی از وظایف خود انجام می‌دهند.
- گروه پاسخگویی به حوادث کامپیوتری داخلی: در این روش یک گروه مشخص که تنها به این منظور ایجاد شده است این کار را انجام می‌دهد.

---

[۱] recovery

[۲] Computer Security incident Response Team

[۳] Morris

[۴] adhoc

[۵] Security team

- گروههای پاسخگویی به حوادث کامپیوتری هماهنگ: در این مدل، گروه پاسخگویی به حوادث کامپیوتری با سازمان‌های داخلی و خارجی تبادل اطلاعات می‌کند این سازمان‌ها می‌توانند گروه پاسخگویی به حوادث کامپیوتری دیگر یا متخصصین امنیت و... باشند. cert/cc یا AusCERT نمونه‌هایی از این دست هستند.

# ۴ سرویسهای گروه پاسخگویی به حوادث کامپیوتری

استانداردی از مجموعه کارها و سرویس‌هایی که یک گروه پاسخگویی به حوادث کامپیوتری باید ارائه دهد وجود ندارد و هر تیمی باید سرویس‌های خود را براساس نیازهای سازمان تعیین کند. ولی سرویس‌هایی که عموما توسط گروه پاسخگویی به حوادث کامپیوتری ارائه می‌شود را می‌توان در سه گروه رده‌بندی کرد: سرویس‌های واکنشی، سرویس‌های پیشگیرانه و سرویس‌های مدیریت کیفیت امنیت.

شکل زیر این سرویسها را نشان می دهد.

**جدول ۱-سرویسهای گروه پاسخگویی به حوادث کامپیوتری**

| سرویسهای واکنشی | سرویسهای پیشگیرانه | بررسی کدهای آسیب‌رسان[1] |
|---|---|---|
| • اخطارها و هشدارها<br>• بررسی حوادث<br>- آنالیز حوادث<br>- پاسخگویی به حوادث با حضور در محل<br>- پشتیبانی برای پاسخ به حوادث<br>- هماهنگ کردن پاسخها<br>• بررسی آسیب پذیریها<br>- آنالیز آسیب پذیریها<br>- پاسخ به آسیب پذیریها<br>- هماهنگ کردن پاسخها | • اعلانها<br>• نظارت بر تکنولوژیها<br>• بررسی و ارزیابی امنیت<br>• پیکربندی و نگهداری از ابزارهای امنیتی<br>• ایجاد ابزارهای امنیتی<br>• سرویسهای تشخیص نفوذ<br>• انتشار اطلاعات مربوط به امنیت | • آنالیز کدهای آسیب‌رسان<br>• پاسخ به کدهای آسیب‌رسان<br>• هماهنگ کردن پاسخها |
| | | **مدیریت کیفیت امنیت** |
| | | • آنالیز ریسک<br>• مشاوره در زمینه امنیت<br>• آموزش<br>• ارزیابی محصولات یا گواهیها |

[1] artifact

## ۴-۱ سرویسهای واکنشی

این سرویس‌ها در پاسخ به یک درخواست یا اتفاق مانند گزارش از آسیب‌پذیری یک نرم‌افزار، تشخیص نفوذ در یک سیستم یا تشخیص کدهای مخرب انجام می‌شوند. این فعالیتها هسته اصلی گروه پاسخگویی به حوادث کامپیوتری هستند. این سرویس شامل آنالیز رویداد و بیان علت آن، تصمیم‌گیری و پیاده‌سازی روش‌هایی در جهت ترمیم سیستم و جلوگیری از وقوع مجدد چنین حملاتی است. برقراری ارتباط با بخش‌هایی که از این حمله تاثیر دیده‌اند و یا برای ترمیم سیستم به مشارکت آن‌ها نیاز است از دیگر فعالیتهای این بخش است.

هر سازمانی باید خود، حملات مربوط به سازمان را تعیین کند این حملات می‌تواند شامل موارد زیر باشد:

- تلاش برای دستیابی به یک سیستم یا داده‌های آن
- ممانعت از سرویس[۱]
- استفاده غیرمجاز از سیستم برای پردازش یا ذخیره داده‌ها
- تغییر سخت‌افزار ، نرم‌افزار سیستم
- کدهای مخرب
- از بین رفتن محرمانگی و جامعیت اطلاعات
- سوء استفاده از سیستم‌های اطلاعاتی

گروه پاسخگویی به حوادث کامپیوتری یک نقطه مرکزی برای گزارش مشکلات امنیتی است که سبب می‌شود که همه گزارشات و فعالیتها در یک مکان جمع‌آوری گردد. این اطلاعات سپس مورد بررسی قرار می‌گیرد تا هدف و الگوی فعالیت مخرب شناسایی شده و عکس العمل مناسب نشان داده شود.

گروه پاسخگویی به حوادث کامپیوتری هم‌چنین می‌تواند با بقیه گروه‌های واقع در خارج سازمان همکاری داشته باشد این همکاری منجر به اشتراک استراتژی‌ها در پاسخگویی به حملات مشابه شده و به عنوان یک هشداردهنده برای مشکلات بالقوه است.

از جمله سرویس‌های واکنشی می‌توان به موارد زیر اشاره کرد:

### ۴-۱-۱ اخطارها و هشدارها

این سرویس شامل انتشار اطلاعاتی درباره حملات، آسیب‌پذیریهای امنیتی، نفوذ، ویروس کامپیوتری و اعمال موقت پیشنهادی برای برخورد با نتایج این موارد است. این اطلاعات راهنماهای لازم برای حفاظت از سیستم‌ها و ترمیم سیستم‌های آسیب‌دیده را فراهم می‌کند.

---

[۱] denial of service

### ۴-۱-۲ بررسی حوادث

بررسی حوادث شامل دریافت، طبقه‌بندی، الویت‌دهی و پاسخ به درخواست‌ها و گزارشات حوادث و آنالیز آنها است و می‌تواند شامل موارد زیر باشد:

- تهیه راه حل‌ها و استراتژی‌هایی برای کاهش اثر حوادث
- جست وجوی حوادث در بقیه بخش‌های شبکه
- فیلتر کردن ترافیک شبکه
- بازسازی سیستم‌ها
- ترمیم و وصله‌زنی[۱] سیستم‌ها

بررسی حوادث را می‌توان به مراحل زیر تقسیم کرد:

- آنالیز حوادث: این مرحله شامل بررسی همه اطلاعات در دسترس، مدارک و کدهای آسیب‌رسان مربوط به حادثه است. هدف از آنالیز، تعیین هدف و ماهیت حادثه، خسارات ناشی از آن و استراتژی‌های در دسترس برای پاسخگویی به حادثه است. گروه پاسخگویی به حوادث کامپیوتری ممکن است از نتایج آنالیز آسیب‌پذیری ها و کدهای آسیب‌رسان برای آنالیز حوادث استفاده کند. دو زیررویه‌ای که بنا بر ماموریت‌ها و اهداف گروه پاسخگویی به حوادث کامپیوتری ممکن است در این بخش انجام شوند در زیر آمده است.

  - جمع‌آوری مدارک قانونی: این بخش شامل جمع‌آوری، نگهداری، مستندسازی و آنالیز مدارک جمع‌آوری شده از سیستم‌های آسیب‌دیده برای تعیین تغییرات اعمال شده به سیستم و نمونه‌سازی حوادثی که منجر به آسیب‌رسانی به سیستم شده‌اند است. کارهایی که در این بخش می‌توان انجام داد عبارتند از: تهیه یک کپی از دیسک سیستم‌های آسیب‌دیده، چک کردن سیستم برای یافتن تغییرات آن از جمله تغییر در برنامه‌ها، فایل‌ها و سرویس‌ها، توجه به رویه‌های در حال اجرا و پورت‌های باز و جست‌وجو برای یافتن برنامه‌های اسبهای تروجان.
  - پیگیری یا ردیابی: این بخش شامل ردیابی منشا حمله یا تعیین سیستم‌هایی که حمله به آن‌ها دسترسی پیدا کرده است می‌باشد. از جمله کارهایی که در این بخش می‌توان انجام داد: تعیین چگونگی وارد شدن حمله‌کننده به سیستم‌های آسیب‌دیده، تعیین سیستم‌هایی که از آن‌ها برای به‌دست‌آوردن دسترسی استفاده شده است، تعیین مبدا حمله و سیستم‌ها و شبکه‌هایی که به عنوان بخشی از حمله مورد استفاده قرار گرفته‌اند و هم‌چنین ممکن است شامل شناسایی حمله‌کننده نیز باشد این کار عموما با همراهی *"فراهم کنندگان سرویس اینترنت"*[۲] و سازمان‌های درگیر و نهادهای قانونی انجام می شود.

- پاسخگویی با حضور در محل: گروه پاسخگویی به حوادث کامپیوتری فقط به پاسخ از طریق پست الکترونیک یا تلفن بسنده نمی‌کند و با حضور در محل سایت‌های آسیب‌دیده، سیستم‌ها را آنالیز کرده و آن‌ها را تعمیر و

---

[۱] patching

[۲] ISP

ترمیم می‌نماید. این بخش شامل همه سرویس‌هایی است که در صورت بروز یک حادثه و یا در صورت تردید به وقوع حادثه باید با حضور در محل انجام شود.

- پشتیبانی برای پاسخ به حوادث: گروه پاسخگویی به حوادث کامپیوتری سازمان‌های آسیب‌دیده را برای ترمیم سیستم‌ها از طریق تلفن، پست الکترونیک، فاکس و مستندات، راهنمایی و کمک می‌کند. این سرویس می‌تواند شامل کمکهای فنی در تفسیر داده‌های جمع‌آوری شده و راهنماهای مربوطه برای کاهش اثر حوادث و ترمیم سیستم باشد. در این سرویس گروه پاسخگویی به حوادث کامپیوتری راهنماهایی را از راه دور فراهم می‌کند و نیروهای موجود، خود می‌توانند با استفاده از این راهنماها ترمیم را انجام داده و اثر حادثه را تا حد ممکن کاهش دهند.

- هماهنگی پاسخ به حوادث: گروه پاسخگویی به حوادث کامپیوتری پاسخهای مختلفی که بخشهای درگیر در یک حادثه می‌دهند را هماهنگ می‌کند. این بخشها عموما شامل قربانیان حملات، سایت‌هایی که درگیر حمله شده‌اند و هر سایت دیگری که برای آنالیز حمله به کمک نیاز دارد است. هم‌چنین ممکن است شامل بخشهایی که برای سازمان آسیب‌دیده سرویس‌های فناوری اطلاعات[1] فراهم می‌کنند مانند فراهم کنندگان سرویس اینترنت‌ها، گروههای پاسخگویی به حوادث کامپیوتری دیگر و سرپرستان سیستم و شبکه نیز باشد. از جمله کارهایی که در این بخش می‌توان انجام داد جمع‌آوری اطلاعات تماس، آگاه‌سازی سایت‌ها از درگیری آن‌ها در حملات (به عنوان قربانی یا مبدا یک حمله)، جمع‌آوری آمار درباره تعداد سایت‌های درگیر و تسهیل مبادله اطلاعات و آنالیز آن‌ها است. بخشی از هماهنگی‌ها شامل آگاه‌سازی و همکاری با نهادهای قانونی و منابع انسانی است. این سرویس شامل حضور در محل سایت آسیب‌دیده نمی شود.

### ۴-۱-۳ بررسی آسیب پذیریها

بررسی آسیب‌پذیریها شامل دریافت اطلاعات و گزارشات درباره آسیب‌پذیریهای سخت‌افزار و نرم افزار، آنالیز ماهیت و تاثیرات آن‌ها و ایجاد استراتژیهایی برای پاسخگویی، کشف و ترمیم آسیب‌پذیریها است. بررسی آسیب‌پذیری را می‌توان به مراحل زیر تقسیم کرد:

- آنالیز آسیب‌پذیریها: گروه پاسخگویی به حوادث کامپیوتری آسیب‌پذیریهای سخت‌افزار و نرم‌افزار را آنالیز و بررسی می‌نماید. این بخش شامل اطمینان از آسیب‌پذیریهای مورد تردید و بررسی فنی آسیب‌پذیریهای سخت‌افزار و نرم‌افزار برای تعیین مکان آسیب‌پذیریها و نحوه بهره‌برداری از آن‌ها می‌باشد. آنالیز ممکن است شامل مرور کد مبدا با استفاده از یک دیباگر برای تعیین مکان آسیب‌پذیری یا تلاش برای تولید مجدد مشکل روی یک سیستم تست باشد.

- پاسخ به آسیب‌پذیریها: این سرویس شامل ایجاد پاسخ‌های مناسب برای کاهش اثر یا تعمیر آسیب‌پذیریها است. ایجاد یا جست‌وجوی وصله‌ها و آگاه‌سازی دیگران از این استراتژیها از طریق انتشار توصیه نامه‌ها و اخطارها از دیگر فعالیتهای این بخش است. این سرویس هم‌چنین می‌تواند شامل پیاده سازی پاسخها از طریق نصب وصله‌ها نیز باشد.

---

[1] Information technology (IT)

- هماهنگی پاسخها: گروه پاسخگویی به حوادث کامپیوتری بخش‌های مختلف را از آسیب‌پذیری آگاه کرده و اطلاعات لازم برای حل یا کاهش اثر آسیب‌پذیری را با آن‌ها به اشتراک می‌گذارد و از پیاده‌سازی موفقیت‌آمیز استراتژی پاسخ به آسیب‌پذیری اطمینان حاصل می‌کند. این سرویس می‌تواند شامل برقراری ارتباط با فروشندگان، گروههای پاسخگویی به حوادث کامپیوتری دیگر، متخصصین فنی، افراد و گروههایی که این آسیب‌پذیری را کشف و گزارش کرده اند؛ هماهنگی در مستندات و وصله‌ها و تلفیق آنالیزهای فنی که توسط بخشهای مختلف انجام شده است باشد.

### ۴-۱-۴ بررسی کدهای آسیب‌رسان

در این سرویس، کپی کدهای آسیب‌رسان مورد استفاده قرار گرفته در حملات دریافت می‌شوند و مورد بررسی و شناسایی قرار می‌گیرند. این بررسی شامل آنالیز ماهیت، مکانیک، نسخه، نحوه عملکرد کدهای آسیب‌رسان و ایجاد (پیشنهاد) استراتژیهایی برای کشف، رفع و دفاع علیه این کدهای آسیب‌رسان است. بررسی کدهای آسیب‌رسان را می‌توان به مراحل زیر تقسیم کرد:

- آنالیز کدهای آسیب‌رسان: گروه پاسخگویی به حوادث کامپیوتری یک آنالیز و بازرسی فنی روی کدهای آسیب‌رسانی که در سیستم یافت می‌شود انجام می‌دهد این آنالیز شامل تعیین نوع فایل و ساختار کدهای آسیب‌رسان، مقایسه کدهای آسیب‌رسان جدید با کدهای آسیب‌رسان موجود و نسخه های پیشین برای تعیین شباهتها و تفاوتها یا مهندسی معکوس، مجزا کردن[۱] کد برای تعیین هدف و نحوه عملکرد کدهای آسیب‌رسان است.
- پاسخ به کدهای آسیب‌رسان: این سرویس شامل تعیین فعالیتهای مناسب برای کشف و رفع کدهای آسیب‌رسان از سیستم و هم‌چنین فعالیتهایی برای پیشگیری از نصب کدهای آسیب‌رسان است. هم‌چنین شامل ایجاد امضای کدهای آسیب‌رسان برای استفاده در نرم افزارهای آنتی ویروس یا سیستم تشخیص نفوذ است.

هماهنگی پاسخها: این سرویس شامل اشتراک و تلفیق نتایج آنالیز و استراتژیهای پاسخگویی مربوط به یک حادثه با پژوهشگران، گروههای پاسخگویی به حوادث کامپیوتری، فروشندگان و دیگر متخصصین امنیت است. این فعالیت شامل آگاه‌سازی دیگران و تلفیق آنالیزهای فنی منابع گوناگون است هم‌چنین می‌تواند شامل ایجاد و نگهداری یک بایگانی از کدهای آسیب‌رسان شناخته شده و تاثیرات آن‌ها و استراتژیهای پاسخگویی مربوطه باشد.

## ۴-۲ سرویسهای پیشگیرانه

این سرویس‌ها برای بهبود امنیت زیرساختار پیش از وقوع یا کشف حوادث طراحی شده‌اند و هدف اصلی آن‌ها پیشگیری از حوادث و کاهش اثر و محدوده اثرگذاری آن‌ها در زمانی که به وقوع می پیوندند است. کارآیی این سرویس‌ها در کاهش حملات در آینده تاثیر مستقیم دارد.

---

[۱] Disassemble

### ۴-۲-۱ اعلانها

این بخش شامل اخطار درباره نفوذها و آسیب‌پذیریها و توصیه های امنیتی است. این اعلان‌ها افراد را قادر می‌سازد تا سیستم‌های خود را علیه مشکلات جدید محافظت کنند.

### ۴-۲-۲نظارت بر تکنولوژیها

گروه پاسخگویی به حوادث کامپیوتری پیشرفتهای فنی جدید، فعالیتهای حمله کنندگان و گرایش آن‌ها را برای تعیین تهدیدات آینده بررسی می‌کند. این سرویس شامل مطالعه و بررسی وب‌سایت‌های امنیت، اخبار و مقالات موجود در زمینه امنیت و تکنولوژیهای مربوطه است. خروجی این سرویس می‌تواند به شکل آگهی‌ها، راهنماها و توصیه‌هایی در زمینه امنیت باشد.

### ۴-۲-۳بررسی و ارزیابی امنیت

این سرویس بر اساس نیازمندیهای سازمان و استانداردهای موجود یک آنالیز وارزیابی کامل روی زیرساختار انجام می‌دهد. زیرساختار را از راههای مختلفی می‌توان مورد ارزیابی قرار داد که از جمله آن‌ها می‌توان به موارد زیر اشاره کرد:

- بررسی زیرساختار: بررسی سخت‌افزار و پیکربندی نرم افزار، مسیریاب‌ها، دیوارهای آتش و سرورها برای اطمینان از تطابق آن‌ها با استانداردها و سیاستهای امنیتی سازمان از فعالیتهای این بخش است.
- پویش کردن: استفاده از پویشگرهای ویروس یا آسیب‌پذیری برای تعیین سیستم‌های آسیب پذیر از فعالیتهای این بخش است.
- تست نفوذ: تست امنیت سایت با استفاده از حملاتی که عمدا برای تعیین آسیب‌پذیری زیرساختار توسط گروه پاسخگویی به حوادث کامپیوتری انجام می‌شود از فعالیتهای این بخش است. انجام این کار به موافقت مدیران رده بالا نیاز دارد و باید مطابق با سیاستهای سازمان انجام شود.

### ۴-۲-۴پیکربندی و نگهداری از ابزارهای امنیتی ،کاربردها،زیرساختارها و سرویسها

این سرویس راهنماهای مناسب برای پیکربندی و نگهداری ابزار، برنامه‌های کاربردی و زیرساختارهایی که توسط گروه پاسخگویی به حوادث کامپیوتری یا مشتریان آن مورد استفاده قرار می گیرد ارائه می‌دهد. علاوه بر تهیه این راهنماها، گروه پاسخگویی به حوادث کامپیوتری پیکربندیهای ابزار و سرویس‌های امنیتی را به‌هنگام می‌کند و به نگهدار ی از آن‌ها می پردازد. از جمله ابزار و سرویس‌های امنیتی می‌توان به سیستم تشخیص نفوذ، سیستم‌های نظارت و پویش شبکه، فیلترها، دیوارهای آتش، شبکه خصوصی مجازی[۱] و مکانیزمهای تصدیق اشاره کرد.

---

[۱] Virtual Private Network (VPN)

### ۴-۲-۵ایجاد ابزارهای امنیتی

این سرویس شامل ایجاد ابزار جدید و خاص مورد نیاز گروه پاسخگویی به حوادث کامپیوتری یا مشتریان آن، است به عنوان مثال می‌توان به ایجاد وصله‌های امنیتی برای نرم افزارهای سفارشی یا نرم افزارهای ایمن شده برای بازسازی سیستم‌های آسیب‌دیده، اشاره کرد .از دیگر فعالیتهای این بخش ایجاد ابزار برای توسعه عملکرد ابزار امنیتی موجود مانند مکانیزمهای اتوماتیک توزیع وصله است.

### ۴-۲-۶سرویسهای تشخیص نفوذ

گروه پاسخگویی به حوادث کامپیوتری که این سرویس را انجام می‌دهدرویدادهای مربوط به سیستم تشخیص نفوذ را بررسی و آنالیز کرده و برای حوادثی که به آستانه تعریف شده رسیده‌اند پاسخ راآغاز می‌کند یا طبق استراتژیهای تعریف شده به بخش مناسب، اخطاری را ارسال می‌کند. تشخیص نفوذ و آنالیز رویدادهای امنیتی کار ساده‌ای نیست تعیین مکان‌های مناسب برای سنسورها در محیط و جمع‌آوری و آنالیز داده‌های زیادی که وجود دارد کار پیچیده‌ای است. بسیاری از سازمان‌ها از ابزار پیچیده و متخصصین برای ترکیب و تعبیر داده‌های جمع‌آوری شده استفاده می‌کنند. برخی سازمان‌ها این کار را به نهادهای دیگر که متخصصین بیشتری دارند مانند *"شرکت ثالث فراهم کننده سرویس امنیت"*[۱] واگذار می‌کنند.

### ۴-۲-۷انتشار اطلاعات مربوط به امنیت

از جمله اطلاعاتی که توسط این سرویس انتشار می‌یابد می‌توان به موارد زیر اشاره کرد:

- راهنماهای گزارش دهی و تماس با گروه پاسخگویی به حوادث کامپیوتری
- آرشیوهایی از اخطارها، هشدارها و اعلان‌های دیگر
- مستنداتی در ارتباط با استانداردهای موجود
- راهنماهایی در ارتباط با امنیت کامپیوتر
- سیاستها، رویه‌ها و چک‌لیستها
- ایجاد وصله‌ها
- آمار موجود در ارتباط با حوادث و گرایش آن‌ها

## ۴-۳ سرویسهای مدیریت کیفیت امنیت

این سرویس‌ها برای بالا بردن امنیت سازمان با استفاده از مطالبی که در طی بررسی و پاسخگویی به حوادث و آسیب‌پذیریها و حملات به دست آمده است طراحی شده‌اند.

---

[۱] Managed security service provider (MSSP)

### ۴-۳-۱ آنالیز ریسک

این سرویس تعیین حملات بالقوه و ارزیابی استراتژیهای حفاظتی و پاسخگویی را ممکن می‌سازد.

### ۴-۳-۲مشاوره در زمینه امنیت

گروه پاسخگویی به حوادث کامپیوتری راهنماها و توصیه‌هایی را برای خرید، ایمن سازی و نصب سیستم‌های جدید، اجزاء شبکه و نرم‌افزارهای مختلف ارائه می‌کند.

### ۴-۳-۳ آموزش

این سرویس شامل فراهم نمودن اطلاعاتی در زمینه امنیت کامپیوتر برای کاربران از طریق سمینار، دوره‌های آموزشی، کارگاهها و.. است. اطلاعات می‌تواند شامل راهنماهایی برای گزارش دادن حوادث، متدهای مناسب پاسخگویی، ابزار پاسخ به حوادث، متدهای پیشگیری از حوادث و اطلاعات ضروری دیگر برای حفاظت، کشف، گزارش و پاسخ به حوادث مربوط به امنیت کامپیوتر باشد.

### ۴-۳-۴ ارزیابی محصولات یا گواهیها

در این سرویس، گروه پاسخگویی به حوادث کامپیوتری ابزار، برنامه‌های کاربردی یا سرویس‌های دیگر را برای اطمینان از امنیت آن‌ها و تطابق با سیاستهای امنیتی سازمان مورد ارزیابی قرار می‌دهد.

لازم به ذکر است که همه گروه پاسخگویی به حوادث کامپیوتری ها ملزم به ارائه همه این سرویس‌ها نیستند. ممکن است این سرویس‌ها در بخشهای مختلف یک سازمان پراکنده شده باشند. گاهی اوقات این سرویس‌ها بین گروه پاسخگویی به حوادث کامپیوتری و بخشهای اجرایی دیگر تقسیم شده است این وضعیت به خصوص در گروه پاسخگویی به حوادث کامپیوتری داخلی مانند نهادهای آموزشی، دولتی، نظامی و تجاری اتفاق می‌افتد. ولی در گروههای پاسخگویی به حوادث کامپیوتری هماهنگ این کارها بین بخشهای تجاری مختلف توزیع نمی شود.

با توجه به ساختار سازمان کارهای مختلفی توسط گروه پاسخگویی به حوادث کامپیوتری انجام می‌شود و در برخی موارد همین کارها توسط گروه فناوری اطلاعات[۱]، یا گروه مدیریت امنیت یا برخی بخشهای دیگر سازمان انجام می شود.

---

[۱] Information Technology (IT)

# ۵ مدیریت حوادث [۱]

در گذشته برای تعریف کارهایی که توسط گروه پاسخگویی به حوادث کامپیوتری انجام می شد عبارات پاسخگویی به حوادث[۲] و بررسی حوادث[۳] را به کار می بردند ولی این عبارات کارهایی که توسط گروه پاسخگویی به حوادث کامپیوتری انجام می‌شود را بسیار محدود می‌کنند. برای بیان طیف وسیعی از سرویس‌هایی که توسط گروه پاسخگویی به حوادث کامپیوتری انجام می‌شود از عبارت مدیریت حوادث استفاده می کنیم .

بررسی حوادث شامل کارهای زیر است:

- تشخیص[۴] و گزارش دهی: توانایی دریافت و مرور اطلاعات و گزارشات حوادث و اخطارها.
- طبقه‌بندی[۵] : طبقه بندی کردن و تعیین الویت حوادث.
- آنالیز: تلاش برای یافتن اینکه چه اتفاقی افتاده است ، تاثیرات و تهدیدها و زیان‌های ناشی از آن و مشخص کردن اعمالی که باید برای ترمیم انجام شود.
- پاسخگویی به حوادث: شامل کارهایی است که برای رفع و کاهش اثر یک حادثه انجام می‌شود. جمع‌آوری و انتشار اطلاعات و مشخص کردن استراتژیهایی برای جلوگیری از وقوع مجدد حادثه از جمله این کارها است.

پاسخگویی به حوادث شامل استراتژیهایی برای ترمیم و کاهش اثر حادثه است و شامل رویه‌های تصمیم گیری ، هماهنگی و اجرا است.

واژه مدیریت حوادث کارهایی که توسط گروه پاسخگویی به حوادث کامپیوتری انجام می‌شود را گسترش داده و آن را شامل سرویس‌هایی نظیر بررسی آسیب‌پذیریها، بررسی کدهای آسیب‌رسان و آموزشهای لازم در زمینه آگاهی از امنیت می‌کند .

مدیریت حوادث فقط در زمانی که حادثه‌ای به وقوع پیوست به آن پاسخ نمی‌دهد بلکه با اقدامات پیشگیرانه و با فراهم کردن راهنماهایی علیه ریسکهای بالقوه و تهدیدات، سعی در پیشگیری از حوادث دارد. برای مثال کاربران نهایی را از اهمیت امنیت کامپیوتر و شرایط غیر نرمال یا رفتارهای مخرب آگاه می‌کند در این صورت کاربران با مشاهده شرایط غیر عادی می‌توانند گروه پاسخگویی به حوادث کامپیوتری را در جریان قرار دهند.

شکل زیر رابطه بین مدیریت حوادث، پاسخگویی به حوادث و بررسی حوادث را نشان می‌دهد.

---

[۱] Incident management

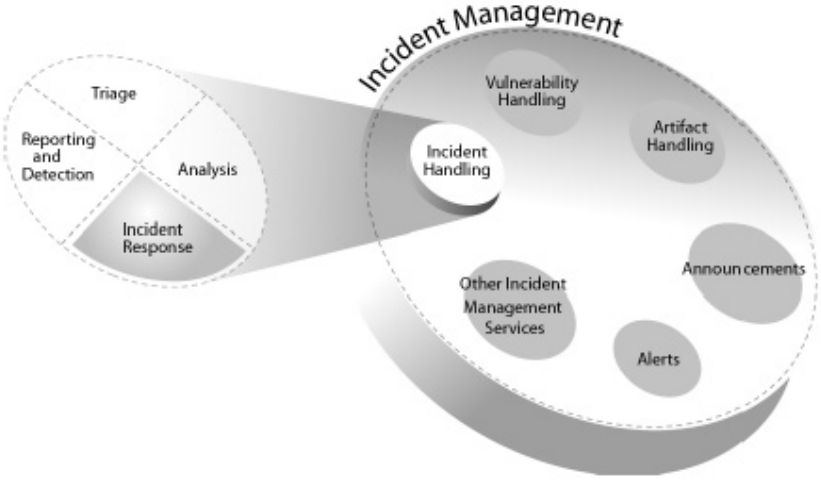
[۲] Incident response

[۳] Incident handling

[۴] detect

[۵] Triage

**شکل ۱–رابطه بین مدیریت،پاسخگویی و بررسی حوادث**




## ۶ مدل فرآیند در مدیریت حوادث

یک سازمان برای تامین امنیت خود به یک معماری چند لایه نیاز دارد.در این معماری چند لایه علاوه بر نیروهای فنی، همه اعضای سازمان باید در جهت تامین امنیت بکوشند .

مدیریت حوادث، مجموعه ای از رویه‌های سازگار با هم، با کیفیت بالا و قابل تکرار و اندازه‌گیری است.

گروه پاسخگویی به حوادث کامپیوتری بخشی از استراتژی کلی سازمان در جهت تامین امنیت و حفاظت از سازمان است و شامل رویه‌هایی برای ایجاد:

- ارتباط و اخطار
- آنالیز و پاسخگویی
- همکاری و هماهنگی
- نگهداری و پیگیری اطلاعات بایگانی شده

می‌باشد.

بدین منظور رویه‌های زیر در گروه پاسخگویی به حوادث کامپیوتری انجام می شود:

- ایجادآمادگی/تقویت /پیشرفت (آمادگی)
- حفاظت از زیرساختار (حفاظت)

- تشخیص حوادث (تشخیص)
- ظبقه بندی کردن حوادث
- پاسخ دهی

لازم به ذکر است که همه این کارها در همه گروههای پاسخگویی به حوادث کامپیوتری انجام نمی شود. انجام برخی از این کارها در برخی از انواع گروههای پاسخگویی به حوادث کامپیوتری مناسب نیست.

## ۷ مروری بر رویه های مدیریت حوادث

سازمان‌ها نه تنها باید رویه‌هایی برای پاسخگویی به حوادث داشته باشند بلکه باید شامل رویه‌هایی برای جلوگیری از وقوع حوادث و تکرار مجدد آن‌ها باشند. رویه‌های زیر این اهداف را تامین می‌کنند:

- طراحی و پیاده سازی یک رویه برای مدیریت حوادث
- ایمن‌سازی زیر ساختار برای جلوگیری از وقوع حوادث یا برای کاهش اثر آن‌ها
- کشف ، طبقه‌بندی و پاسخگویی به حملات در زمانی که به وقوع می پیوندند.

این رویه‌های ابتدایی ، رویه‌های سطح بالای گروه پاسخگویی به حوادث کامپیوتری را تشکیل می‌دهند .

در سطوح پایین تر می‌توان این رویه‌ها را به صورت زیر بیان کرد.

- ایجادآمادگی /تقویت /پیشرفت که شامل زیر رویه‌های زیر است:
  - طراحی و پیاده سازی یک مدیریت حوادث ابتدایی
  - تقویت این توانایی
  - بهبود بخشیدن به این توانایی از طریق ارزیابی مداوم سیستم و مطالبی که به مرور فراگرفته می‌شود.
  - مرور رویه‌های مدیریت حوادث در زمان نیاز.

- حفاظت از زیرساختار (حفاظت) که شامل زیر رویه‌های زیر است:
  - اعمال تغییراتی در زیرساختار برای متوقف ساختن یا کاهش اثر آسیب‌پذیری موجود در ساختار سخت افزاری یا نرم افزاری
  - پیاده سازی پیشرفتهای ساختاری که نتیجه *"بازبینی های پس از رفع حادثه"* [۱] است.
  - سنجش زیرساختار با انجام اعمالی نظیر پویش یا نظارت بر شبکه.
- تشخیص حوادث (تشخیص) که شامل زیر رویه‌های زیر است:
  - آگاهی از حوادث و گزارش دادن آن‌ها
  - دریافت گزارشات حوادث
  - نظارت بر شاخص‌هایی نظیر سیستم تشخیص نفوذ
  - آنالیز شاخص‌ها پس از جمع‌آوری آن‌ها (برای مشخص کردن فعالیتهایی که ممکن است در سیستم خرابی به وجود آورند و یا تهدیدات و ریسکهایی را متوجه ساختار کنند.)

---

[۱] Postmortem review

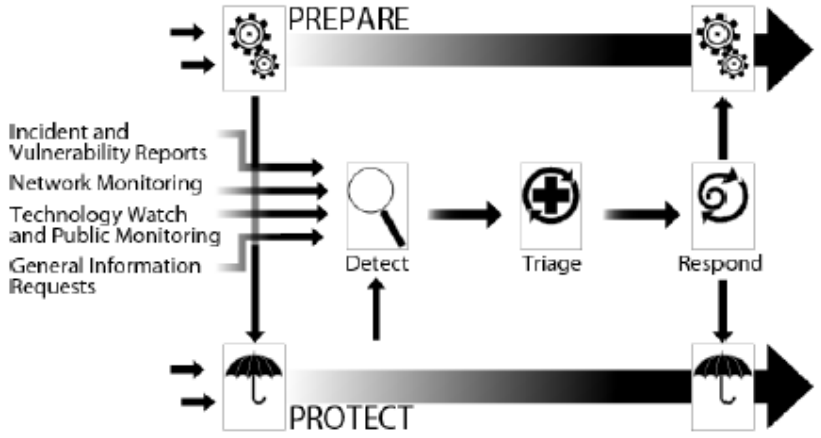
- اطلاعات مربوط به حوادث قابل توجه و مشکوک به رویه طبقه‌بندی ارسال می‌شود.
- بستن همه حوادثی که به بخش طبقه‌بندی ارسال نشده‌اند.

- طبقه‌بندی که شامل زیر رویه‌های زیر است:
  - طبقه بندی و مرتبط کردن حوادث
  - الویت‌دهی به بررسی حوادث
  - مشخص کردن حوادثی که باید به رویه پاسخگویی ارسال شوند.
  - ارسال اطلاعات مربوطه به بخش پاسخگویی
  - بستن همه حوادثی که به بخش پاسخگویی ارسال نشده‌اند و یا به بخشهای دیگر واگذار شده‌اند.

- پاسخگویی که شامل زیر رویه‌های زیر است:
  - آنالیز حوادث
  - طراحی یک استراتژی برای پاسخگویی
  - تهیه پاسخهای فنی ، مدیریتی و حقوقی که شامل اعمالی در جهت ترمیم سیستم و تعمیر آن و کاهش اثر حادثه است.
  - برقرای ارتباط با بخشهای خارجی
  - بستن پاسخها
  - ارسال درسها و اطلاعات وقایع به تابع مناسب برای استفاده در بازبینی پس از حادثه

شکل زیر رابطه بین این رویه‌ها را نشان می‌دهد:

**شکل ۲-فرآیندهای مدیریت حوادث**



شکل۳، رویه‌های آمادگی و حفاظت را به صورت رویه‌هایی مداوم نشان می‌دهد. این رویه‌ها شامل تدارک کارکنان لازم و تکنولوژیهای مورد نیاز، ایجاد یک زیرساختار و تهیه رویه‌هایی برای فعالیتهای مدیریت حوادث است. این دو رویه انجام رویه‌های دیگر، یعنی تشخیص، طبقه‌بندی و پاسخگویی را حمایت کرده و آن‌ها را ممکن می سازند.

فلش های کوچکی که به دو رویه آمادگی و حفاظت وارد می‌شوند نشان دهنده نیازهای این دو بخش، سیاستها و قوانینی که بر ساختار و کارکرد این رویه‌ها حکومت می‌کنند و توصیه‌هایی که برای بهبود و پیشرفت عملکرد رویه‌ها پیشنهاد می‌شوند است.

خطی که از رویه آمادگی به رویه حفاظت کشیده شده است نشان دهنده ارتباطی است که بین این دو رویه وجود دارد. اطلاعاتی که از بازبینی پس از حادثه توسط رویه آمادگی به دست آمده است به رویه حفاظت ارسال می‌شود تا تغییراتی در ساختار ایجاد گردد اگر این تغییرات اعمال شود از وقوع حوادث مشابه و یا وقوع مجدد این حادثه جلوگیری می شود.

رویه‌های تشخیص، طبقه‌بندی و پاسخگویی در شکل به صورت یک دنباله نشان داده شده‌اند . اطلاعاتی که به رویه تشخیص وارد می‌شوند مورد بررسی قرار می گیرند، اگر اطلاعات به آنالیز بیشتر نیاز داشته باشند به رویه طبقه‌بندی ارسال می‌شوند. در رویه طبقه‌بندی اگر اطلاعات دریافت شده (که می‌تواند به صورت یک گزارش حادثه یا آسیب‌پذیری یا یک حادثه مشکوک باشد) به پاسخگویی نیاز داشته باشد به رویه پاسخگویی ارسال می شود.

خطی که از رویه حفاظت به رویه تشخیص رسم شده نشان دهنده گزارشهای آسیب‌پذیری یا حوادثی است که ممکن است از بازبینی زیرساختار به دست آمده باشند. امکان دارد در طی ارزیابی زیرساختار، یک آسیب‌پذیری، یک حادثه مداوم و اثر یا باقیمانده حوادث قبلی کشف شود این اطلاعات باید به رویه تشخیص ارسال شوند.

رابطه ای که بین رویه‌های پاسخگویی و آمادگی وجود دارد نشان دهنده اطلاعاتی است که از این بخش به رویه آمادگی برای استفاده در بازبینی پس از حادثه ارسال می‌شود و می‌تواند باعث بهبود رویه‌ها شود.

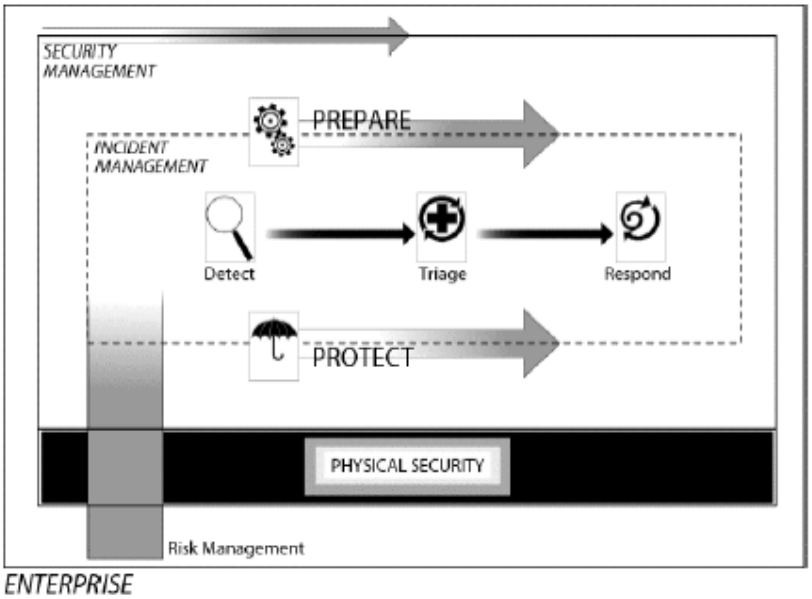
مدیریت حوادث بخشی از مدیریت امنیت است. در برخی موارد از ما خواسته می‌شود تا بین مدیریت حوادث و مدیریت امنیت تفاوت قائل شویم به خصوص در زمانی که مدیریت حوادث شامل رویه‌هایی برای حافظت از زیر ساختار و تشخیص حوادث با استفاده از نظارت بر شبکه و سیستم تشخیص نفوذ است. بین مدیریت امنیت و مدیریت حوادث به طور مشخص مرزی وجود ندارد و ممکن است در برخی موارد مرز بین این دو گمراه کننده باشد. مرزی که بین این دو بخش وجود دارد بستگی به ساختار امنیت سازمان و توانایی های مدیریت حوادث دارد. مدیریت امنیت شامل همه وظایف و کارهایی است که برای تامین امنیت و حفاظت از بخشهای مهم یک سازمان انجام آن‌ها ضروری است و این از کارهایی است که توسط مدیریت حوادث انجام می‌شود گسترده‌تر است. مدیریت امنیت شامل تعیین و الویت‌دهی فعالیتهای امنیتی سازمان بر پایه ماموریتها و اهداف سازمان و تعیین ریسکهای امنیتی است. مدیریت امنیت علاوه بر سازماندهی، پیکر بندی و نگهداری ساختار کامپیوترها به شیوه ای مطمئن شامل مدیریت ریسک، بازرسی، کنترل دسترسی، مدیریت حساب[۱] کاربران، امنیت فیزیکی، سیاستهای امنیتی، مدیریت پیکربندی، مدیریت تغییرات و وصله‌ها و ترمیم سیستم پس از حوادث امنیتی است . مدیریت حوادث ممکن است از بسیاری از این توانایی‌ها مانند مدیریت وصله، مدیریت پیکر بندی یا سیاستهای امنیتی در جهت رسیدن به اهداف خود استفاده کند ولی در قبال سازماندهی و نگهداری این توانایی‌ها مسئولیتی بر عهده ندارد. مدیریت حوادث بخشی از مدیریت امنیت است . مدیریت امنیت یک چهارچوب ایجاد می‌کند که مدیریت حوادث می‌تواند در داخل آن فعالیتهای خود را به انجام برساند.

برخی از فعالیتهایی که توسط مدیریت حوادث انجام می‌شود با فعالیتهای مدیریت امنیت همپوشانی دارد.

---

[۱] account

**شکل۳- مقایسه مدیریت امنیت و مدیریت حوادث**




همانطور که در شکل مشاهده می‌شود رویه‌های آمادگی و محافظت در مدیریت امنیت و در مدیریت حوادث انجام می‌شود. رویه محافظت در مدیریت حوادث، شامل ایجاد تغییرات در زیرساختار در پاسخ به یک تهدید امنیتی که در حال حاضر در سازمان وجود دارد است در حالی که مدیریت امنیت شامل طیف وسیعی از فعالیتهای حفاظتی (شامل فعالیتهای لازم برای پیکربندی و ایمن‌سازی زیر ساختار و نگهداری و نظارت بر پیکربندیها) می‌باشد. رویه‌های تشخیص، طبقه‌بندی و پاسخگویی فقط در مدیریت حوادث انجام می شود.

## ۸ نگاشت فرآیند[۱]

نگاشت فرآیند یک تکنیک معمول برای نشان دادن فعالیتهایی است که برای رسیدن به ماموریتها و اهداف سازمان باید انجام شوند. بسیاری از این تکنیکها نه تنها فعالیتها را مشخص می‌کنند بلکه رابطه بین آنها، وابستگی‌ها و ترتیب انجام آن‌ها را نیز نشان می‌دهند. هم‌چنین ویژگیهای مختلف از جمله ورودی ، خروجی ، انجام دهنده کار و جزئیات مشابه دیگر را نشان می‌دهند.

[۱] Process mapping

نگاشت مدیریت حوادث ، یک سازمان را قادر می‌سازد که بفهمد که چه فعالیتهایی در سازمان انجام می‌شوند و وابستگی آنها چگونه است.

## ۹ نمودار جریان کاری[۱] مدیریت حوادث

این مرحله بالاترین سطح در نگاشت رویه ای است و پنج رویه عمده ای که پیش از این توضیح داده شد را در بر می گیرد.

رویه آمادگی شامل کارهای لازم برای پاسخ سریع به هر ریسک ، تهدید یا حمله ای است. این به معنی آن است که افراد کافی، سیاستها و تجهیزات مورد نیاز در دسترس باشند و هم‌چنین ساختاری برای تعیین وظایف وجود داشته باشد. رویه آمادگی هم‌چنین شامل زیر رویه‌هایی برای ارزیابی مدیریت حوادث و مرور پس از حادثه نیز می‌باشد. هر نتیجه ای که از بازبینی پس از حادثه و یا ارزیابی زیرساختار به دست آمده باشد و منجر به پیشرفت در ساختار گروه پاسخگویی به حوادث کامپیوتری گردد به رویه‌های برنامه‌ریزی و طراحی ارسال می شود. نتایجی که منجر به ایجاد تغییرات در زیرساختار شود از بخش آمادگی به بخش محافظت ارسال می گردد این تغییرات، به منظور ایجاد استحکام و امنیت و جلوگیری از وقوع حوادث، به زیرساختار اعمال می‌شود.

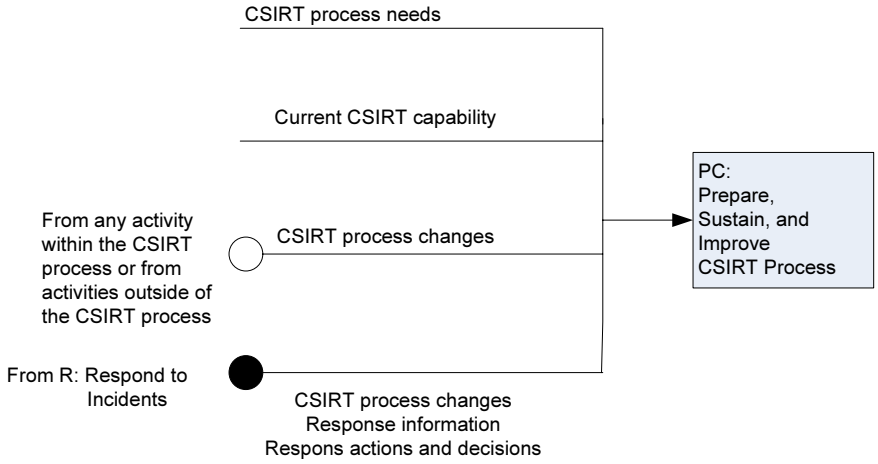
رویه محافظت، در پاسخ به حملات و یا برای جلوگیری از وقوع حملات در زیرساختار کامپیوتری تغییراتی ایجاد می‌کند. این تغییرات، نتایج آنالیز حملات، کدهای آسیب‌رسان و آسیب‌پذیری‌ها است. رویه محافظت شامل زیر رویه‌هایی برای ارزیابی زیرساختار برای تشخیص آسیب‌پذیریها نیز می‌باشد. در چنین ارزیابی هایی آسیب‌پذیریهای بالقوه ، فعالیتهای مخرب مداوم و در حال پیشرفت یا باقیمانده اثر حملات قبلی ممکن است کشف شوند. در چنین مواردی گزارشات آسیب‌پذیری به رویه تشخیص ارسال می‌شوند .

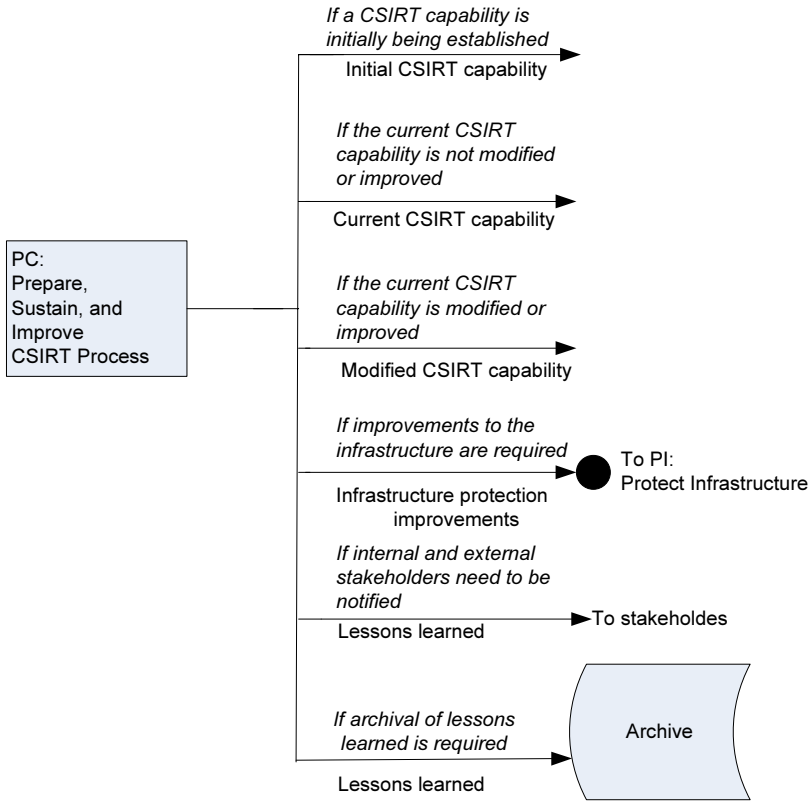
رویه تشخیص، زمانی که فعالیتهای مشکوک مشاهده شود فعال می‌شود. حوادثی که به آنالیز بیشتری نیاز دارند به رویه طبقه‌بندی ارسال می‌شوند و در آنجا برای افزایش بازدهی و هرچه موثرتر بودن پاسخها طبقه‌بندی و الویت‌دهی می‌شوند. آسیب‌پذیریها و هر اتفاق قابل توجهی برای پاسخگویی مناسب به رویه پاسخگویی ارسال می‌شوند.

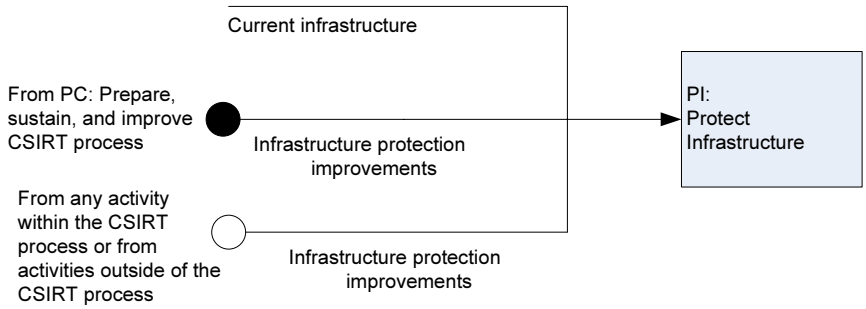
در برخی موارد ممکن است یک گزارش یا حادثه در محدوده فعالیتهای مدیریت حوادث نباشد در این صورت اطلاعات به واحدهای سازمانی دیگر ارسال می‌شوند و یا بسته می‌شوند چون برای آن‌ها نمی‌توان کاری در این حوزه انجام داد . این اتفاق ممکن است در رویه‌های تشخیص، طبقه‌بندی یا پاسخگویی به وجود آید.

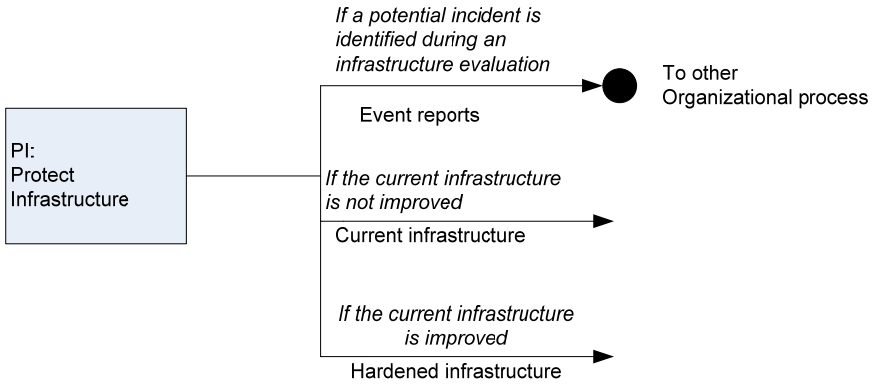
---

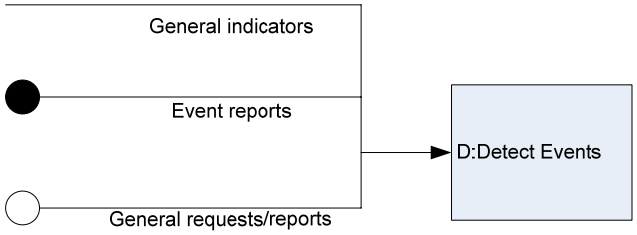
[۱] Work flow

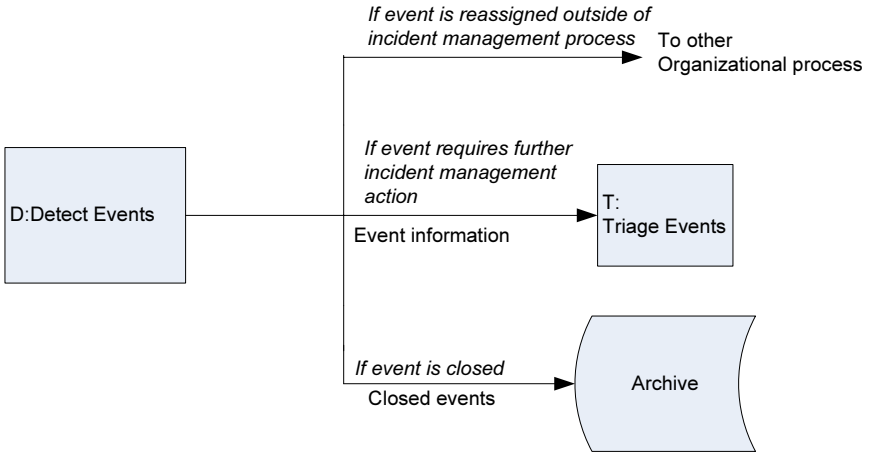

CSIRT process needs
Current CSIRT capability
From any activity within the CSIRT process or from activities outside of the CSIRT process
CSIRT process changes
PC: Prepare, Sustain, and Improve CSIRT Process
From R: Respond to Incidents
CSIRT process changes
Response information
Respons actions and decisions

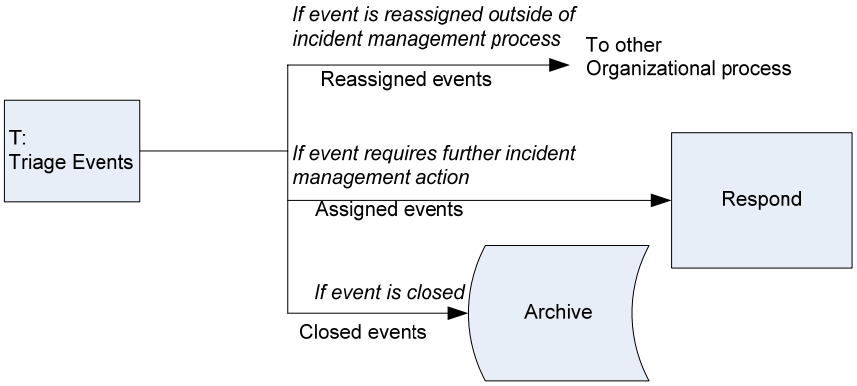

If a CSIRT capability is initially being established
Initial CSIRT capability
If the current CSIRT capability is not modified or improved
Current CSIRT capability
PC: Prepare, Sustain, and Improve CSIRT Process
If the current CSIRT capability is modified or improved
Modified CSIRT capability
If improvements to the infrastructure are required
To PI: Protect Infrastructure
Infrastructure protection improvements
If internal and external stakeholders need to be notified
To stakeholdes
Lessons learned
If archival of lessons learned is required
Archive
Lessons learned

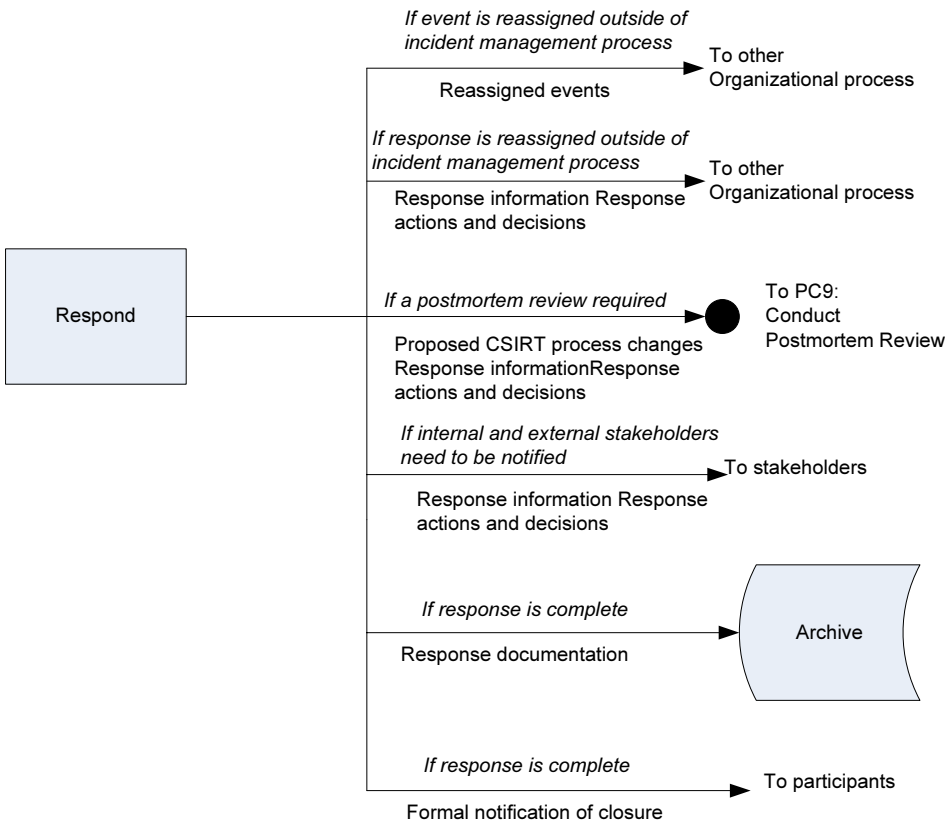

Current infrastructure
From PC: Prepare, sustain, and improve CSIRT process
Infrastructure protection improvements
PI: Protect Infrastructure
From any activity within the CSIRT process or from activities outside of the CSIRT process
Infrastructure protection improvements


If a potential incident is identified during an infrastructure evaluation
To other Organizational process
Event reports
PI: Protect Infrastructure
If the current infrastructure is not improved
Current infrastructure
If the current infrastructure is improved
Hardened infrastructure


General indicators
Event reports
D:Detect Events
General requests/reports


If event is reassigned outside of incident management process
To other Organizational process
If event requires further incident management action
D:Detect Events
T: Triage Events
Event information
If event is closed
Closed events
Archive


If event is reassigned outside of incident management process
To other Organizational process
Reassigned events
T: Triage Events
If event requires further incident management action
Assigned events
Respond
If event is closed
Archive
Closed events




**شکل ۳-نمودار جریان کاری مدیریت حوادث**

که هر یک از این مراحل نمودار جریان کاری مربوط به خود را دارد که در ادامه خواهد آمد.

## ۱۰ منابع و مراجع


۱. *A STEP-BY-STEP APPROACH ON HOW TO SET UP A CSIRT*. ۲۰۰۶, European Network and information Security Agency (ENISA). Available at www.enisa.europa.eu/cert_guide/downloads/CSIRT_setting_up_guide_ENISA.pdf

۲. Albert,C , Dorofee,A ,Killcrece, G, Ruefle, R,Zajicek, M. *Defining incident Management Processes for CSIRTS:A Work in Progress*. Available at www.cert.org/archive/pdf/۰۴tr۰۱۵.pdf

۳. Grance, T,Karent, k,Kim, B., *Computer Security incident Handling Guide*.

۴. Killcrece, G.,Kossakowski ,K., Ruefle ,R.,Zajicek ,M., *State of the Practice of Computer incident Response Teams (CSIRTs).* p. ۲۹۱.Available at www.cert.org/archive/pdf/۰۳tr۰۰۱.pdf

۵. Stikvoort, D,Kossakowski, K,Killcrece, G,Ruefle, R,Zajicek, M. *Handbook for Computer Security incident Response Teams(CSIRTs)*.Available at www.cert.org/archive/pdf/csirt-handbook.pdf