مدیریت حوادث

فهرست

مقدمه: مفاهیم اولیه ی رسیدگی به حادثه

- تاریخچه
  - انتشار کرم اینترنتی موریس در سال ۱۹۸۸

- حادثه(Incident)
  - آسیب/نفوذ و یا تلاش برای آسیب رسانی/ نفوذ به سیستم اطلاعاتی یا شبکه با هدف مختل شدن

    یک یا چند مؤلفه ی امنیتی یا سیاست‌های سیستم و شبکه

- انواع حوادث

- رخداد(Event)
  - هر اتفاق قابل مشاهده در سیستم یا شبکه

مقدمه: مفاهیم اولیه ی رسیدگی به حادثه

- مفهوم رسیدگی به حادثه(Incident Handling)
  - روالی جهت نحوه ی پاسخگویی شخص یا سازمان به یک حادثه

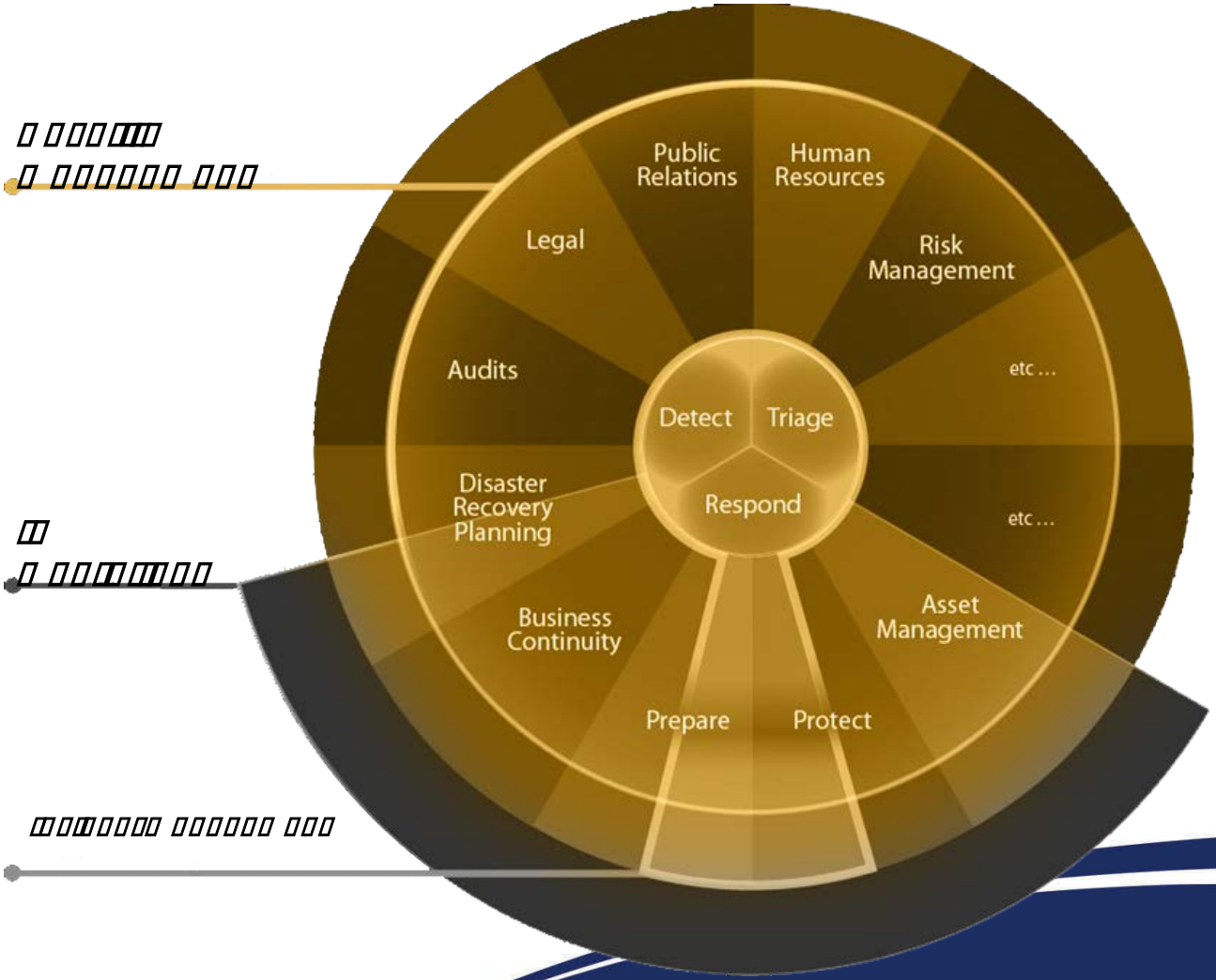
- اهمیت رسیدگی به حادثه
  - هدف اصلی: کاهش خسارت وارده
  - آمادگی پاسخگویی در شرایط بروز یک حادثه ی اساسی
  - مطابقت با سیاست های پاسخگویی و قوانین اجرایی سازمان

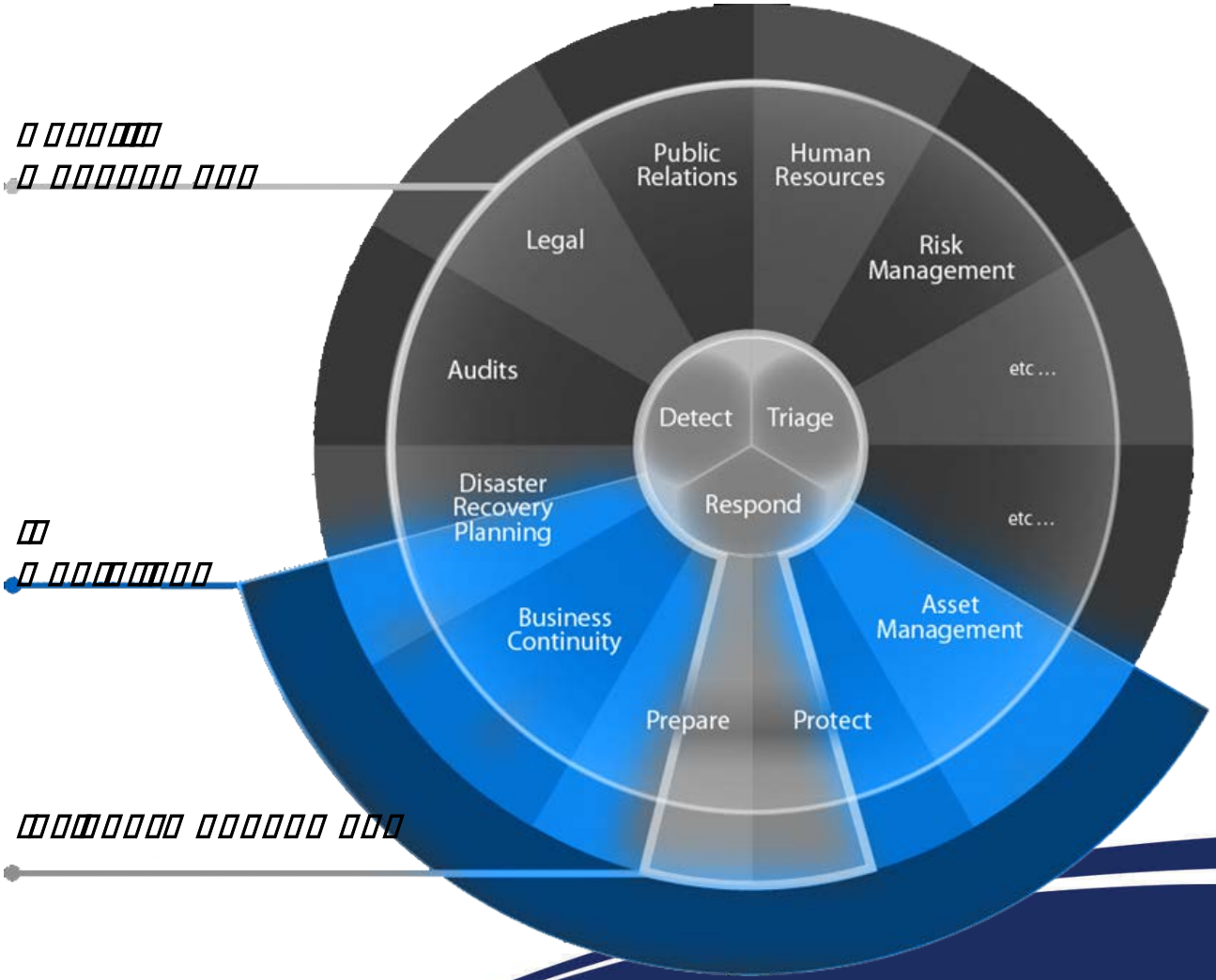
- جایگاه رسیدگی به حادثه در فرایند مدیریت حوادث

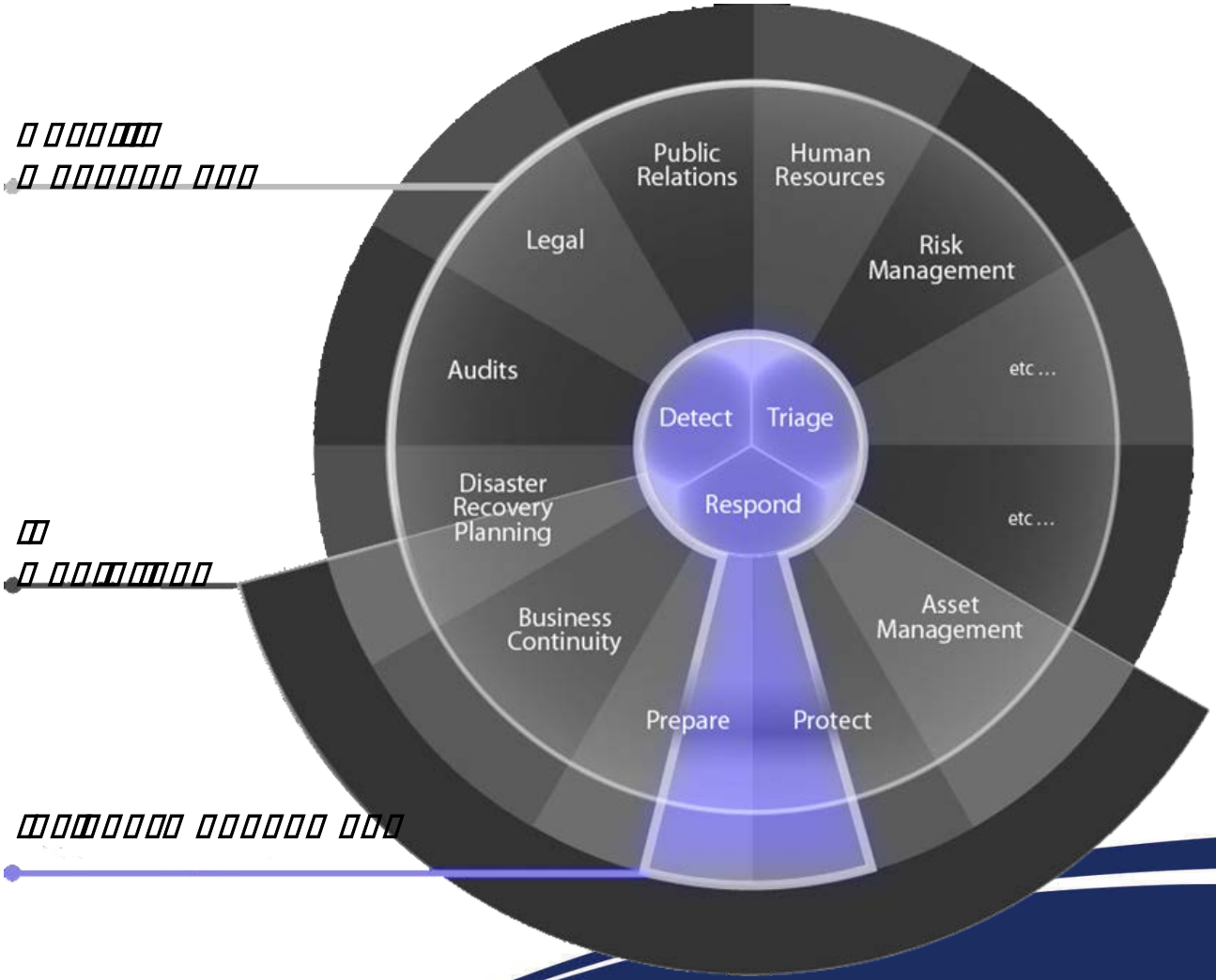
مدیریت حادثه یا رسیدگی به حادثه؟

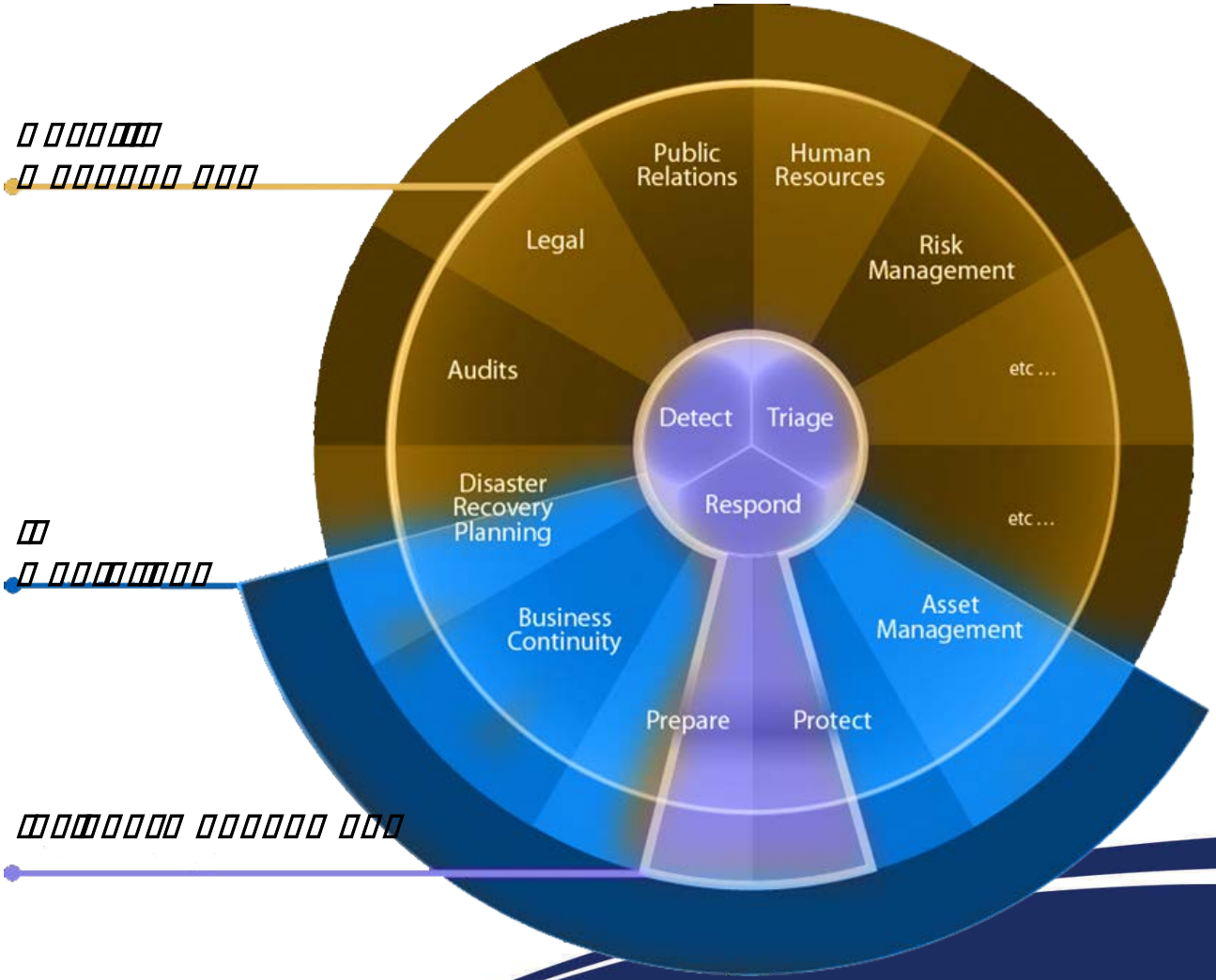
- اقدامات پایه (اقدامات پیشگیری)

  - نصب وصله‌ها
  - بروز سازی مرتب
  - اطمینان از امنیت هر یک از میزبان های شبکه
  - استفاده از نرم افزار های تشخیص نفوذ
  - اطمینان ار تأمین امنیت کلی شبکه
  - نصب نرم افزار های جلوگیری از انتشار بد افزار ها


Public Relations
Human Resources
Legal
Risk Management
Audits
etc ...
Detect
Triage
Disaster Recovery Planning
Respond
etc ...
Business Continuity
Asset Management
Prepare
Protect

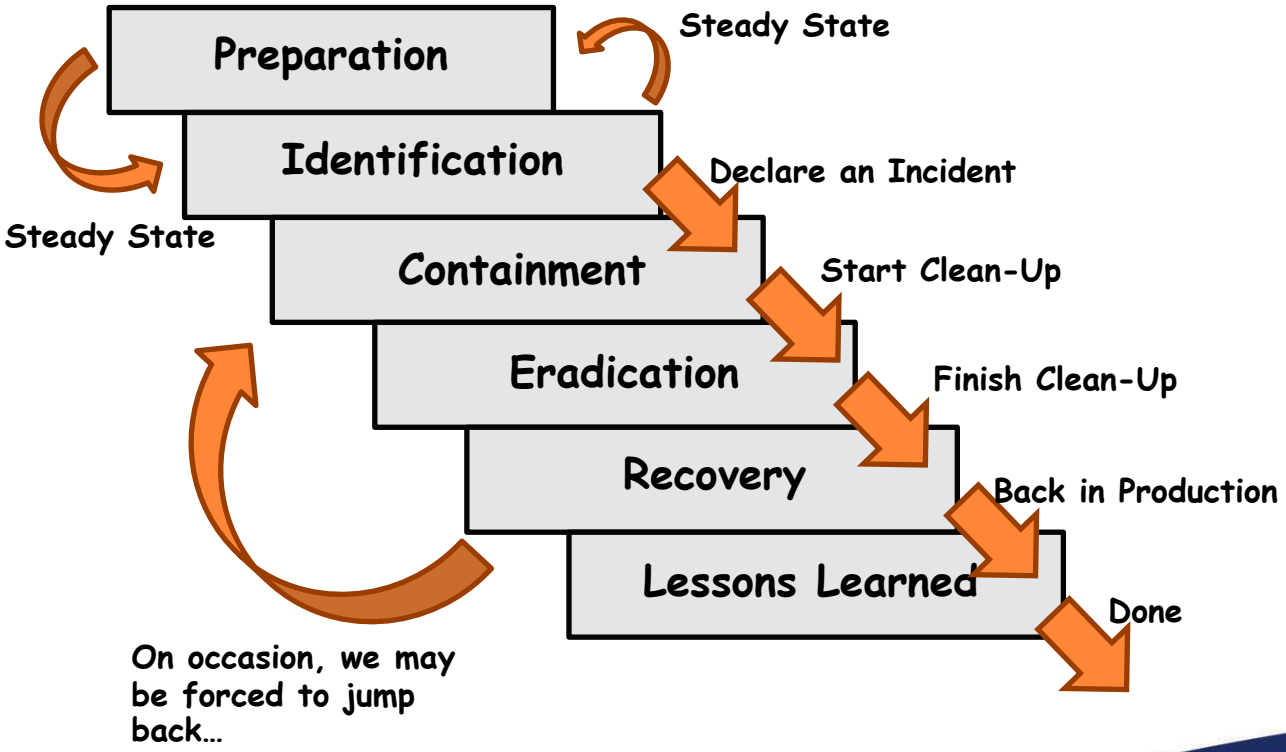

Public Relations
Human Resources
Legal
Risk Management
Audits
etc ...
Detect
Triage
Disaster Recovery Planning
Respond
etc ...
Business Continuity
Asset Management
Prepare
Protect


Public Relations
Human Resources
Legal
Risk Management
Audits
etc ...
Detect
Triage
Respond
Disaster Recovery Planning
etc ...
Business Continuity
Asset Management
Prepare
Protect


Public Relations
Human Resources
Legal
Risk Management
Audits
etc ...
Detect
Triage
Disaster Recovery Planning
Respond
etc ...
Business Continuity
Asset Management
Prepare
Protect

مراحل فرایند رسیدگی به حادثه SANS

- شش مرحله ی اصلی روال رسیدگی به حادثه
  - آمادگی
  - تشخیص
  - محدودسازی
  - ریشه کنی
  - ترمیم
  - فعالیت های پس از حادثه



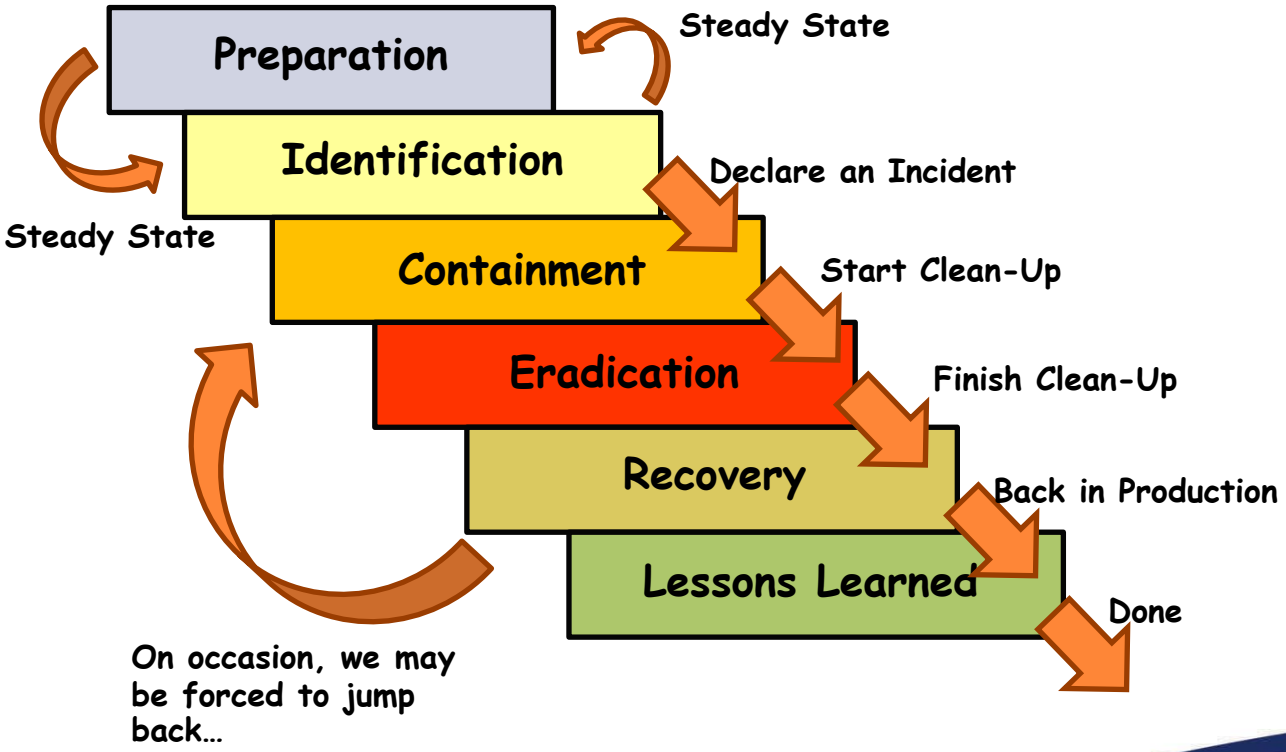
گام‌های رسیدگی به حادثه

- دسته بندی
- اولیت بندی
- تعیین حساسیت
- تعیین تاثیر تکنیکی
- تعیین بیشینه زمان رفع حادثه

- تعیین راهبرد مناسب
- محدود سازی
- درمان

مراحل فرایند رسیدگی به حادثه

- شش مرحله ی اصلی روال رسیدگی به حادثه
  - آمادگی
  - تشخیص
  - محدودسازی
  - ریشه کنی
  - ترمیم
  - فعالیت های پس از حادثه



آمادگی

رسیدگی به حادثه: آمادگی

- هدف این مرحله

- مشخص کردن موارد زیر
  - سیاست های امنیتی و قوانین پایه
  - ابزارها و امکانات ارتباطی
  - ایجاد تیم و آموزش افراد
  - تجهیزات، نرم افزار و سخت افزارهای موردنیاز
  - مستندسازی

آمادگی: سیاست های امنیتی و قوانین پایه

- ایجاد بنرهای هشدار
- استراتژی های پاسخگوئی به حادثه
- یادداشت برداری
- نحوه ی اطلاع رسانی به مراجع قانونی
- آگاهی سازمان های همتا
- پشتیبانی مدیریتی

آمادگی: ابزارها و امکانات ارتباطی

- اطلاعات کامل تماس
- ایجاد یک طرح ارتباطی اضطراری
- مکانیزم های گزارش دهی حادثه
- پیجرها/تلفن های همراه
- اتاق جنگ(□□□ □□□ □)

آمادگی: ایجاد تیم و آموزش قبلی افراد

- ساخت تیم و انتخاب اعضای آن
- سازمان تیم
- آموزش های نحوه ی برخورد با حادثه

آمادکی: ابزارها و منابع

- ۲) نرم افزار ها و سخت افزار های تحلیل حادثه

  - نرم افزار های تهیه پشتیبان و تصویر از دیسک
  - Packet Snifferها و تحلیل کننده های پروتکل
  - سیستم های کامپیوتری قابل حمل
  - چاپگر قابل حمل برای چاپ logها
  - رسانه های خام
  - تجهیزات شبکه بندی

آمادگی: ابزارها و منابع

- ۳) منابع تحلیل حادثه

  - لیست پورت های فعال و پورت های مورد استفادهٔ اسب های تروای معروف
  - مستند سازی مشخصات سیستم ها: سیستم عامل، پروتکل ها، ...
  - برنامه های کاربردی و سیستم تشخیص نفوذ (IDS)
  - نمودار های ترافیکی شبکه روی تمام نقاط حساس
  - درهم ساز روی تمامی فایل های حساس

- ۴) تجهیزات بازیابی سیستم پس از حادثه

آمادگی: مستندسازی

- ایجاد چک لیست از سیستم ها
- نمودارهای ترافیک شبکه
- استفاده از تابع درهم ساز

تشخیص و
تحلیل
حادثه

تشخیص و تحلیل حادثه

- دلایل اهمیت

- تاثیر تشخیص صحیح در واکنش مناسب
- تعداد زیاد نشانه ها
- تعداد پایین حوادث واقعی

تشخیص و تحلیل حادثه-مراحل

تشخیص و تحلیل حادثه-مراحل

- Triage
  - در علم پزشکی:
    - فرآیند اولویت بندی بیماران بر اساس میزان وخامت وضعیت آنها
  - در توسعه و طراحی سیستم ها:
    - به جای بیماران روی منابع و ملزومات هر طرح انجام می شود
    - هدف: استفاده‌ی بهینه از منابع و نیروها

تشخیص و تحلیل حادثه-مراحل

- Triage

- RFC2350:
  - فرآیند Triageشامل:
    - ارزیابی گزارش ها: تفسیر و اولویت بندی گزارش های دریافتی و مربوط کردن هریک از آنها به حوادث جاری
    - وارسی : واقعا حادثه‌ای رخ داده؟ در چه مقیاسی؟

تشخیص و تحلیل حادثه- علائم

- انواع علائم دریافتی از یک حادثه

  - پیش علامت ها(Precursors):نشانگر احتمال وقوع حادثه امنیتی در آینده
  - نشانه ها(Indications): نشانگرحادثه ای در حال وقوع

- منابع دریافت علائم

  - هشدار های نرم افزار های امنیتی
  - رخدادنماهای ثبت شده از وقایع
  - اطلاعاتی که به صورت عمومی در دسترس است
  - افراد ناظر بر شبکه

تشخیص و تحلیل حادثه-دسته‌بندی

- اهمیت

- تنوع حوادثی که ممکن است رخ دهد
- تفاوت در نحوه‌ی پاسخگویی به حوادث گوناگون
- نیاز به دستورالعمل معین منعطف برای پاسخگویی به انواع حوادث

تشخیص و تحلیل حادثه-دسته بندی

- انواع حوادث
  - حملات جلوگیری از سرویس(DoS)
  - گسترش بد افزار ها(Malicious Code)
  - دسترسی غیر مجاز به شبکه(Unauthorized Access)
  - استفاده بی جا از شبکه توسط کاربران مجاز(Inappropriate Usage)
  - حملات ترکیبی (Multiple Component)

تشخیص و تحلیل حادثه- تشخیص بهینه

- شرایط نمونه برای تشخیص بهینه

- اندازه گیری مشخصات شبکه و سیستم
  - مرجع مقایسه در هنگام تشخیص حادثه
- درک شرایط عادی شبکه
  - چرا: تشخیص تغییر وضعیت عادی
  - چگونه: مرور رخدادنماها و هشدار های نرم افزار های امنیتی
- اجرای عملیات جستجوی همبستگی بین وقایع
  - چگونه: الگوریتم های هوش مصنوعی
  - نتیجه: دقت بیشتر در عملیات تحلیل حادثه

تشخیص و تحلیل حادثه- تشخیص بهینه

- شرایط نمونه برای تشخیص بهینه

- وجود سیاست های مدیریت رخدادنماها و مرکزی نگهداری رخدادنما
  - چرا: دسترسی به تمام رخدادنماها دریک مکان و به صورت تدوین شده در صورت لزوم
  - شرایط مرکز:
    - مکان فیزیکی امن
    - غیر فعال بودن سرویس های دیگر
    - فعال نبودن سرویس های RPC
    - ثبت رمان انتقال رخدادنماها به سیستم
    - حذف حساب های کاربری اضافه روی سیستم

تشخیص و تحلیل حادثه- تشخیص بهینه

- شرایط نمونه برای تشخیص بهینه

- تهیه یک ماتریس تشخیص توسط افراد با تجربه گروه
  - کاربرد: بیان نوع حادثه و احتمال وقوع آن را در صورت مشاهده علائم مختلف
- استفاده از Packet Snifferها برای جمع آوری اطلاعات بیشتر:
  - زمانی که اطلاعات کافی در دست نیست
  - با اجازهٔ مستقیم مدیر سیستم فناوری اطلاعات

تشخیص و تحلیل حادثه-اولویت بندی

- اولویت بندی حوادث

- چرا ؟
  - بدلیل محدودیت منابع موجود
  - معمولاً درجه اهمیت حوادث و منابع تحت تأثیر متفاوت است.
- چه زمانی؟
  - قرار داد های موجود (SLA) معمولاً محدودیت زمانی برای پاسخگویی مشخص نمی کنند.

تشخیص و تحلیل حادثه- اطلاع رسانی

- اطلاع رسانی

- تمام اعضای گروه باید آمادۀ پاسخ گویی به سؤالات مدیر سیستم فناوری اطلاعات باشند
- پاسخ را در قالب گزارش به مدیر ارائه می شود
- در سیاست های گروه امداد امنیت نحوه پاسخ گویی و محدودۀ اطلاع رسانی مشخص شده است
- حداکثر زمان در اختیار برای اطلاع رسانی از مواردی است که باید تعیین شده و به اعضای گروه ابلاغ شود.

تشخیص و تحلیل حادثه- مستند سازی

- مستند سازی روال تشخیص حادثه

- چرا؟
  - انتقال سریع و دقیق اطلاعات به گروه پاسخگویی به حادثه
  - کاهش میزان خطا
  - در مسائل قانونی به عنوان شاهد در دادگاه
- چه مواردی ؟
  - ثبت وضعیت عملیات در هر زمان
  - اقدامات انجام شده ودر حال انجام
  - تغییرات صورت گرفته در فایل ها
  - مکالمات تلفنی
  - ...

تشخیص و تحلیل حادثه-مستند سازی

- مستند سازی روال تشخیص حادثه

- چند نکته:
  - مکان نگهداری مستندات
  - زمان تولید سند
  - امضای سند
  - در برخی موارد وظیفه اختصاصی افراد

محدودسازی

رسیدگی به حادثه: محدودسازی

- هدف این مرحله
- فعالیت های اولیه
  - توسعه ی سیستم
  - آگاهی به مدیریت
- مراحل مختلف محدودسازی
  - محدودسازی کوتاه مدت(Short-Term Containment)
  - گرفتن نسخه ی پشتیبان از سیستم(System Backup)
  - محدودسازی درازمدت(Long-Term Containment)
- معیارهای کلی انتخاب راهبرد مناسب

محدودسازی: محدودسازی کوتاه مدت

- هدف از محدودسازی کوتاه مدت
- برخی از فعالیت های این مرحله
  - قطع کابل برق و شبکه
  - مجزاکردن سرور هک شده روی یک سوئیچ مجزا
  - به کارگیری فیلتر برای روترها یا دیواره های آتش
  - تغییر پیکربندی DNS
  - اطلاع به مدیریت سازمان و اعلان قطعی سیستم ها

محدودسازی: فعالیت های جانبی

- هماهنگی با سرویس دهنده ی موردنظر(ISP)
- نگهداری یک پروفایل
- تهیه ی نسخه ی پشتیبان از سیستم
  - مجزا کردن سیستم
  - تحلیل رونوشتی از تصاویر قانونی
- ادامه ی عملیات

محدودسازی: محدودسازی درازمدت

- هدف از محدودسازی دراز مدت
- نحوه ی انتقال به مرحله ی ریشه کنی
- برخی از فعالیت های این مرحله
  - □□□□ کردن سیستم و سیستم های مرتبط
  - تغییر پسوردها
  - مسیریابی تهی
  - به کارگیری قوانین دیواره ی آتش و مسیریاب ها
  - حذف/غیرفعال کردن حساب ها

محدودسازی: معیارهای انتخاب راهبرد مناسب

- میزان اطلاعات سرقت شده و خسارت بالقوه
- میزان مدارک لازم برای جمع آوری
- اهمیت قابلیت دسترسی سرویس
- منابع و زمان لازم جهت پیاده سازی استراتژی موردنظر
- میزان اثربخشی استراتژی

ریشه کنی

رسیدگی به حادثه: ریشه کنی

- هدف از این مرحله
- برخی از فعالیت های این مرحله
  - بازگرداندن سیستم بااستفاده از نسخه ی پشتیبان
  - حذف نرم افزارهای مخرب
  - مقاوم سازی و افزایش امنیت سیستم
  - ارزیابی آسیب پذیری

ریشه کنی: بازگرداندن سیستم و حذف نرم افزارهای مخرب

- استفاده از آخرین نسخه ی پشتیبان
  - نیاز به ساخت مجدد سیستم در حملاتی مانند Rootkit
- حذف نرم افزارهای مخرب
  - ویروس ها
  - Backdoor
  - Rootkit یا Kernel Rootkit

ریشه کنی: مقاوم سازی و افزایش امنیت سیستم

- پیاده سازی مکانیزم های حفاظتی مناسب
  - به کارگیری مسیریاب ها و دیواره ی آتش
  - تغییر آدرس IP یا نام سیستم
  - مسیریابی تهی آدرس های IP خاص
  - تغییر نام های سرور نام حوزه(DNS)
  - به کارگیری patchها و مقاوم کردن سیستم

ریشه کنی: ارزیابی آسیب پذیری

- انجام تحلیل کامل آسیب پذیری
  - ارزیابی شبکه
  - ارزیابی سیستم
  - بررسی آسیب پذیری های مرتبط
  - پویش کامل شبکه برای پورت های خاص(Nessus،Nmap)

ترمیم

رسیدگی به حادثه: ترمیم

- هدف این مرحله
- اعتبارسنجی سیستم
  - بررسی عملیات موردنظر و حالت سیستم
  - ارزیابی عملکرد سیستم توسط بازرسان حادثه و واحد موردنظر در سازمان
- بازیابی عملیات
- نظارت

ترمیم : نظارت

- نظارت پیوسته و کامل پس از شروع به کار مجدد سیستم
- استفاده ی کامل از ابزارهای مختلف نظارت بر شبکه
  - ایجاد یک نشانه ی شخصی(Custom Signature) از مسیر حمله ی اصلی
- بررسی دقیق رخدادنماهای مرتبط با سیستم عامل و برنامه های کاربردی

فعالیت‌های پس از حادثه

رسیدگی به حادثه: فعالیت های پس از حادثه

- هدف از این مرحله
- اقدامات بعدی
  - مرور حادثه، مستندسازی مشکلات، و برطرف کردن ضعف های سیاست ها و روال ها
  - تشکیل جلسات به منظور مرور مستندات و تبادل نظر پیرامون آن
  - ارسال پیشنهادات به مدیریت
  - پیگیری جلسات