روش های ارزیابی آسیب پذیری امنیتی

Cyber Security Vulnerability Assessment

By Dr Nasser Modiri – Jan 10, 2020

Characterizing and Scoring Vulnerabilities


Threat
Asset
Vulnerability
Risk

آسیب پذیری کسب و کار

- هر سازمانی ماموریتی را دنبال می کند و برای پشتیبانی بهتر از ماموریت هایش از سیستم های فناوری خودکار استفاده می کند.
- بنابراین مدیریت ریسک نقش حیاتی را در حفاظت از دارایی های سازمان و در نتیجه به انجام رساندن ماموریت های سازمان ایفا می کند.
- توانایی یک سازمان برای نگه داشت و استمرار فعالیت‌های محوری و حیاتی خود پس از بروز یک حادثه و همچنین سرعت بازیابی سازمان و بازگشت به حالت عادی، می‌توانند عوامل اساسی موفقیت و یا شکست یک سازمان را تعیین نمایند.

آسیب پذیری کسب و کار

- اگر هدف،ایجاد امنیت است نباید فقط امنیت مطرح شود(زیرا امنیت یک فرایند است و نه یک محصول) حتماً باید استمرار کسب و کار نیز وجود داشته باشد.
- زیراکه رقابتی شدن محیط کسب و کار، ضرورت ایجاد یکپارچگی درون سازمانی و بین سازمانی را ایجاد می کند و سازمانی یکپارچه است که از امنیت بالایی برخوردار باشد.

آسیب پذیری کسب و کار

- امنیت از نظر مفهومی به وضعیتی اطلاق می‌شود که نیروهای حفظ کننده ی وضع موجود، توان محافظت را از نیروهای شناخته شده ی برهم زننده ی آن داشته باشند.
- همچنین امنیت بسیار هزینه‌بر است پس نباید به صورت مجزا به امنیت پرداخت بلکه باید بتوان در راستای استمرار کسب و کار که سبب ایجاد امنیت هم خواهد شد، هزینه کرد.
- شاید بتوان گفت یکی از مهم‌ترین موضوعاتی که امنیت به ارمغان خواهد آورد استمرار کسب و کار است و یکی از دلایلی که سبب اختلال در استمرار کسب و کار می شود نادیده گرفتن امنیت می باشد.

آسیب پذیری کسب و کار

- اشتباه رایجی که وجود دارد این است که تصور می شود امنیت و کسب و کار دو مقوله مجزا هستند. اما واقعیت این است که امنیت باید بخشی از فرایند کسب و کار سازمان باشد.
- فرایند کسب و کار سازمان باید تغییر یا گسترش یابد تا امنیت را بتوان در انتها احساس نمود.
- باید استمرار کسب و کار سازمان را پیش‌بینی کرده و در جاهای مناسب سیاست امنیتی به آن اضافه شود تا فرآیند کسب و کار با موضوعات امنیتی بهینه گردد.

پایه‌ها و اصول مبنا برای استمرار کسب و کار

- تمامی فعالیت‌های کسب و کار با نوعی خطر انقطاع در ارتباط خواهند بود
- مواردی همچون اختلالات تکنولوژیکی، سیل، انقطاع تجهیزات، حملات تروریستی و رکود اقتصادی از آن جمله می‌باشند.
- توانایی یک سازمان برای نگه داشت و استمرار فعالیت‌های محوری و حیاتی خود پس از بروز یک حادثه و همچنین سرعت بازیابی سازمان و بازگشت به حالت عادی، می‌توانند عوامل اساسی موفقیت و یا شکست یک سازمان را تعیین نمایند.
- امروزه نیاز برای کسب اطمینان از استمرار خدمات در سازمان‌ها به حداکثر میزان خود رسیده است چرا که امروزه سازمان‌های نوین، ۲۴ ساعت شبانه روز را در طی ۷ روز هفته در حال ارایه خدمات بوده و وابستگی و بعضا دامنه قابل تحمل سازمان برای در دسترس بودن برخی از خدمات فناوری اطلاعات به زمانی کمتر از ساعت می رسد.
- استمرار کسب و کار، فعالیتی است که برای حصول اطمینان از در دسترس بودن بخش‌های حیاتی کسب و کار برای مشتریان، تأمین کنندگان و .... انجام می‌شود.
- استمرار کسب و کار به آن دسته از فعالیت‌هایی اشاره می‌کند که به طور روزانه برای نگهداری سرویس، سازگاری و بازیابی مجدد انجام می‌گیرد.

پایه‌ها و اصول مبنا برای استمرار کسب و کار

- برای پایداری و استمرار کسب و کار همانند هر موضوع مهندسی دیگر، مراحل ۸ گانه‌ای بایستی رعایت شوند که این مراحل در شکل .... نشان داده شده‌اند.
- هشت مرحله برای ایجاد و پایداری کسب و کار سازمان
- رعایت ترتیب این مراحل و چگونگی طرح هر یک، دارای اهمیت بسیار است. اگر بتوان برای هر کدام از این مراحل، نمونه‌های مختلفی داشت مطمئناً سازمان می‌تواند به اهداف خاص خود به صورت مناسب دست یابد. در ادامه اشاره مختصری به هر یک از این مراحل شده است:
- در ابتدا لازم است استراتژی‌هایی برای استمرار کسب و کار داشته باشیم و آنها را مشخص نماییم. باید توجه داشت استراتژی‌ها همان چشم‌اندازها هستند که معمولاً دست نیافتنی می‌باشند. استراتژی فراتر از هر چیز، یک مفهوم ذهنی و مستندی است که ماموریت و چشم‌انداز سازمان را در بر می‌گیرد.
- در مرحله بعد استراتژی‌ها، تبدیل به یک سری اهداف می‌شوند. مدل‌های مختلفی برای تعریف اهداف سازمانی وجود دارد و ممکن است یک یا چندین مدل بکار گرفته شود. اهداف باید برنامه‌هایی باشند که بتوانند دقیقاً ما را به نتیجه برسانند و باید بر اساس استراتژی (راهبرد) تعریف شده باشند. جهت اجرایی و عملیاتی نمودن یک راهبرد، می‌توان اهداف بلند مدت، میان مدت، کوتاه مدت و مقطعی داشت.

هشت مرحله برای ایجاد و پایداری کسب و کار سازمان

پایه‌ها و اصول مبنا برای استمرار کسب و کار

- بعد از اهداف، سیاست‌ها مطرح می‌شوند که به تعریف آنچه برای دستیابی به اهداف باید انجام شود کمک می‌کنند و در واقع ناشی از منطق و استراتژی‌های کسب و کار می‌باشند.
- سیاست‌ها، قوانین و اصول کسب و کار یک سازمان هستند که از پیوستگی و برآوردن مسیر و اهداف سازمان اطمینان می‌دهند. سیاست‌ها، قوانین کسب و کاری که تحت آن سازمان و واحدها کار خواهند کرد را طرح‌ریزی و چیدمان می‌کنند اما هیچ گونه صحبتی در مورد چگونگی انجام کار نمی‌کنند.
- بر طبق سیاست‌ها، استانداردها انتخاب می‌شوند. معمولاً در سیاست‌ها به ذکر استانداردهایی که باید استفاده شوند اشاره می‌شود. در این مرحله، باید این استانداردها مورد بررسی قرار گیرند. استانداردها، کنترل‌های اجباری سطح پایینی هستند که به اجرای سیاست‌ها و حمایت از آن‌ها کمک می‌کنند. به عنوان مثال در زمینه فناوری اطلاعات حتماً باید استانداردهای متداول و مرتبط را استفاده کنیم.
- پس از استانداردها، تاکتیک‌ها با همان روش‌های انجام کار مطرح می‌شوند. به عبارت دیگر ابتدا کار باید استاندارد باشد تا بر اساس آن، روش‌هایی ذکر شود. معمولاً برای انجام هر کاری چندین روش مختلف وجود دارد. برای نیل به اهداف، ممکن است بتوان از روش‌های مختلفی استفاده کرد. به عنوان مثال برای تداوم کسب و کار ممکن است یکی از تاکتیک‌ها، برون سپاری کل یک کار باشد یا ممکن است تاکتیک دیگر به این صورت باشد که بخشی از کار را خودمان انجام دهیم و تنها بخشی از آن مثلاً قسمت فروش را برون سپاری کنیم. حال از بین این روش‌های مختلف که در راستای نیل به اهداف وجود دارد مسلماً روشی وجود خواهد داشت که براساس شاخص‌های مورد نظر، مناسب‌تر خواهد بود. لازم به ذکر است تاکتیک‌ها چگونگی انجام و اجرا را مشخص نمی‌کنند.

پایه‌ها و اصول مبنا برای استمرار کسب و کار

- هر تاکتیک به یک سری راهنما تبدیل خواهد شد که دارای کنترل‌های اختیاری و پیشنهادی هستند و براساس مراحل طی شده تا این مرحله، توصیه‌ها و پیشنهاداتی مطرح می‌شود. از آنجایی که استانداردها کلی هستند اگر بخواهیم آنها را مثلاً در یک صنف خاص به کار ببریم لازم است یک سری پیشنهادات در حوزه آن کار بیان شود.

- علاوه بر پیشنهاداتی که در راهنماها بیان کردیم در کنار آنها به بررسی بهترین تجارب (بهترین کارکردها) در هر حوزه پرداخته می‌شود. در واقع همواره قبل از انجام کار توصیه می‌شود بهترین نمونه‌های موجود از انجام آن کار مورد بررسی قرار گیرد و با شناخت وضع موجود آن و متناسب با شرایط و استراتژی‌های سازمان، به آن روش‌ها نزدیک شویم. به کارگیری بهترین تجارب به معنی یادگیری از تجارب موفق دیگران است و به عنوان یک الگو و معیاری برای محک زدن و مقایسه کسب و کارمان با سایر کسب و کارهای موفق توصیه می‌شود.

- مرحله آخر همان مرحله اجرایی کردن نهایی کار (دستورالعمل‌ها) می‌باشد که چگونگی انجام کار را شرح می‌دهد و به صورت گام به گام به شرح مراحل اجرایی کار می‌پردازد. رویه‌ها اغلب شامل چک‌لیست‌هایی هستند که کنترل‌های افزوده‌ای را برای اطمینان از درستی انجام کار فراهم می‌کنند. دستورالعمل‌ها به تفصیل شرح می‌دهند چه گام‌هایی، چه زمانی و چگونه انجام شده‌اند.

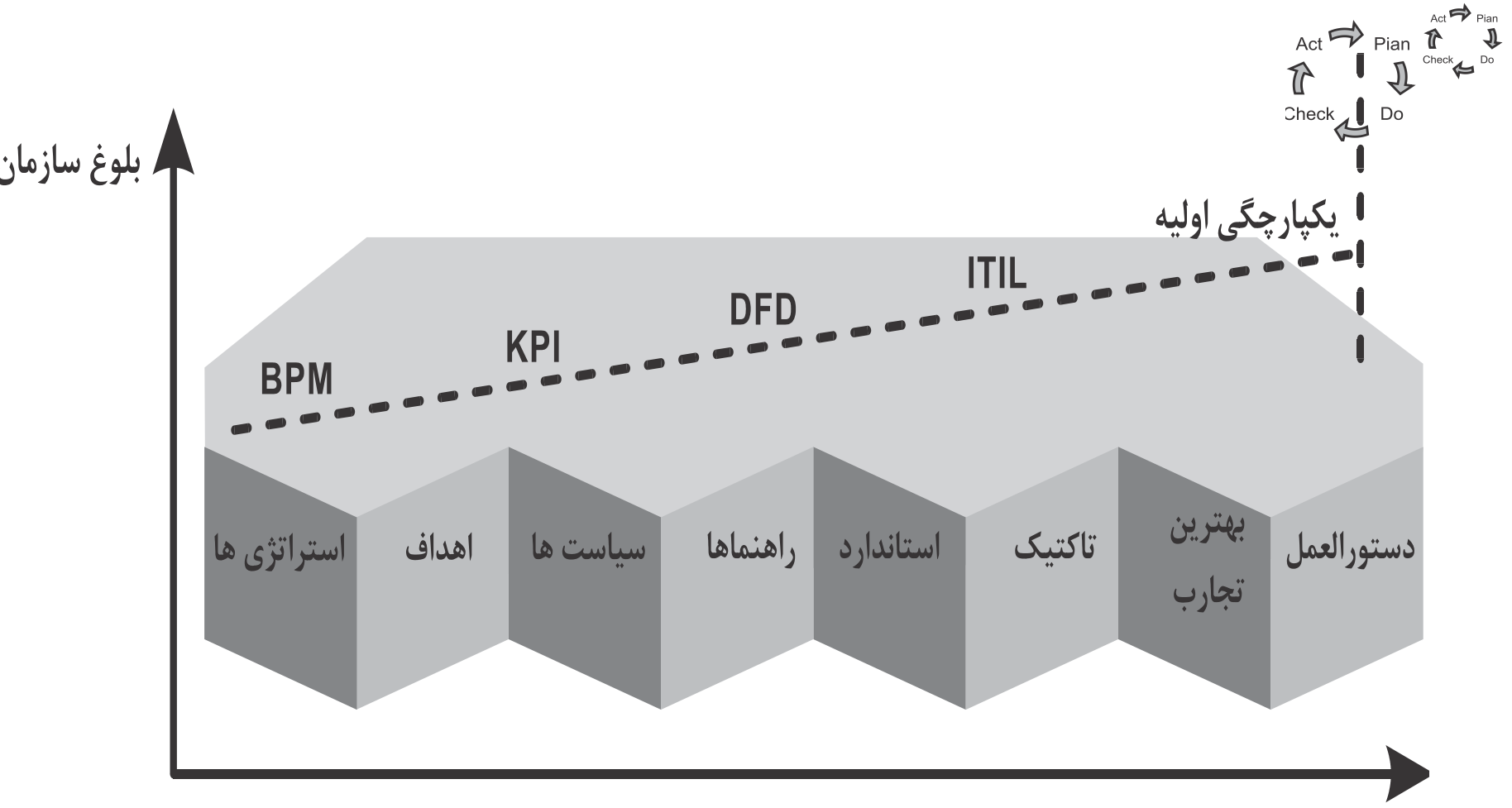
مدل‌سازی فرآیند کسب و کار

- این ۸ مرحله به عنوان ستون‌های سازمان محسوب می‌شوند و سایر فرآیندها و عملیات در این محدوده قرار می‌گیرند و برای برقراری امنیت باید در راستای امنیت در آن سازمان، این پیش فرض‌ها و مراحل اولیه را به اجرا رساند. پس از این ۸ مرحله، لازم است ۴ گام دیگر در سطحی بالاتر طی شود تا سازمان به مرحله یکپارچگی اولیه و بلوغ برسد:
- مهم‌ترین کار این است که ابتدا مدل‌سازی فرآیند کسب و کار (BPM) برای هر واحد سازمان ترسیم شود. باید تصویر مشخصی از فرایند کسب و کار هر واحد وجود داشته باشد و به درستی درک شود هر واحد چه کاری باید انجام دهد. انواع مختلف نرم‌افزارها، استانداردها و زبان‌ها، برای پیاده‌سازی BPM وجود دارد.
- پس از انجام عمل (ترسیم) BPM ، بایستی برای آن، تعدادی نقاط عملکردی تعریف نمود. در واقع باید در آن فرآیند، شاخص‌های کلیدی عملکرد (KPI)مربوطه دیده شود و نقاط عملکردی سازمان شناخته شود.

مدل‌سازی فرآیند کسب و کار

- مرحله بعد شامل جزئیات بیشتری است، یعنی در این مرحله جزئیات ارتباط داده‌ها (DFD) اهمیت پیدا می‌کند؛ و ترسیم جریان داده‌ها صورت می‌گیرد. جزئیات ارتباطات جریان داده را حداقل در سه سطح DFD, DFD,DFD ، باید داشته باشیم.
- در نهایت باید بتوان به منظور کنترل هر واحد، خدماتی را که ارائه می‌شود، توصیف نمود. به عبارت دیگر باید بتوَان بر مبنای یک استاندارد، نیازهای خود را به عنوان سرویس تعریف نمود. در این مرحله باید نسبت به سازمانی که تاکنون شناخته شده است، دید و تصورIT داشته و KPI هایی را که در رابطه با فناوری اطلاعات هستند شناسایی شوند.(ITIL KPI).
- اگر این چهار مرحله را برای همه واحدهای سازمانی طی کنیم، در مرحله پنجم می‌توانیم مرز کار خود را مشخص نماییم. به عبارتی برای نخستین بارمی توان، سازمان را به صورت جامع و یکپارچه نگریست. این وضعیت موجود، طی سال‌ها (در طول عمر سازمان) می‌تواند فرآیندها را بهبود بخشیده و کسب و کار را روز به روز بهینه‌تر سازد تا به وضعیت مطلوب نزدیک شد.

مراحل برای رسیدن به یکپارچگی اولیه و تصویر جامع از سازمان



فرآیند طرح‌ریزی استمرار کسب و کار

- برای ایجاد طرح استمرار، فرآیندی برای طرح‌ریزی آن در ادامه آمده است. چهار مرحله اصلی تحت عناوین کلی پیشگیری و اجتناب، ایجاد آمادگی، پاسخ و در نهایت بازیابی و ترمیم بایستی صورت پذیرد.
- در نهایت پس از تهیه طرح باید به صورت دوره‌ای آن را بازبینی و تست نمود.
- پیشگیری و اجتناب
  - اقدامات صورت گرفته برای کاهش یا حذف احتمال و اثرات ریسک در یک رخداد است که به طور گسترده یا برنامه‌ریزی مدیریت ریسک پوشش داده می‌شوند.
- ایجاد آمادگی در صورت مواجه شدن با رخداد
  - اقدامات انجام شده قبل از یک رخداد به منظور اطمینان یافتن از پاسخ و بازیابی مؤثر می‌باشد که به طور گسترده با آنالیز اثر کسب و کار پوشش داده می‌شود.

فرآیند طرح‌ریزی استمرار کسب و کار

- پاسخ
  - اقدامات انجام شده برای پاسخ به یک رخداد به منظور محدود نگه داشتن، کنترل و حداقل کردن اثرات است که به طور گسترده با برنامه‌ریزی پاسخ رخداد پوشش داده می‌شود.
- بازیابی
  - اقدامات انجام شده برای بازیابی یک رخداد به منظور حداقل کردن وقفه و زمان بازیابی که توسط برنامه ریزی و طرح بازیابی پوشش داده می‌شود.

مراحل اول و دوم کلیه تحلیل‌ها و اقدامات پیش از وقوع رخداد را مورد بررسی قرار می‌دهند و در فازهای سوم و چهارم با کمک تحلیل‌های بدست آمده از دو فاز قبل (مدیریت ریسک و آنالیز تاثیر کسب و کار)، اقدامات لازم در صورت رویارویی با رخداد را در بر می‌گیرند.

ارزیابی آسیب پذیری

- آسیب پذیری هایی که در معرض تهدید قرار ندارند نیازمند به یک کنترل امنیتی نیستند تنها می بایست شناسایی و تحت نظارت تغییرات قرار گیرند . ل
- ازم به ذکر است که پیاده سازی نادرست کنترل های امنیتی می تواند به خودی خود منجر به بروز یک آسیب پذیری شود.
- آسیب پذیری ها به خصوصیات یک دارایی و اهداف کاربرد آنها نیز بستگی دارند.
- آسیب پذیری ها می توانند از منابع مختلفی نتیجه شوند.

شناسایی نقاط آسیب پذیر

- یک آسیب پذیری به خودی خود منجر به آسیب نمی شود بلکه نیازمند به یک تهدید جهت بهره برداری از آن آسیب پذیری است.
- پس از شناسایی دارایی ها و لیست تهدیدات و کنترل های موجود می بایست به شناسایی نقاط آسیب پذیر پرداخت.
- نقاط آسیب پذیری می توانند توسط تهدیدات مورد بهره برداری قرار گرفته و منجر به آسیب رسانی به دارایی های اطلاعاتی گردند.

شناسایی نقاط آسیب پذیر

- آسیب پذیری ها در حوزه های زیر ممکن است شناسایی شود:
  - سازمانی
  - فرآیندها و رویه ها
  - روتین های مدیریتی
  - افراد
  - محیط فیزیکی
  - پیکربندی سیستم های اطلاعاتی
  - تجهیزات سخت افزاری، نرم افزاری یا مخابراتی
  - وابستگی به بخش های بیرونی و خارجی

شناسایی عواقب آسیب پذیری

- پس از شناسایی نقاط ضعف و تهدیدات مربوط به دارایی های اطلاعاتی، می بایست عواقب ناشی از بهره برداری از آسیب پذیری ها بوسیله نقص محرمانگی، دسترس پذیری و صحت دارایی ها شناسایی گردد.

آسیب پذیری های غیر تکنیکال

آسیب پذیری های غیرتکنیکال در قالب ۶ نوع تقسیم بندی میگردند:

1.سازمانی
2.نیروی انسانی
3.مکان و موقعیت
4.سخت افزاری
5.نرم افزاری
6.شبکه های

آسیب پذیری سازمانی

- فقدان یک رویه رسمی برای ثبت نام و انصراف کاربران
- فقدان یک رویه رسمی برای بازبینی حق دسترسی ها (نظارت)
- فقدان ماده های امنیتی کافی در قرارداد با مشتریان و شخص ثالث
- فقدان رویه مانیتورینگ برای امکانات پردازش اطلاعات
- فقدان ممیزی منظم (نظارت)
- فقدان رویه برای شناسایی و ارزیابی ریسک
- فقدان گزارشات خطای ثبت شده از Log های اپراتوری و مدیریتی
- پاسخگویی ناکافی نگهداری سرویس ها
- فقدان یا کمبود قرارداد سطح سرویس (SLA)
- فقدان رویه کنترل تغییر
- فقدان رویه ای رسمی برای کنترل اسناد ISMS
- فقدان رویه ای رسمی برای ثبت نظارت ISMS
- فقدان یک فرآیند رسمی برای مجوز اطلاعات دسترسی عمومی
- فقدان تخصیص مناسب مسئولیت های امنیت اطلاعات

آسیب پذیری سازمانی

- فقدان طرح تداوم
- فقدان سیاست های استفاده از ایمیل
- فقدان یک رویه برای ارائه نرم افزار به سیستم های عملیاتی
- عدم ثبت log های عملیاتی و مدیریتی
- فقدان یک رویه برای استفاده از اطلاعات طبقه بندی شده
- فقدان تعریف مسئولیت های امنیت اطلاعات در توصیفات شغلی
- فقدان ماده های امنیت اطلاعات در قرارداد با کارمندان
- فقدان تعریف فرآیند انظباطی در مواقع بروز رخداد امنیتی
- فقدان سیاست های رسمی برای استفاده از کامپیوترهای قابل حمل
- فقدان کنترل برای دارایی های خارج از فرضیه
- فقدان سیاست گذاری برای رعایت اصل , میز و صفحه دسکتاپ پاک ,
- فقدان مجوز مرکز پردازش اطلاعات
- فقدان ایجاد مکانیزم مانیتورینگ برای نقض های امنیتی
- فقدان بازبینی منظم مدیریتی
- فقدان رویه برای گزارش ضعف های امنیتی
- فقدان رویه برای پیروی از مقررات حقوق معنوی

آسیب پذیری نیروی انسانی

- عدم وجود پرسنل
- روش های جذب ناکافی
- آموزش ناکافی در حوزه امنیت
- استفاده نادرست از سخت افزار و نرم افزار
- فقدان آگاهی امنیتی
- فقدان مکانیزم های مانیتورینگ
- کار بدون نظارت خارجی
- فقدان سیاست گذاری در استفاده صحیح از رسانه های ارتباطی و پیامی

آسیب پذیری مکان و موقعیت

- بی دقتی در استفاده از کنترل دسترسی فیزیکی به ساختمان ها و اتاق ها
- موقعیت های در معرض خطر سیل
- شبکه برق بی ثبات
- فقدان محافظت فیزیکی از ساختمان ها، درها، پنجره ها

آسیب پذیری سخت افزاری

- نگهداری ناکافی/ نصب ناقص رسانه های ذخیره سازی
- فقدان طرح جایگزین دوره ای
- حساسیت به رطوبت، غبار و رطوبت، نشت مواد
- حساسیت به تابش الکترومغناطیس
- فقدان کنترل کارآمد برای تغییرات پیکربندی
- حساسیت به تغییرات ولتاژ
- حساسیت به تغییرات درجه حرارت
- رسانه های محافظت نشده
- عدم مراقبت از سخت افزارهای در اختیار
- کپی های کنترل نشده

آسیب پذیری نرم افزاری

- فقدان یا ناکافی بودن تست نرم افزار
- نقص های مشهور در نرم افزار
- Logout نکردن هنگام ترک ایستگاه کاری
- استفاده از رسانه های ذخیره سازی بدون پاک کردن مناسب
- فقدان ممیزی ادامه دار
- تخصیص اشتباه حقوق دسترسی
- نرم افزارهای توزیع شده گسترده
- استفاده از برنامه کاربردی برای داده های غلط در مقطعی از زمان
- رابط کاربری پیچیده
- فقدان مستندسازی
- راه اندازی پارامترهای نادرست
- داده های نادرست
- فقدان مکانیزم های شناسایی و احراز هویت نظیر احراز هویت کاربر
- جداول پسورد محافظت نشده
- مدیریت رمز عبور ضعیف
- فعال بودن سرویس های غیرضروری
- نرم افزارهای جدید یا نابالغ
- مشخصات مبهم و ناقص برای برنامه نویسان
- عدم کنترل موثر در تغییر
- استفاده از نرم افزارها و دانلودهای کنترل نشده
- فقدان کپی Backup ها
- فقدان حفاظت فیزیکی از ساختمان ، درها و پنجره ها
- شکست در تولید گزارشات مدیریتی

آسیب پذیری شبکه ای

- فقدان مدارکی از پیام های ارسالیو دریافتی
- خط های ارتباطی محافظت نشده
- ترافیک حساس محافظت نشده
- کابل کشی مشترک ضعیف
- نقطه شکست
- فقدان شناسایی و احراز هویت فرستنده و گیرنده
- معماری شبکه ناامن
- انتقال واضح پسوردها (عدم رمزگذاری پسورد)
- مدیریت نامناسب شبکه
- ارتباطات محافظت نشده شبکه عمومی

ارزیابی آسیب پذیری های فنی و تکنیکال

- آسیب پذیری فنی با رویکرد پیشگیرانه به شناسایی نقاط آسیب پذیر سرویس ها و تجهیزات شبکه از لحاظ فنی می پردازد.
- در این رویکرد از تکنیک های مختلف نظیر: ابزارهای پویش اتوماتیک، ارزیابی و تست امنیتی، تست های نفوذ و مرور کد استفده میگردد.
- کنترل آسیب پذیری‌های فنی تجهیزات و سرویس‌های شبکه تا آنجا اهمیت دارد که به عنوان یکی از مهمترین الزامات استاندارد ISO/IEC 27001:2018 در پیاده سازی سیستم مدیریت امنیت اطلاعات (ISMS) نیز مورد توجه بوده است.
- متد ارزیابی انتخابی ما برای ارزیابی آسیب پذیری های فنی مبتنی بر راهنمای NIST 800-115 متعلق به وزارت بازرگانی ایالات متحده می باشد.

ارزیابی آسیب پذیری های فنی و تکنیکال

- استفاده از این روش مستند و قابل تکرار در انجام ارزیابی و آزمون آسیب پذیری مزایای زیر را به همراه دارد:
  - فرآهم سازی فرآیندی ساختارمند برای انجام ارزیابی که خطر آسیب رساندن به اطلاعات، تجهیزات و فعالیت جاری آن‌ها را به حداقل کاهش می‌دهد؛
  - عدم وابستگی نتایج به تجربه و نظر شخصی ارزیاب؛
  - استفاده محدود از منابع سیستم‌ها جهت انجام ارزیابی؛

ارزیابی آسیب پذیری های فنی و تکنیکال

- این متد با رویکرد White-Box به ارزیابی شبکه می پردازد.
- در رویکرد جعبه سفید فرد ارزیاب در موقعیت مدیران شبکه قرارگرفته و با حق دسترسی های آنان اقدام به ارزیابی نقاط آسیب پذیر شبکه می نماید.
- برای شناسایی آسیب‌پذیریهای فنی در شبکه، از ابزارهای خودکار پویش آسیب‌پذیری نظیر Nessus، Nipper و همچنین جهت تحلیل یافته‌ها و اعتبارسنجی آنها از ابزارهایی نظیر Acunetix و Metasploit استفاده میگردد تا نتایج خروجی حاصل از کشف آسیب‌پذیری‌ها برای حذف خطای مثبت مورد اعتبارسنجی قرار گیرد.
- False Positive

ارزیابی آسیب پذیری های فنی و تکنیکال

- روش امتیاز دهی و رتبه بندی بر اساس متد CVSS V3.0 می باشد.
- ارزیابی آسیب پذیری های فنی شامل دو بخش است که یکی به شناسایی و دیگری به اعتبار سنجی آسیب‌پذیری‌ها اختصاص دارد.
- در بخش اول لیستی از آسیب‌پذیری‌های سیستم هدف که یک منبع تهدید بالقوه می‌تواند از آنها بهره‌برداری کند استخراج شد.
  - در شناسایی آسیب‌پذیری‌ها ابزارهای خودکار پویش آسیب‌پذیری مورد استفاده قرار میگیرند.
- سپس برخی از آسیب‌پذیری‌ها که از درجه Critical و High بوده‌اند با رعایت اصل عدم وقفه در سرویس‌های حساس مورد بازبینی و اعتبارسنجی قرار میگیرند.

امتیازدهی و تعیین شدت آسیب‌پذیری‌ها

- این بخش به چگونگی امتیاز دهی به آسیب‌پذیری‌ها مبتنی بر متد CVSS V3.0 می‌پردازد.
- این روش توسط پایگاه ملی آسیب‌پذیری موسسه‌ی NIST برای امتیاز بندی شدت آسیب‌پذیری‌های کشف شده مورد استفاده قرار می‌گیرد.
- متد CVSS به یک آسیب‌پذیری از سه جنبه‌ی (پایه) Base ، (زمانی) Temporal و (محیطی) Environmental در مقیاسی از ۰ تا ۱۰ امتیاز اختصاص می‌دهد.
- شناخت مفاهیم این روش امتیاز دهی و عوامل موثر در آن برای محاسبه یک مقدار عددی که به عنوان شدت آسیب‌پذیری از آن نام برده می‌شود در فهم صحیح‌تر از گزارش و اینکه هر آسیب‌پذیری به چه نحوی می‌تواند منتج به خسارات شود ضرروی است.


TEMPORAL
METRIC GROUP
Exploitability
Remediation
Level
Report
Confidence

امتیازدهی و تعیین شدت آسیب‌پذیری‌ها

- امتیاز Base در متد CVSSv3 مربوط به خصایص ذاتی آسیب‌پذیری کشف شده و نرم‌افزاری که آسیب‌پذیری به آن تعلق دارد می‌باشد و براساس ضربه ناشی از بهره‌برداری به سیستم اطلاعاتی که آسیب‌پذیری در آن موجود است و قابلیت بهره‌برداری از آن آسیب‌پذیری، محاسبه می‌شود.

امتیازدهی و تعیین شدت آسیب‌پذیری‌ها

- امتیاز Temporal علاوه بر امتیاز Base، خصایص دیگری از آسیب‌پذیری را مدنظر قرار می‌دهد که در گذر زمان تغییر می‌کنند.
- امتیاز Temporal از ترکیب Base با پارامترهایی اضافی محاسبه می‌شود.
- پارامترها عبارتند از: ۱) سطح تائید جزئیات فنی و اطمینان از وجود یک آسیب‌پذیری گزارش شده ۲) وجود patch ویا وصله‌ی امنیتی برای رفع آسیب‌پذیری و ۳) امکان دسترسی به کد و یا تکنیک بهره‌برداری از آسیب‌پذیری برای مهاجمین.
- همانطور که مشخص است، این پارامترها در طول زمان تغییر می‌کنند و در تعیین شدت آسیب‌پذیری مجزا از امتیاز Base و بصورت انتخابی درنظر گرفته شده‌اند.

امتیازدهی و تعیین شدت آسیب‌پذیری‌ها

- امتیاز Environmental نیز همانند Temporal از پارامترهای بیشتری برای محاسبه شدت آسیب‌پذیری بهره می‌برد و بواسطه ترکیب امتیاز Temporal با چندین پارامتر دیگر بدست می‌آید.
- این پارامترها به اهمیت سیستم اطلاعاتی که آسیب‌پذیری برروی آن کشف شده از منظر کسب و کار سازمان می‌پردازند و از یک سازمان به سازمان دیگر متفاوت هستند.
- به همین دلیل Environmental در گزارش آسیب‌پذیری‌های کشف شده مورد توجه قرار نمی گیرد.

امتیاز Base– شدت فنی آسیب‌پذیری

- پارامترهای مورد استفاده در محاسبه امتیاز Base شامل:
  - بردار دسترسی،
  - پیچیدگی دسترسی،
  - احراز هویت،
  - ضربه به محرمانگی،
  - ضربه به صحت و تمامیت،
  - و ضربه به دسترس‌پذیری
- این پارامترها خصوصیات آسیب‌پذیری را مستقل از زمان و محیط بکارگیری سیستم آسیب‌پذیر نشان می‌دهند.
- از پارامترهای بیان شده سه پارامتر اول قابلیت بهره‌برداری از آسیب‌پذیری را مدنظر دارند
- و سه پارامتر بعدی برای سنجش میزان تاثیرگذاری بر سیستم هدف در صورت بهره‌برداری بکار می روند.

- Access Vector (AV)
- Access Complexity (AC)
- Authentication (AU)
- Confidentiality (C)
- Integrity (I)
- Availability (A)

امتیاز Base– شدت فنی آسیب‌پذیری

بردار دسترسی

- این پارامتر مربوط به چگونگی بهره‌برداری از آسیب‌پذیری توسط مهاجم است و تاثیر مکان دسترسی مهاجم نسبت به هدف را در قابلیت بهره‌برداری از سیستم آسیب‌پذیر می‌سنجد.
- هرچه مهاجم امکان بهره‌برداری دورتر داشته باشد، این پارامتر امتیاز بالاتری می‌گیرد.
- سه مقدار قابل تخصیص به این پارامتر شامل دسترسی محلی (Local)، دسترسی شبکه مجاور (Adjacent Network) و دسترسی از طریق شبکه (راه دور) (Network) هستند.

امتیاز Base– شدت فنی آسیب‌پذیری

پیچیدگی دسترسی

- پیچیدگی حمله‌ای که باید برای بهره‌برداری از سیستم آسیب‌پذیر پیاده شود در این پارامتر بیان می‌شود.
- برای این پارامتر سه مقدار بالا (High)، متوسط (Medium) و پائین (Low) درنظر گرفته شده است.
- هرچه پیچیدگی لازم برای بهره‌برداری از آسیب‌پذیری کمتر باشد، امتیاز آسیب‌پذیری بالاتر خواهد بود.

امتیاز Base– شدت فنی آسیب‌پذیری

احراز هویت

- این پارامتر نشان‌دهنده‌ی تعداد دفعات مورد نیاز احراز هویت است که یک مهاجم باید پیش از بهره‌برداری از آسیب‌پذیری انجام دهد.
- مقادیر شامل چندین بار (Multiple)، یک‌بار (Single) و بدون احرازهویت (None) می‌باشد که هرچه تعداد دفعات مورد نیاز احراز هویت بالاتر باشد، امتیاز آسیب پذیری کمتر خواهد بود.

امتیاز Base– شدت فنی آسیب‌پذیری

ضربه به محرمانگی

- این پارامتر، ضربه‌ای را که در صورت بهره‌برداری موفق از آسیب‌پذیری سیستم هدف به محرمانگی اطلاعات موجود وارد می‌شود را می‌سنجد و نشان می‌دهد که مهاجم چه سطحی از دسترسی به اطلاعات محرمانه را برروی سیستم هدف پس از حمله خواهد داشت. در تخصیص مقدار به این پارامتر، طبقه‌بندی اطلاعات موجود برروی سیستم اطلاعاتی ملاک نخواهد بود و تنها امکان آن برای مهاجم مورد سنجش قرار می‌گیرد. مقادیر این پارامتر هیچ (None)، قسمتی (Partial) و کامل (Complete) است.

امتیاز Base– شدت فنی آسیب‌پذیری

ضربه به صحت و تمامیت

- این پارامتر ضربه‌ای که به صحت و تمامیت اطلاعات موجود بر سیستم هدف در صورت بهره‌برداری موفق از آسیب‌پذیری وارد می‌شود را می‌سنجد و نشان می‌دهد که مهاجم تا چه حدی امکان می‌یابد به صحت و تمامیت اطلاعات برروی سیستم هدف (بدون توجه به طبقه‌بندی اطلاعات) پس از حمله خدشه وارد کند. مقادیر این پارامتر هیچ، قسمتی و کامل است.

امتیاز Base– شدت فنی آسیب‌پذیری

ضربه به دسترس‌پذیری

- این پارامتر ضربه‌ای که به دسترس‌پذیری اطلاعات موجود بر سیستم هدف در صورت بهره‌برداری موفق از آسیب‌پذیری وارد می‌شود را می‌سنجد و نشان می‌دهد که مهاجم تا چه حدی امکان می‌یابد اطلاعات موجود برروی سیستم هدف را از دسترس خارج نماید. مقادیر این پارامتر هیچ، قسمتی و کامل است.

امتیاز Base– نحوه محاسبه

- در زیر فرمول محاسبه امتیاز Base با توجه به مقادیر تخصیص داده شده به هریک از پارامترها آورده شده است. مقدار بدست آمده برای امتیاز Base عددی بین ۰ تا ۱۰ است که شدت فنی آسیب‌پذیری را نشان می‌هد (عدد ۱۰ بیشترین شدت آسیب‌پذیری است).

- BaseScore6 = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)–1.5)*f*(Impact))
  - Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))
  - Exploitability = 20* AccessVector*AccessComplexity*Authentication
  - *f(impact)= 0 if Impact=0, 1.176 otherwise

امتیاز Base– نحوه محاسبه

AccessVector = case AccessVector of
requires local access: 0.395
adjacent network accessible: 0.646
network accessible: 1.0
AccessComplexity = case AccessComplexity of
high: 0.35
medium: 0.61
low: 0.71
Authentication = case Authentication of
requires multiple instances of authentication: 0.45
requires single instance of authentication: 0.56
requires no authentication: 0.704
ConfImpact = case ConfidentialityImpact of
none: 0.0
partial: 0.275
complete: 0.660
IntegImpact = case IntegrityImpact of
none: 0.0
partial: 0.275
complete: 0.660
AvailImpact = case AvailabilityImpact of
none: 0.0
partial: 0.275
complete: 0.660

- برای تبدیل مقادیر پارامترها به مقادیر عددی که در فرمول فوق قابل اعمال باشد از عبارات زیر کمک گرفته می‌شود.

امتیاز Base– نحوه محاسبه

- در ضمن برای تعیین شدت کیفی آسیب‌پذیری‌ها از ماتریس زیر استفاده شده است.
- در این ماتریس شرحی از سطوح کیفی قابل تخصیص به آسیب‌پذیری‌های یک سیستم اطلاعاتی آورده شده است.

امتیاز Base– نحوه محاسبه

شدت	امتیاز Base	شرح
پایین	۲-۴	این آسیب‌پذیری‌ها ممکن است باعث از بین رفتن، افشاء و یا تغییر برخی اطلاعات محدود و غیر مهم برروی سیستم‌های اطلاعاتی شوند، ولی به مهاجم مستقیماً اجازه ایجاد وقفه در کار سیستم نمی‌دهند. با این حال، آسیب‌پذیری‌هایی از این دست ممکن است در کنار دیگر مشکلات امنیتی، حمله به سیستم اطلاعاتی را تسهیل نمایند.
متوسط	۴-۷	این آسیب‌پذیری‌ها ممکن است باعث از بین رفتن، افشاء و یا تغییر برخی اطلاعات بر روی سیستم اطلاعاتی شوند که با کارکرد آن در ارتباط است. با این‌حال اطلاعات مربوط به سازمان و افراد دست نخورده باقی می‌ماند. بازگرداندن سیستم اطلاعاتی از یک حمله موفق به چنین آسیب‌پذیری ممکن است باعث ایجاد وقفه در سرویس شود.
بالا	۷-۹	این آسیب‌پذیری‌ها ممکن است باعث از بین رفتن، افشاء و یا تغییر اطلاعات حیاتی برروی سیستم اطلاعاتی شوند که مربوط به سازمان و عملیات آن یا افراد مرتبط با سازمان است (از بین رفتن حریم خصوصی). این آسیب‌پذیری‌ها می‌توانند به از بین رفتن کارکرد سیستم و وقفه در سرویس منجر شوند. بازگرداندن سیستم از یک حمله موفق در این حالت نیاز به تلاش زیادی دارد.
بحرانی	۹-۱۰	آسیب‌پذیری‌های از این دست امکان اجرای کد برروی سیستم اطلاعاتی را از راه دور و احتمالا با سطح دسترسی بالا پدید می‌آورند و به مهاجم این امکان را می‌دهند که کنترل کامل سیستم هدف را دردست بگیرد.

جزئیات گزارش آسیب‌پذیری‌ها

گزارش جزئیات آسیب‌پذیری‌های کشف شده در فرمت جدولی که شامل:

- نام میزبان/آدرس IP سیستم آسیب‌پذیر،
- عنوان و شرح مختصری از آسیب‌پذیری،
- مرجع،
- شدت فنی آسیب‌پذیری
- و راه‌حل رفع آسیب‌پذیری ارائه میگردد.

- Technical Impact

جزئیات گزارش آسیب‌پذیری‌ها

جزئیات گزارش آسیب‌پذیری‌ها

- آیتم‌های قالب گزارش هر آسیب‌پذیری به شرح زیر است:
- Host Name: نام سرویس دهنده یا تجهیزات شبکه دارای آسیب‌پذیری
- Vuln. Title: عنوان آسیب‌پذیری کشف شده
- Reference (CVE/BID): مراجعی که برای آسیب‌پذیری در دسترس می‌باشند نظیر شماره CVE و BID در این قسمت بیان می‌گردد.
- Port/Service: در این بخش سرویس آسیب‌پذیر و پورت مربوط به آن آورده می شود.

جزئیات گزارش آسیب‌پذیری‌ها

- Description: توصیف کلی آسیب‌پذیری، جزئیات چگونگی کشف و اعتبار سنجی آن و عواقب ناشی از بهره‌برداری از آسیب‌پذیری، نسخه‌های آسیب‌پذیر نرم‌افزار مربوطه، مشکلات پیکربندی منجر به آسیب‌پذیری بطور خلاصه در این قسمت آورده می‌شود.
- Treatment(s): این قسمت از گزارش آسیب‌پذیری به ارائه راهکارهایی برای رفع مشکل اختصاص دارد که شامل وصله‌های ارائه شده از طرف سازندگان، اصلاح تنظیمات پیکربندی، ارتقاء به نسخه‌های امن و نکات دیگر می‌باشد.
- CVSS Base-Score: در این آیتم امتیاز آسیب‌پذیری کشف‌شده از دو جنبه ضربه فنی و قابلیت بهره‌برداری محاسبه می‌شود. مبنای این امتیاز دهی متدولوژی CVSS است که به هر آسیب‌پذیری بطور مستقل از کارکرد سیستم میزبان و نقش آن در کسب‌وکار می‌پردازد.

جزئیات گزارش آسیب‌پذیری‌ها

- CVSS Vector: مقادیر پارامترهای Base Score را نشان می‌دهد که امتیاز پایه از روی آن محاسبه شده است. محاسبه ضربه فنی در امتیاز Base Score، اثر آسیب‌پذیری را بر محرمانگی (C)، صحت (I) و دسترس‌پذیری (A) میزبانی که آسیب‌پذیری برروی آن قرار دارد درنظر می‌گیرد.
- عبارات داخل پرانتز اختصارات هستند که در نمایش بردار CVSS مورد استفاده قرار می‌گیرند.
- از طرف دیگر، قابلیت بهره‌برداری آن جنبه‌ای از آسیب‌پذیری را نشان می‌دهد که مشخص می‌کند مهاجم تا چه میزان امکان سوءاستفاده از آسیب‌پذیری را خواهد داشت.
- محاسبه قابلیت بهره‌برداری با سه پارامتر بردار دسترسی (AV)، سطح احراز هویت لازم (AU) و پیچیدگی دسترسی (AC) بیان می‌شود. مجددا مقادیر داخل پرانتز اختصارات مورد استفاده در نمایش بردار CVSS هستند.

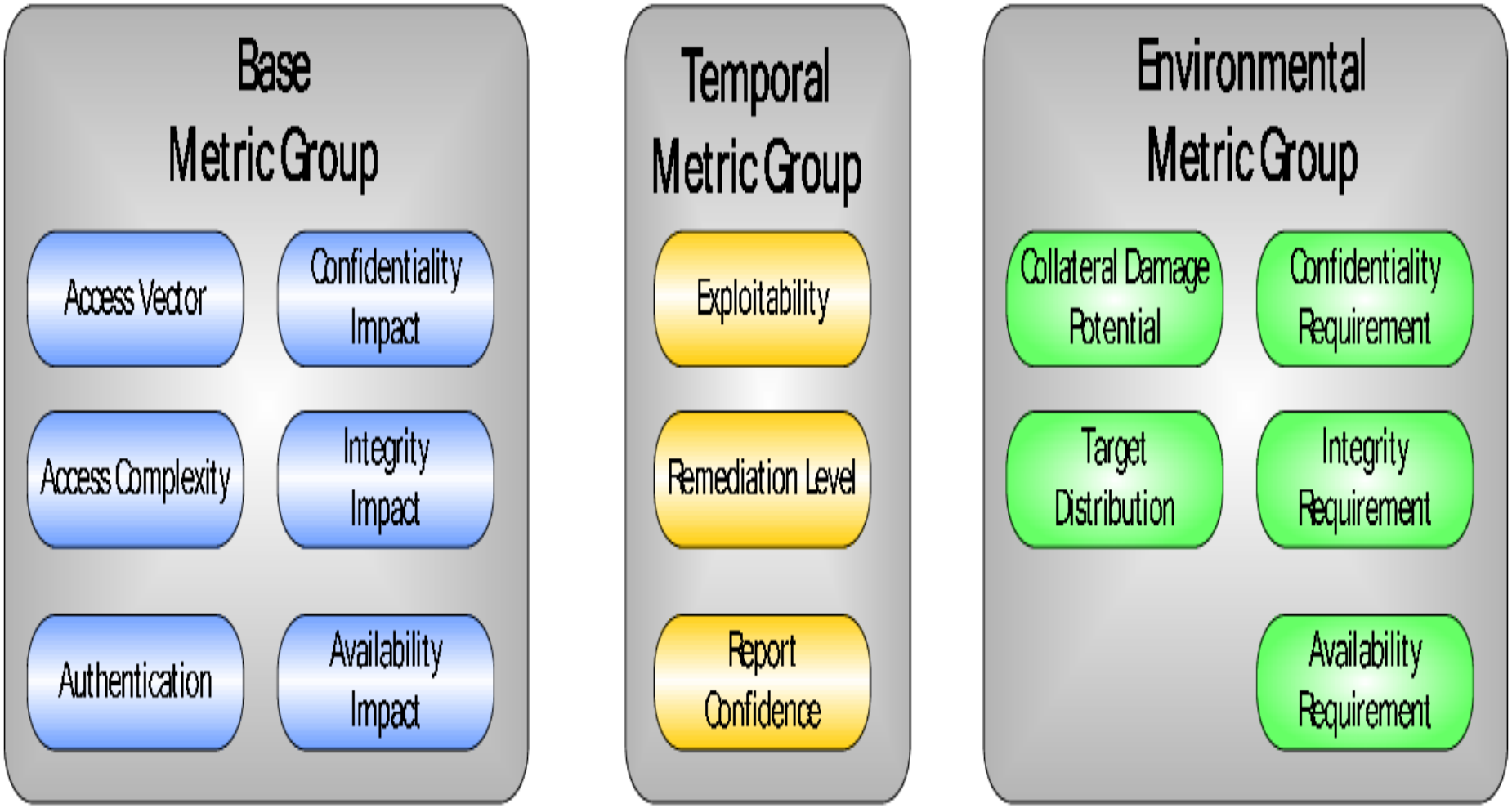
جزئیات گزارش آسیب‌پذیری‌ها

- در خصوص ضربه هریک از پارامترهای محرمانگی، صحت و دسترس‌پذیری مقادیر کمی و گسسته‌ی None، Partial و Complete را می‌توانند داشته باشند.
- برای نمایش آنها در بردار به ترتیب از N، P و C استفاده می‌شود.
- برای قابلیت بهره‌برداری نیز اختصارات بصورت زیر است:
  - بردار دسترسی می‌تواند Local (L)، Adjacent Network (A) و Network (N) باشد.
  - احراز هویت می‌تواند None (N)، Single (S) و Multiple (M) باشد.
  - سطح پیچیدگی نیز یکی از مقادیر High (H)، Medium (M) و Low (L) را می‌تواند داشته باشد.

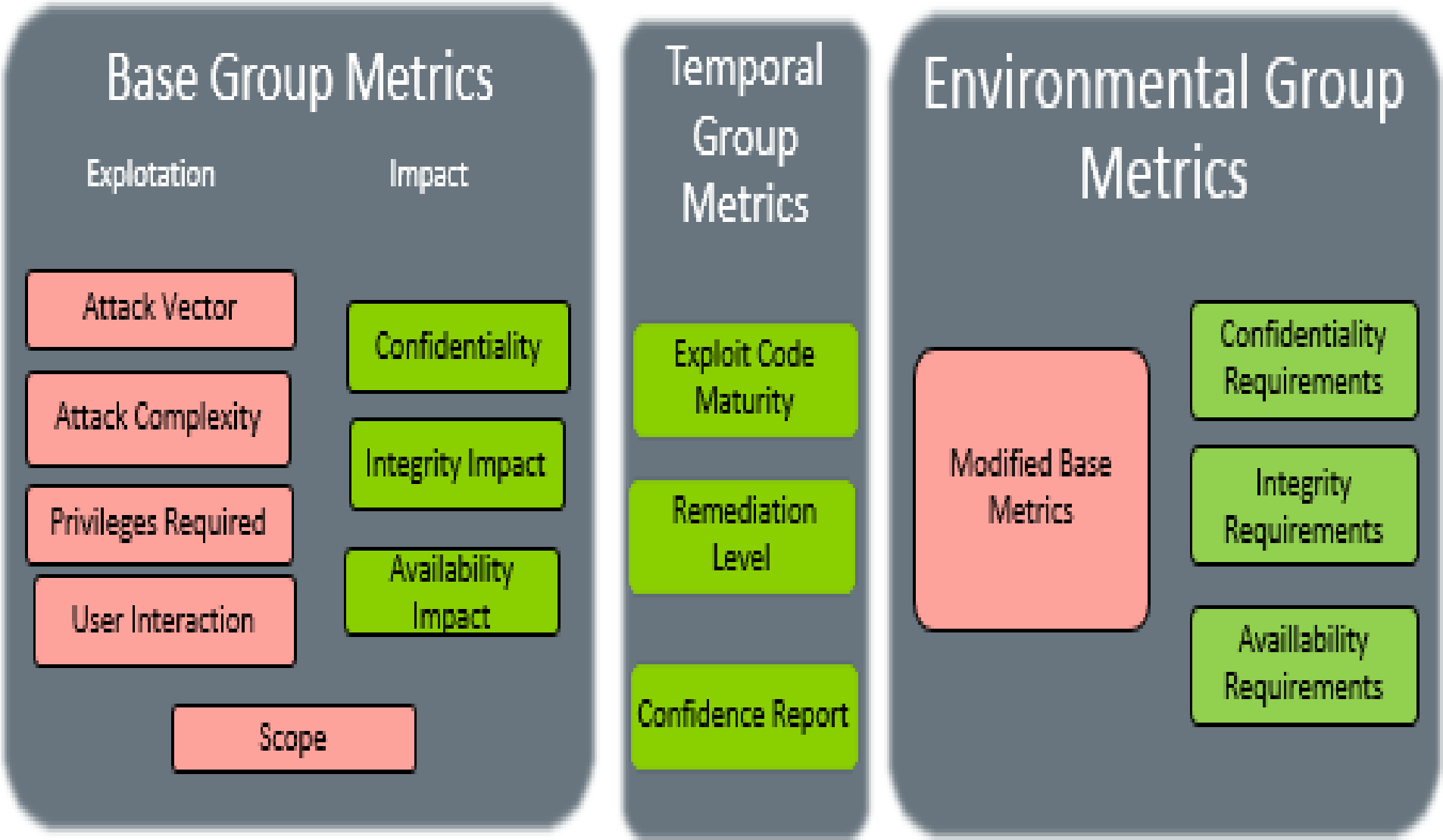
جزئیات گزارش آسیب‌پذیری‌ها

- Exploitability in the context: براساس اطلاعات بدست آمده از پیکربندی شبکه و سطوح دسترسی موجود مشخص می‌کند که آسیب‌پذیری از چه بخشی قابل بهره‌برداری است.
- Exploitability

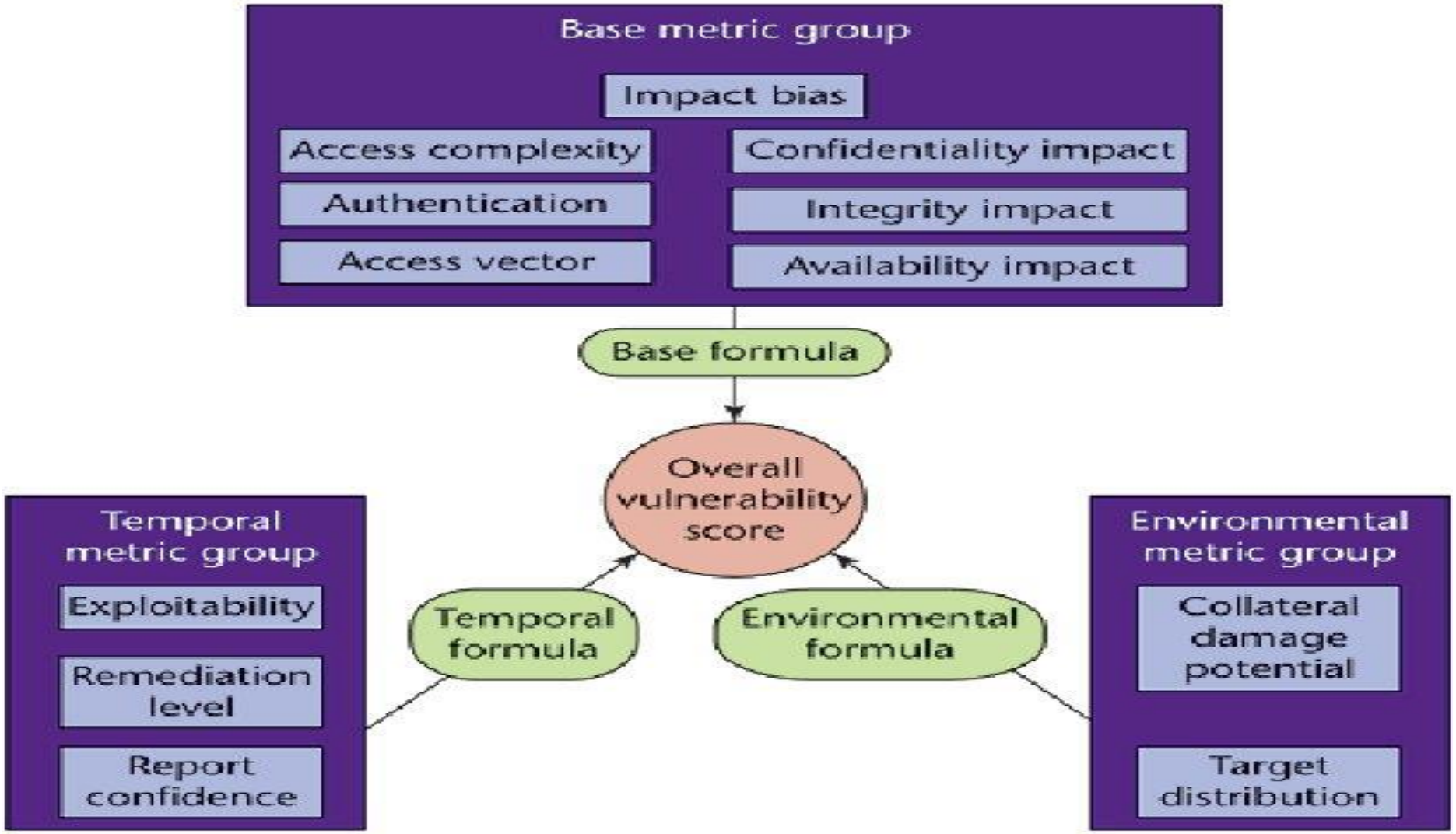
Metrics Groups



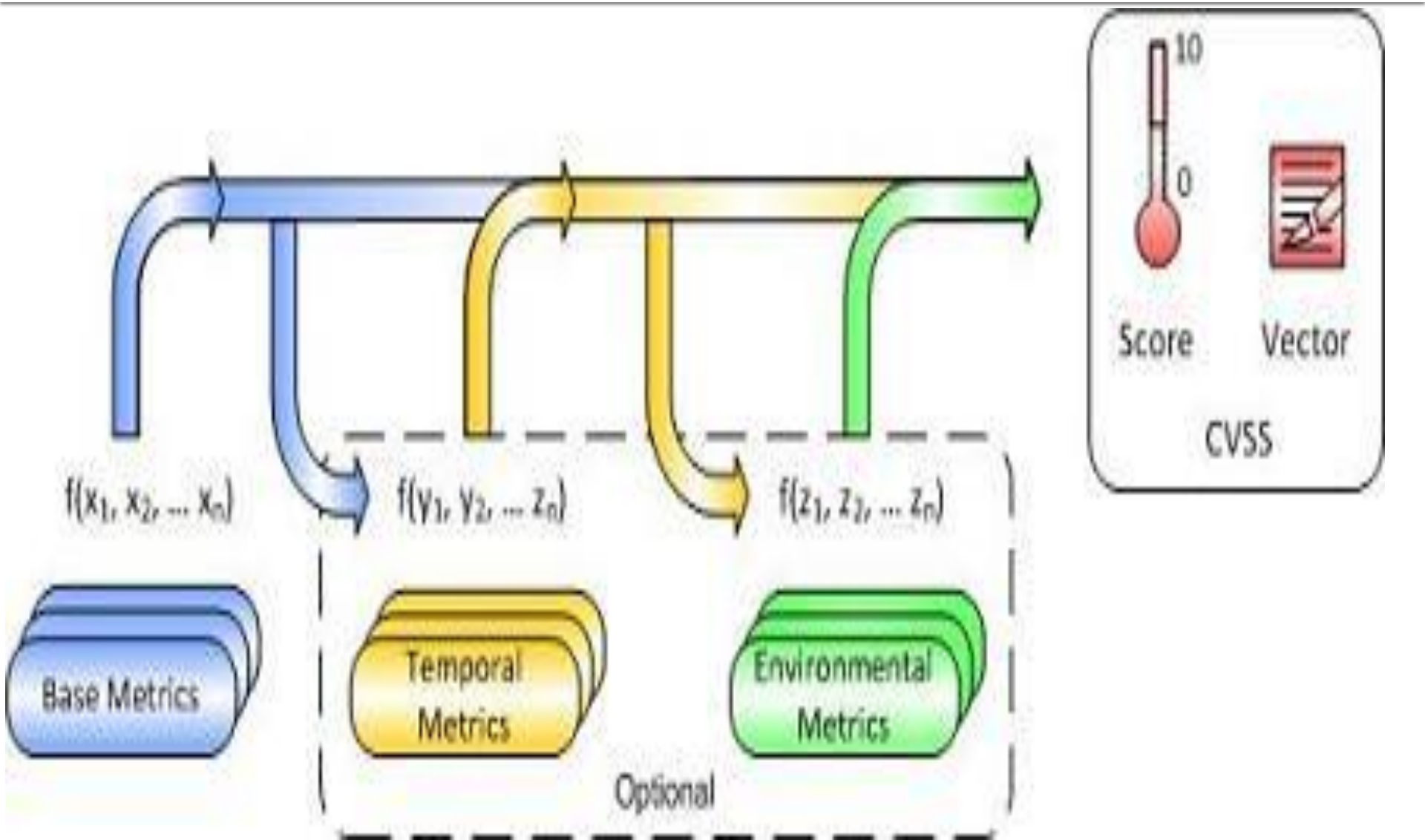
Metrics Groups



Overall Vulnerability Score



CVSS Score

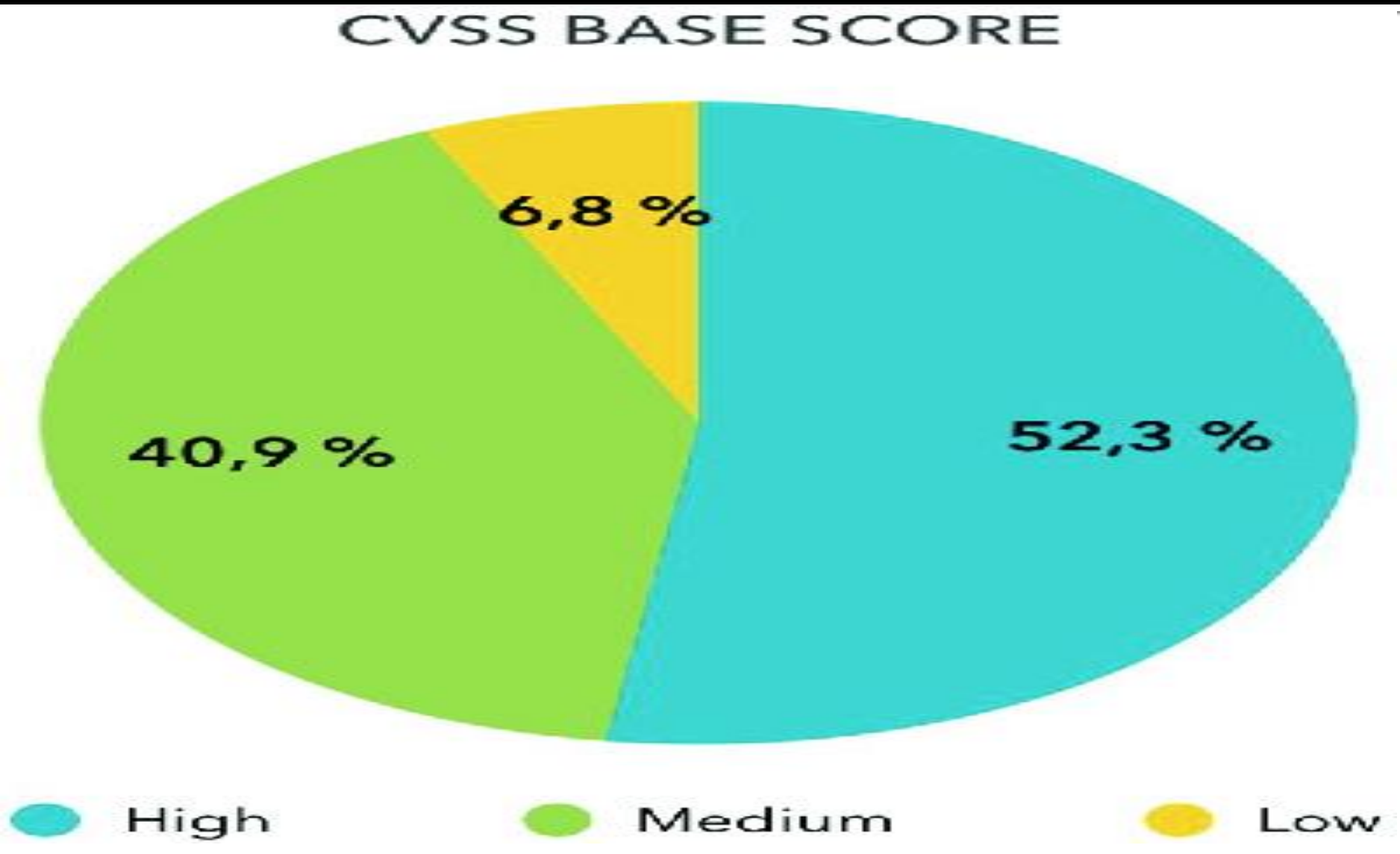

10
0
Score
Vector
CVSS
f(x1, x2, ... xn)
f(y1, y2, ... zn)
f(z1, z2, ... zn)
Base Metrics
Temporal Metrics
Environmental Metrics
Optional

CVSS V2 and V3

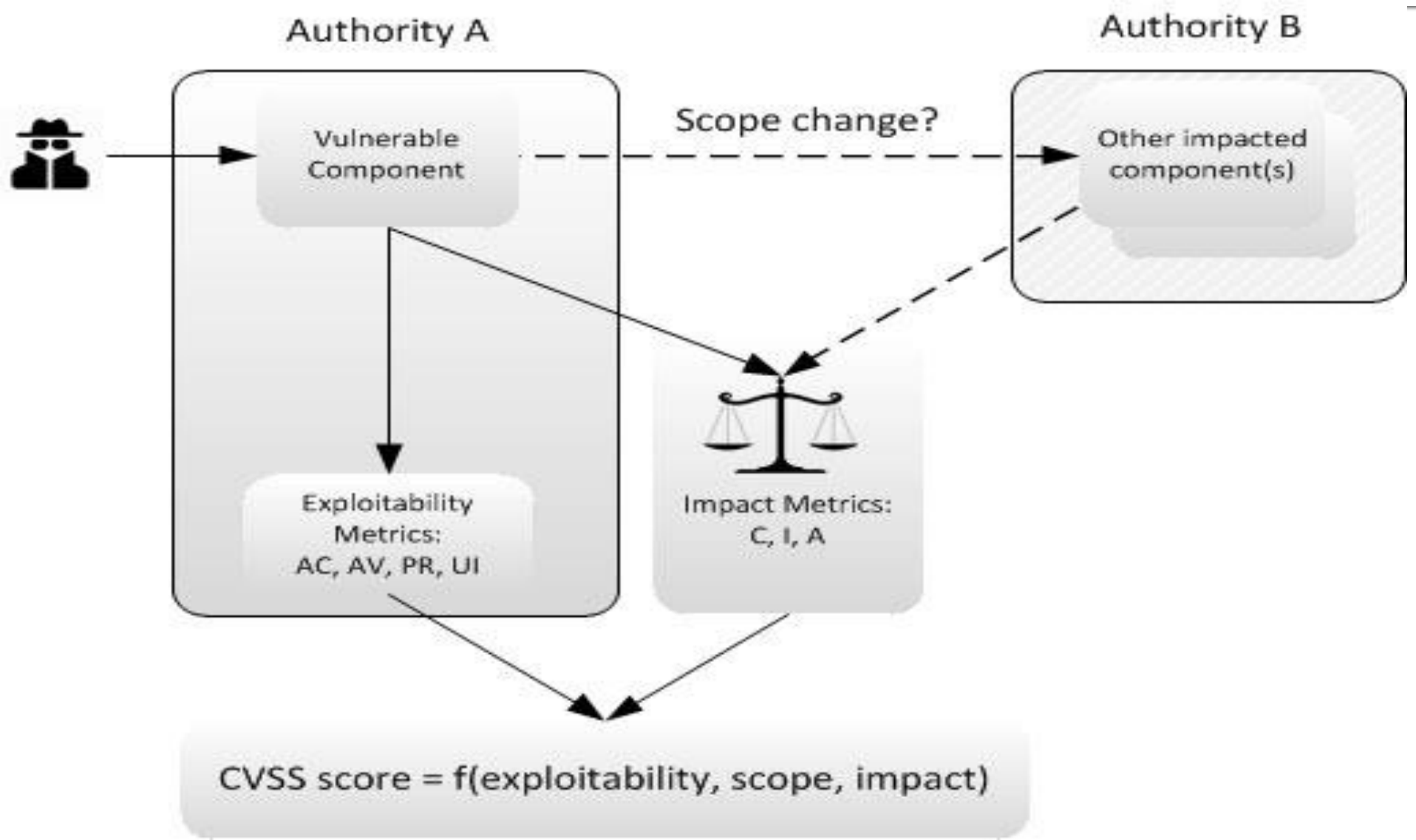
Categories of CVSS v2.0

Categories of CVSS v3.0

CVSS Base Score

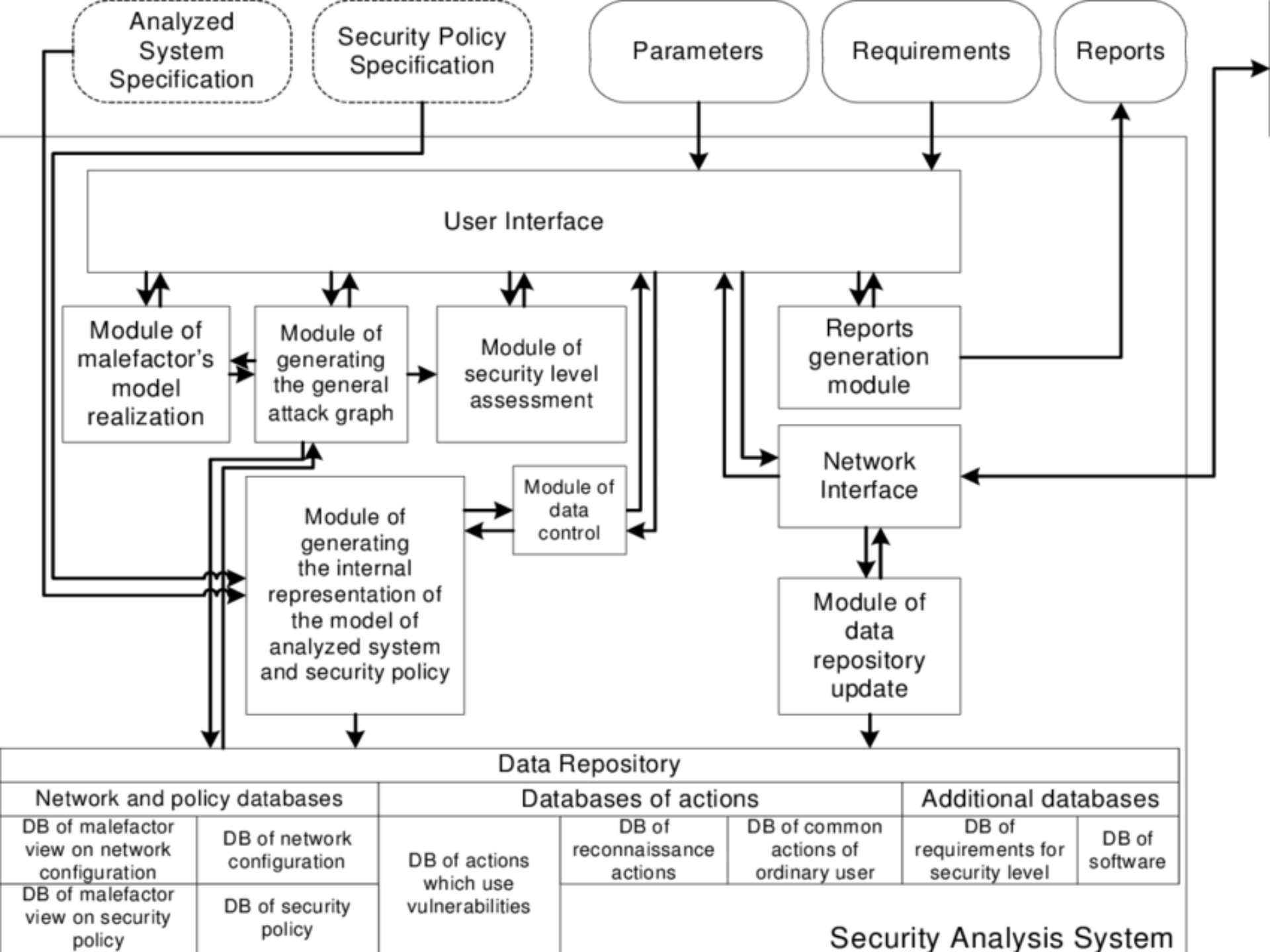


CVSS Score

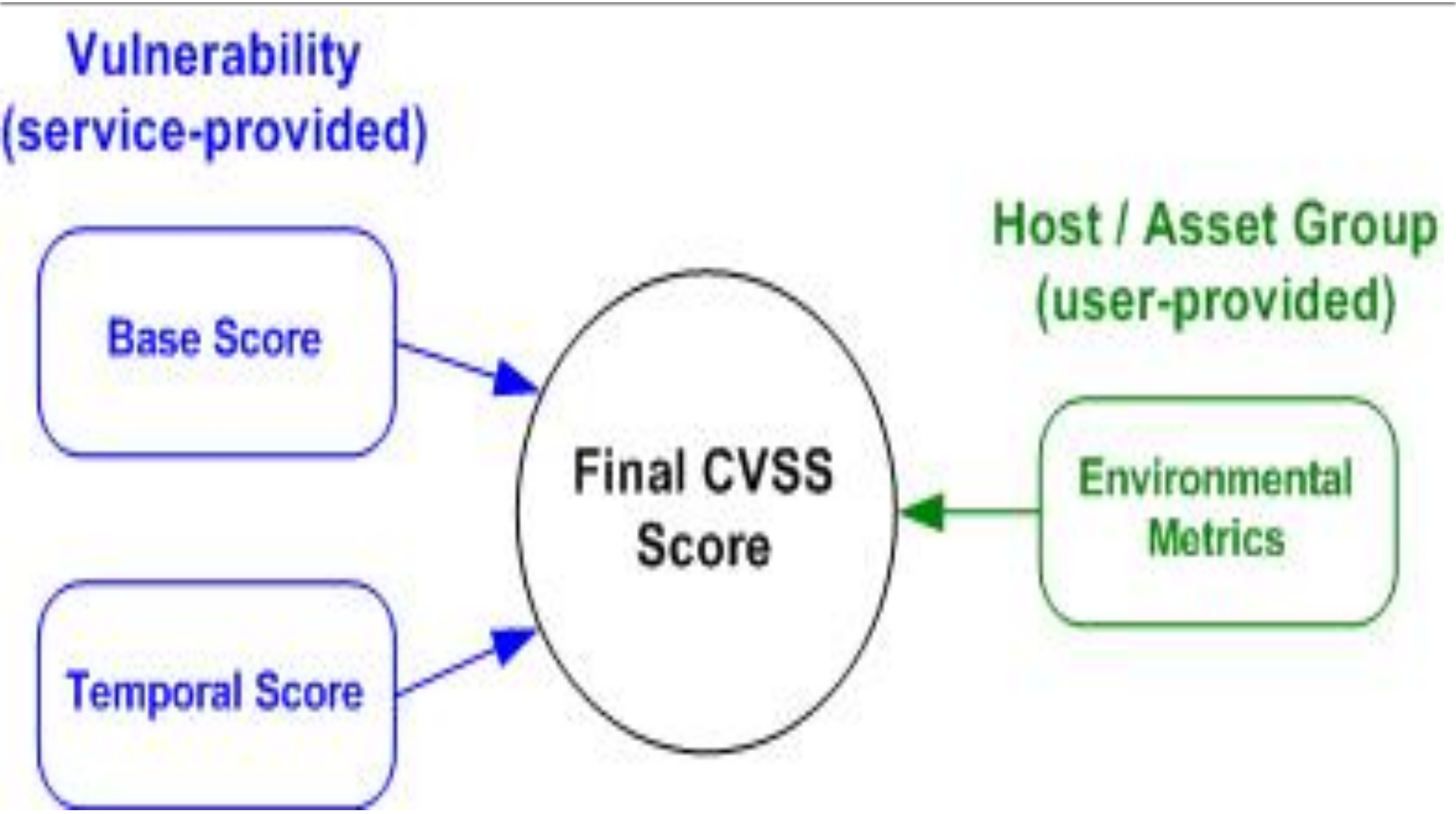

Authority A
Authority B
Vulnerable Component
Scope change?
Other impacted component(s)
Exploitability Metrics: AC, AV, PR, UI
Impact Metrics: C, I, A
CVSS score = f(exploitability, scope, impact)

CVSS Example

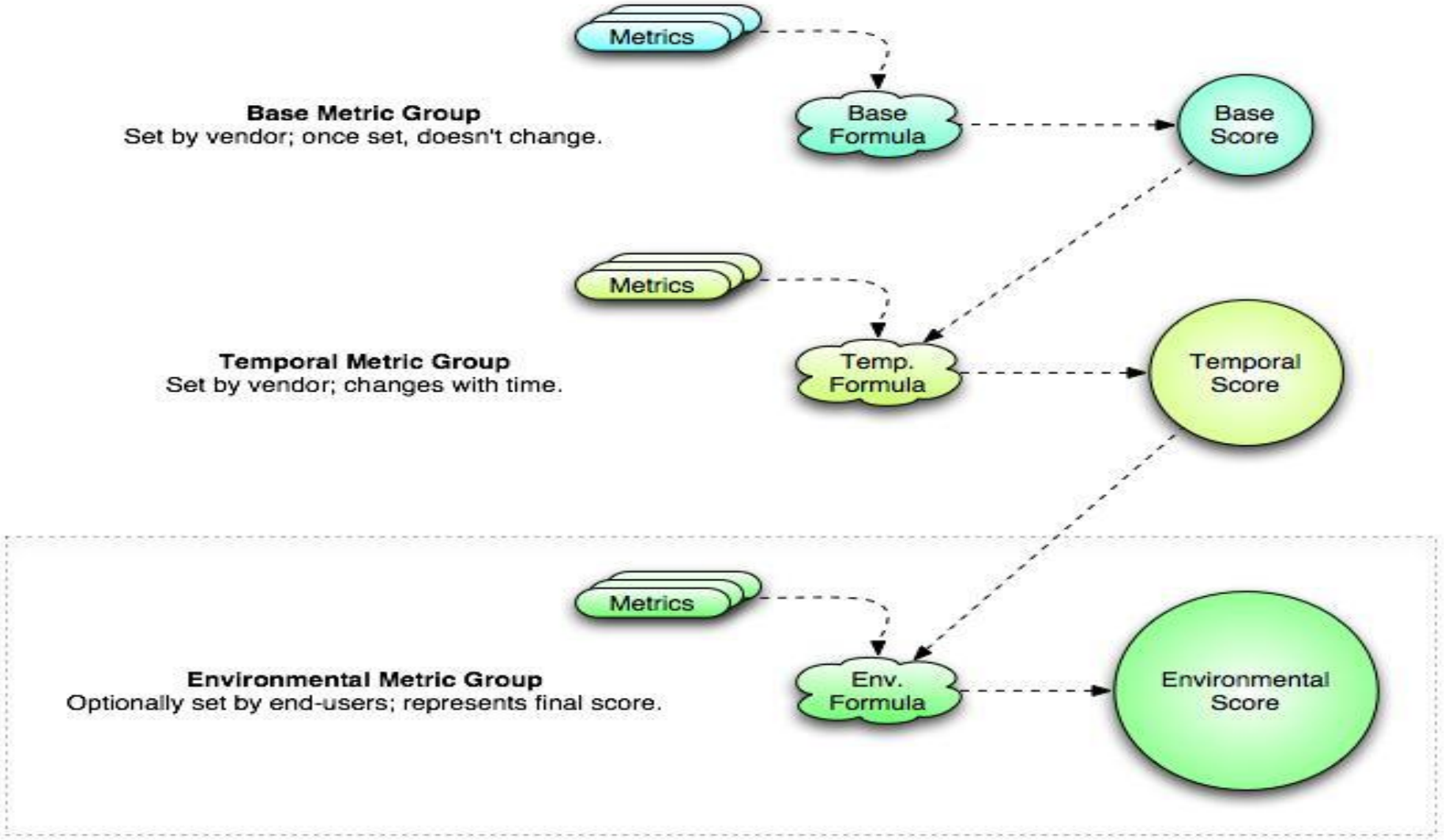
CVSS V3 Score METRICS		NetCAT CVE-2019-11184
Attack Vector	AV	**Adjacent**
Attack Complexity	AC	High
Privileges required	PR	Low
User Interaction	UI	Required
Scope	S	Changed
Confidentiality	C	Low
Integrity	I	None
Availability	A	None
Base Score		**2.6 (Low)**


Analyzed System Specification
Security Policy Specification
Parameters
Requirements
Reports
User Interface
Module of malefactor's model realization
Module of generating the general attack graph
Module of security level assessment
Reports generation module
Network Interface
Module of data control
Module of generating the internal representation of the model of analyzed system and security policy
Module of data repository update
Data Repository
Network and policy databases
DB of malefactor view on network configuration
DB of network configuration
DB of malefactor view on security policy
DB of security policy
Databases of actions
DB of actions which use vulnerabilities
DB of reconnaissance actions
DB of common actions of ordinary user
Additional databases
DB of requirements for security level
DB of software
Security Analysis System

Vulnerability Providers

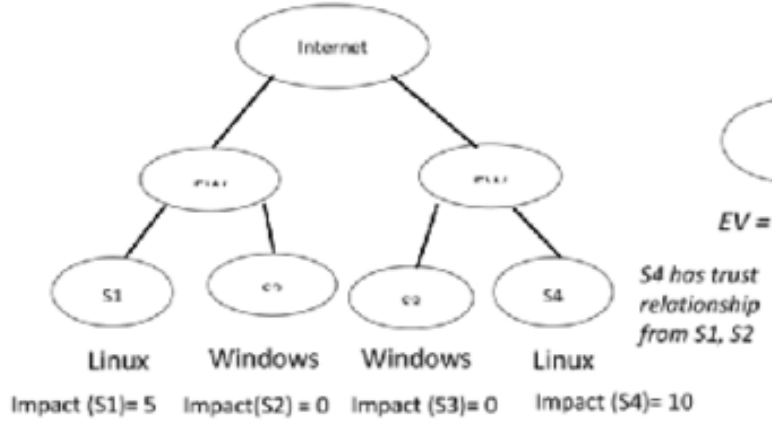


Metrics Process

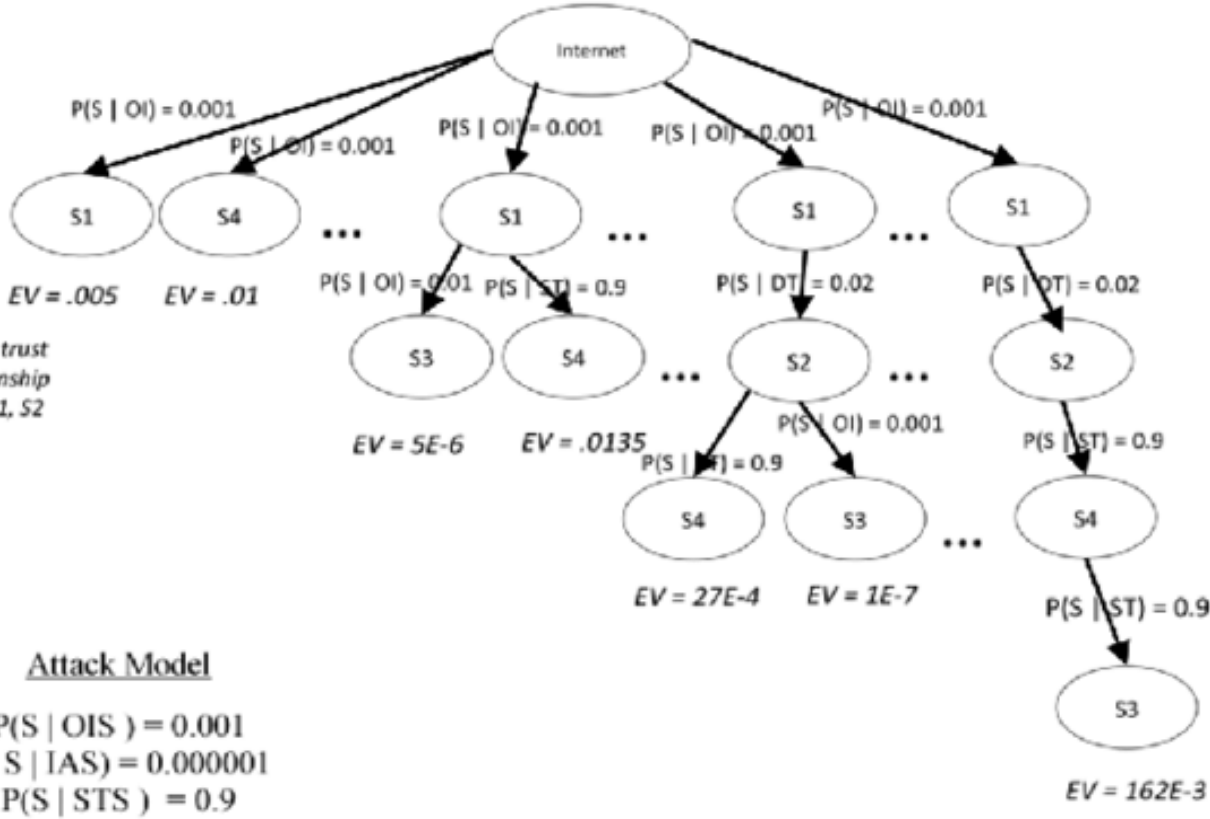


Attack Tress

System Topology



Attack Tree



Mission Impacts

Impact(S1,S2) = 5
Impact(S1,S3) = 5
Impact(S1,S4) = 15
Impact(S2,S3) = 0
Impact(S2, S4) = 10

} Independent additive impacts

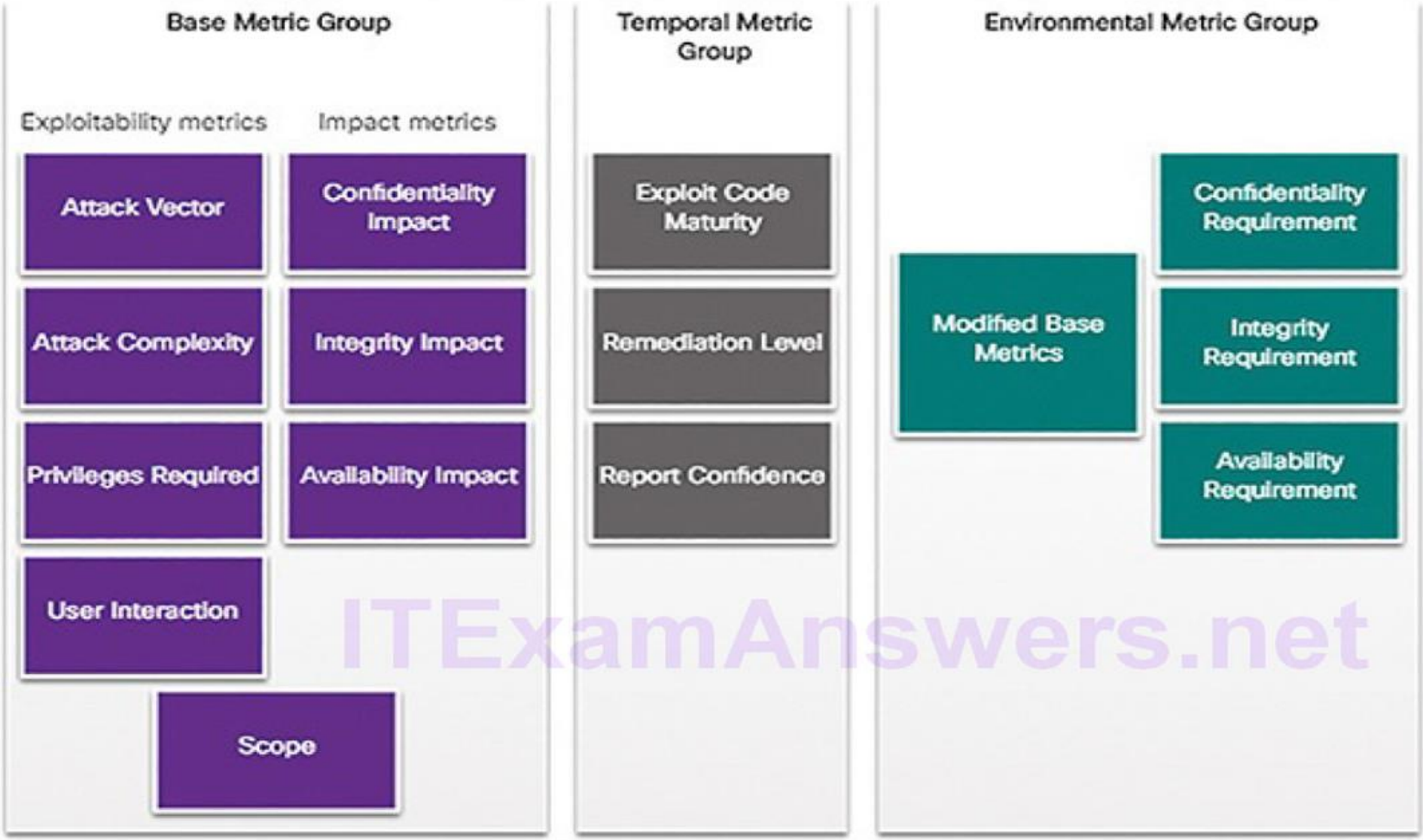
Impact(S3,S4) = 50
Impact(S1,S2,S3,S4) = 1000

} Dependent impacts

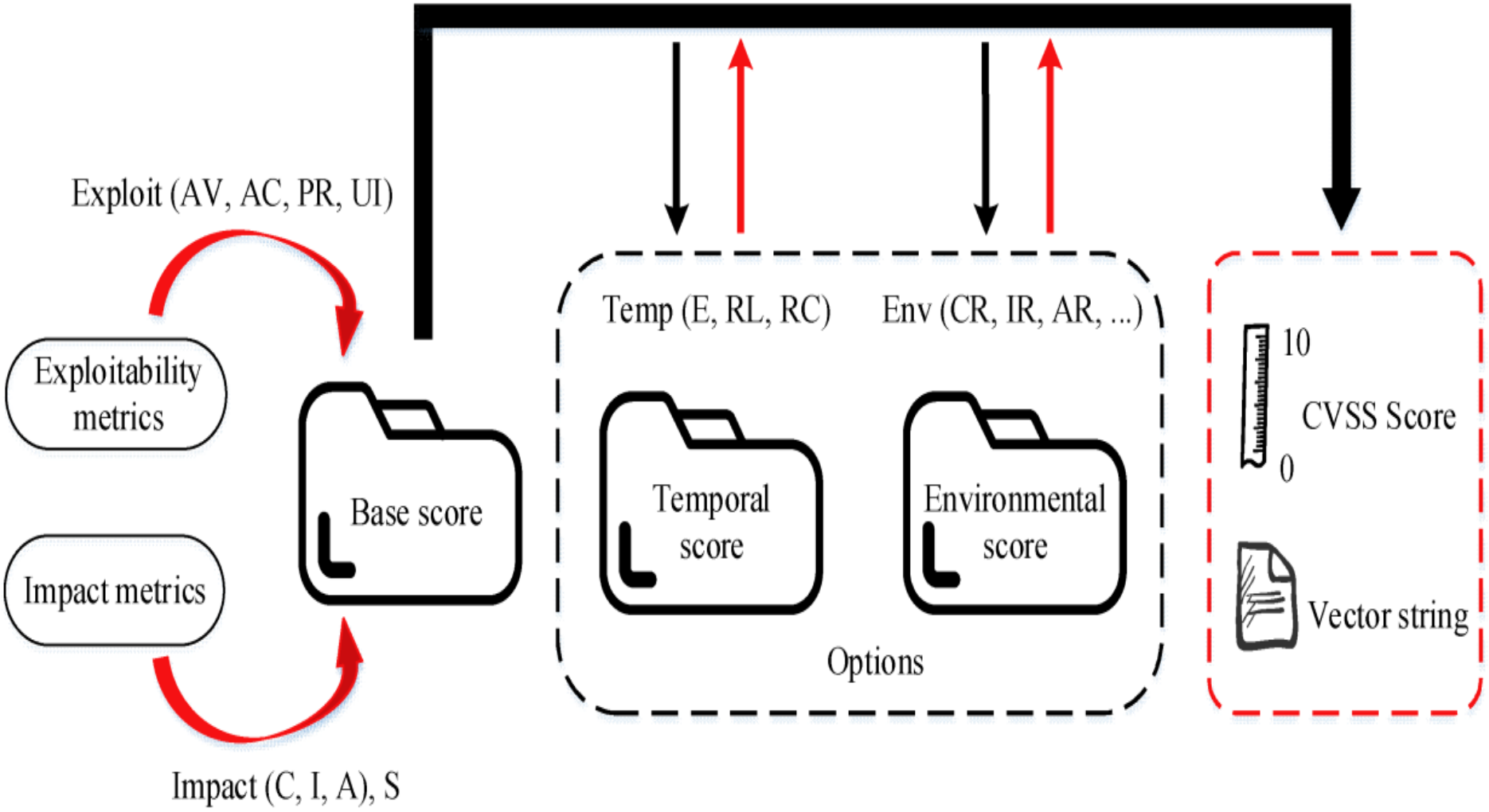
Attack Model

$P(S \mid OIS) = 0.001$
$P(S \mid IAS) = 0.000001$
$P(S \mid STS) = 0.9$
$P(S \mid DTS) = 0.02$

CVSS Metrics



CVSS Vestors



CVSS Metrics

Grupo de Métricas	Métrica	Valores Posibles	Obligatorio
Base	Attack Vector, **AV**	**[N,A,L,P]**	Yes
	Attack Complexity, **AC**	**[L,H]**	Yes
	Privileges Required, **PR**	**[N,L,H]**	Yes
	User Interaction, **UI**	**[N,R]**	Yes
	Scope, **S**	**[C,U]**	Yes
	Confidentiality, **C**	**[H,L,N]**	Yes
	Integrity, **I**	**[H,L,N]**	Yes
	Availability, **A**	**[H,L,N]**	Yes
Temporal	Exploit Code Maturity, **E**	**[X,H,F,P,U]**	No
	Remediation Level, **RL**	**[X,U,W,T,O]**	No
	Report Confidence, **RC**	**[X,C,R,U]**	No
Environmental	Confidentiality Req., **CR**	**[X,H,M,L]**	No
	Integrity Req., **IR**	**[X,H,M,L]**	No
	Availability Req., **AR**	**[X,H,M,L]**	No
	Modified Attack Vector, **MAV**	**[X,N,A,L,P]**	No
	Modified Attack Complexity, **MAC**	**[X,L,H]**	No
	Modified Privileges Required, **MPR**	**[X,N,L,H]**	No
	Modified User Interaction, **MUI**	**[X,N,R]**	No
	Modified Scope, **MS**	**[X,U,C]**	No
	Modified Confidentiality, **MC**	**[X,N,L,H]**	No
	Modified Integrity, **MI**	**[X,N,L,H]**	No
	Modified Availability, **MA**	**[X,N,L,H]**	No

Distribution of Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	32	0.50
1-2	54	0.80
2-3	223	3.50
3-4	307	4.80
4-5	1368	21.30
5-6	1006	15.70
6-7	1055	16.50
7-8	1141	17.80
8-9	46	0.70
9-10	1180	18.40
Total	6412	

Weighted Average CVSS Score: **6.8**

PCI DSS CVSS Scores

CVSS Score	Severity Level	Scan Results
0.0–3.9	Low	Pass
4.0–5.9	Medium	Fail
6.0–9.9	High	Fail
10	Critical	Fail

Source: PCI DSS Quick Reference Guide

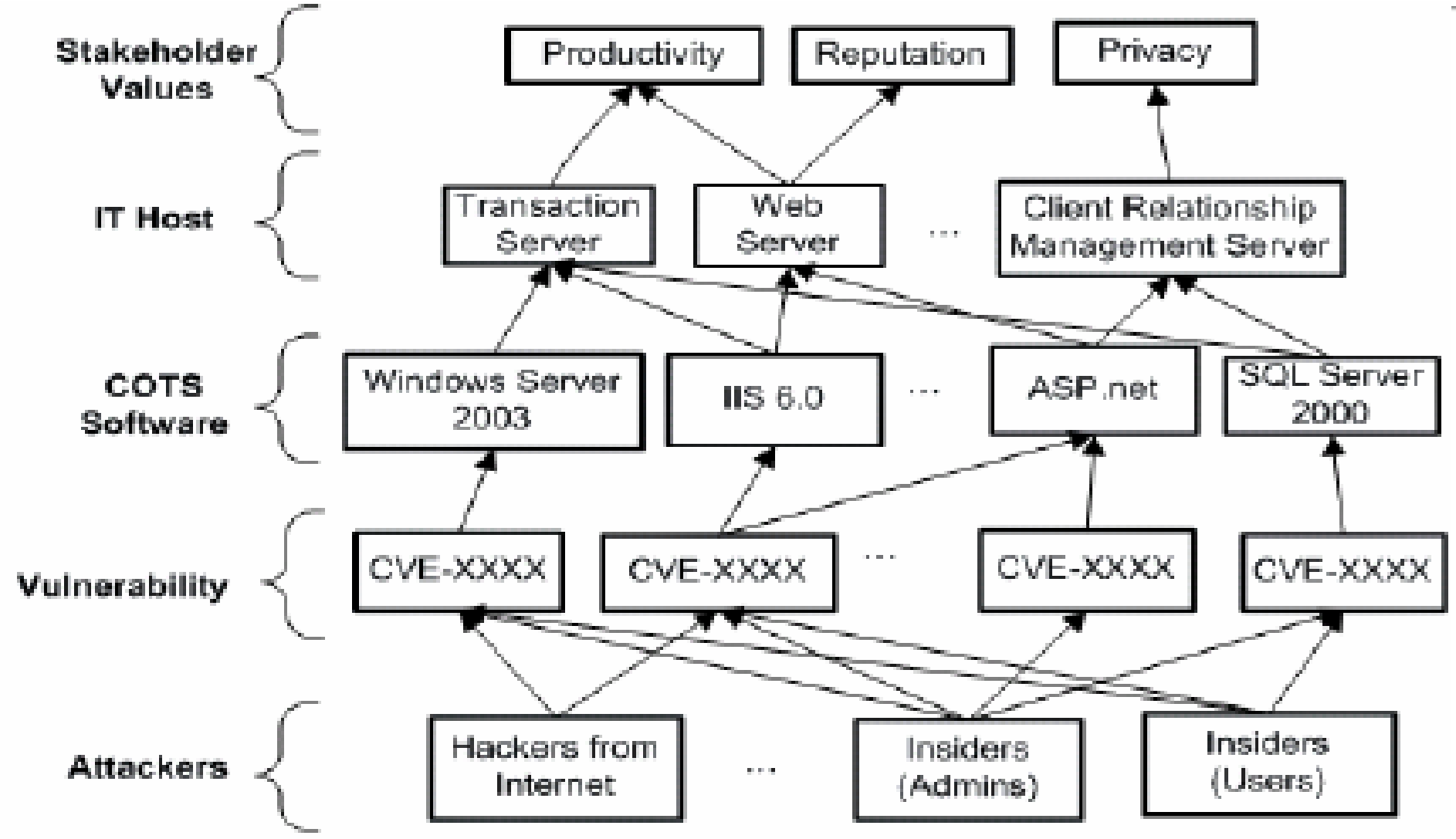
QM	CVSSv2	CVSSv3	Change
Critical	941	687	↓
High	671	1755	↑
Medium	1944	1311	↓
Low	306	109	↓

ATTACK VECTOR	ATTACK COMPLEXITY	PRIVILEGES REQUIRED	USER INTERACTION
Network	Low	None	None
Adjacent	High	Low	Required
Local		High	
Physical			

CVSS v3.1

SCOPE	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Changed	High	High	High
Unchanged	Low	Low	Low
	None	None	None

SEVERITY · SCORE · VECTOR		
Medium	5.4	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:H


Stakeholder Values
IT Host
COTS Software
Vulnerability
Attackers
Productivity
Reputation
Privacy
Transaction Server
Web Server
...
Client Relationship Management Server
Windows Server 2003
IIS 6.0
...
ASP.net
SQL Server 2000
CVE-XXXX
CVE-XXXX
...
CVE-XXXX
CVE-XXXX
Hackers from Internet
...
Insiders (Admins)
Insiders (Users)

CVSS v3.0 - Base Score Metrics

Exploitability Metrics

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope

Scope (S)

Changed (C) | Unchanged (U)

Impact Metrics

Confidentiality Impact (C)

High (H) | Low (L) | None (N)

Integrity Impact (I)

High (H) | Low (L) | None (N)

Availability Impact (A)

High (H) | Low (L) | None (N)

Top 25 Remediations by Risk with Details

April 26, 2018 15:38:32

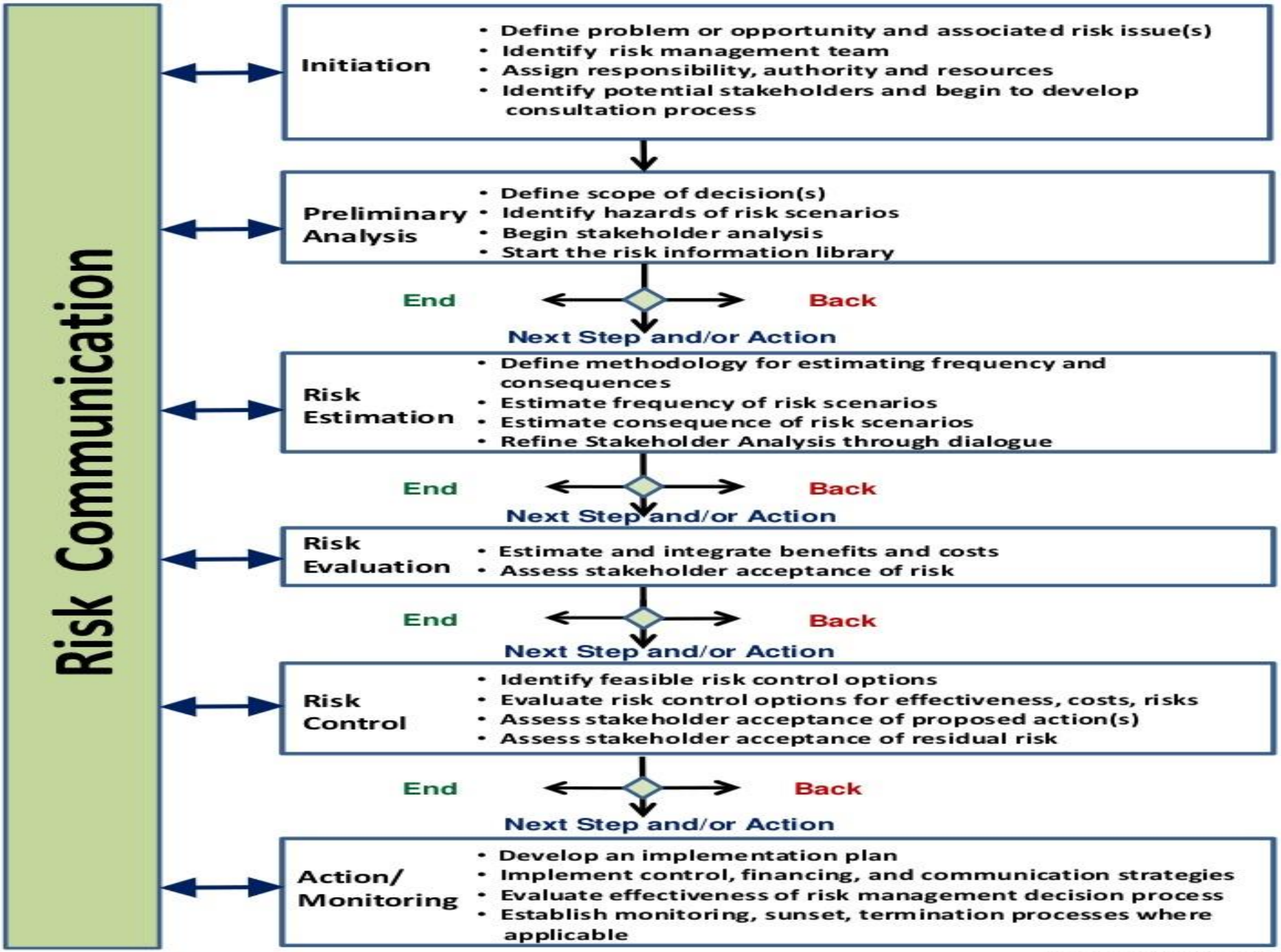
Top Remediations with Details

Applying
25
Top Remediations

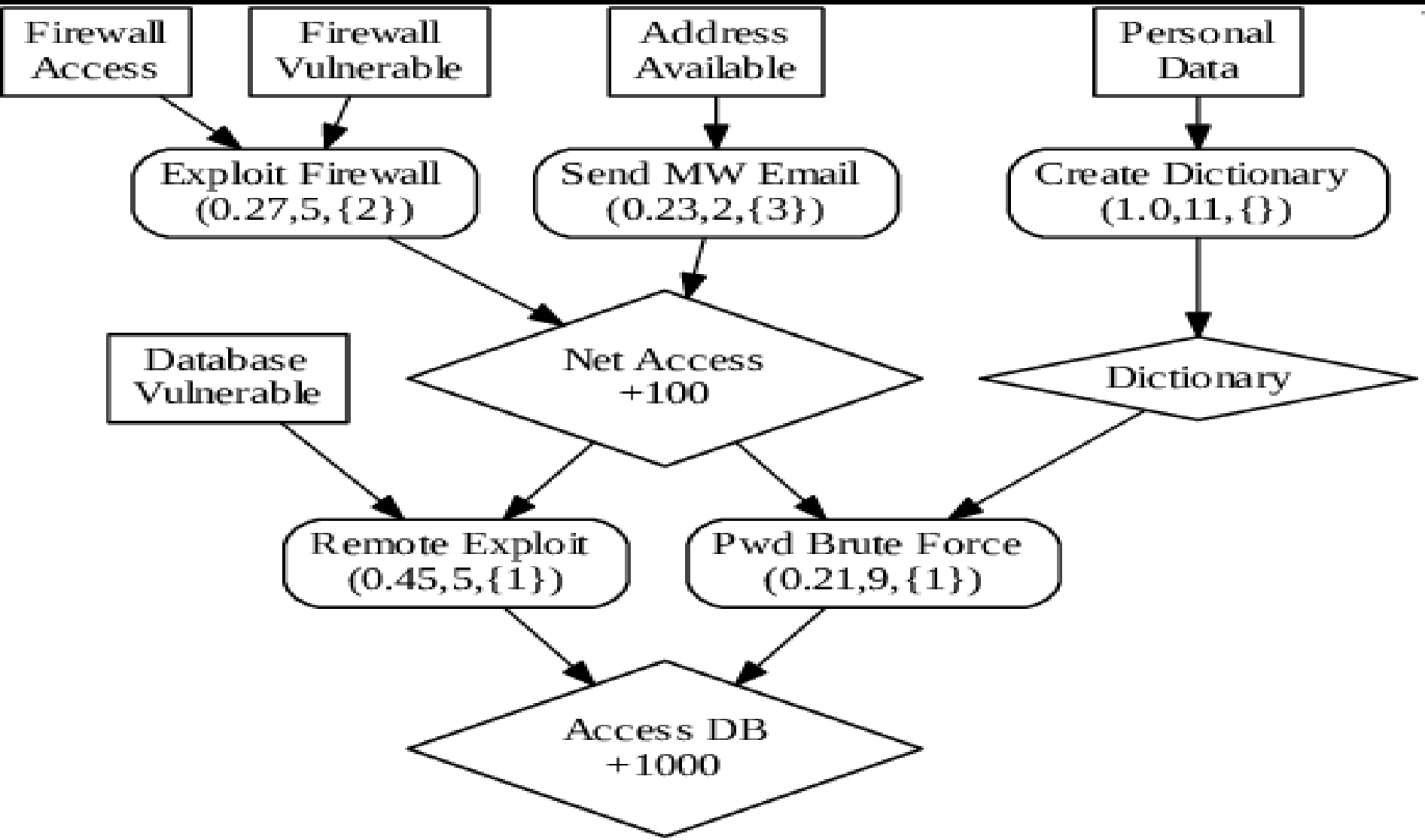
Will Remediate
71%
Vulnerabilities
including:
36% published exploits
20% available malware kits

Affecting
9
Assets

Remediations	Remediated Vulns			Affected Assets	Risk
Upgrade to the latest version of PHP	168	13	0	2	67688
Upgrade to the latest version of Mozilla Firefox	97	0	0	1	44016
Upgrade to the latest version of Mozilla Firefox ESR	60	0	0	1	27665
Upgrade to the latest version of Oracle MySQL	54	3	0	1	11791
Upgrade to the latest version of Google Chrome	21	0	0	1	9423
Upgrade to the latest version of Apache HTTPD	31	3	0	2	7568
Upgrade to the latest version of PostgreSQL	21	0	0	1	5698
Upgrade to Samba 3.0.33	9	8	0	1	5454
Enable authorization for linux single user mode	6	0	0	6	5176

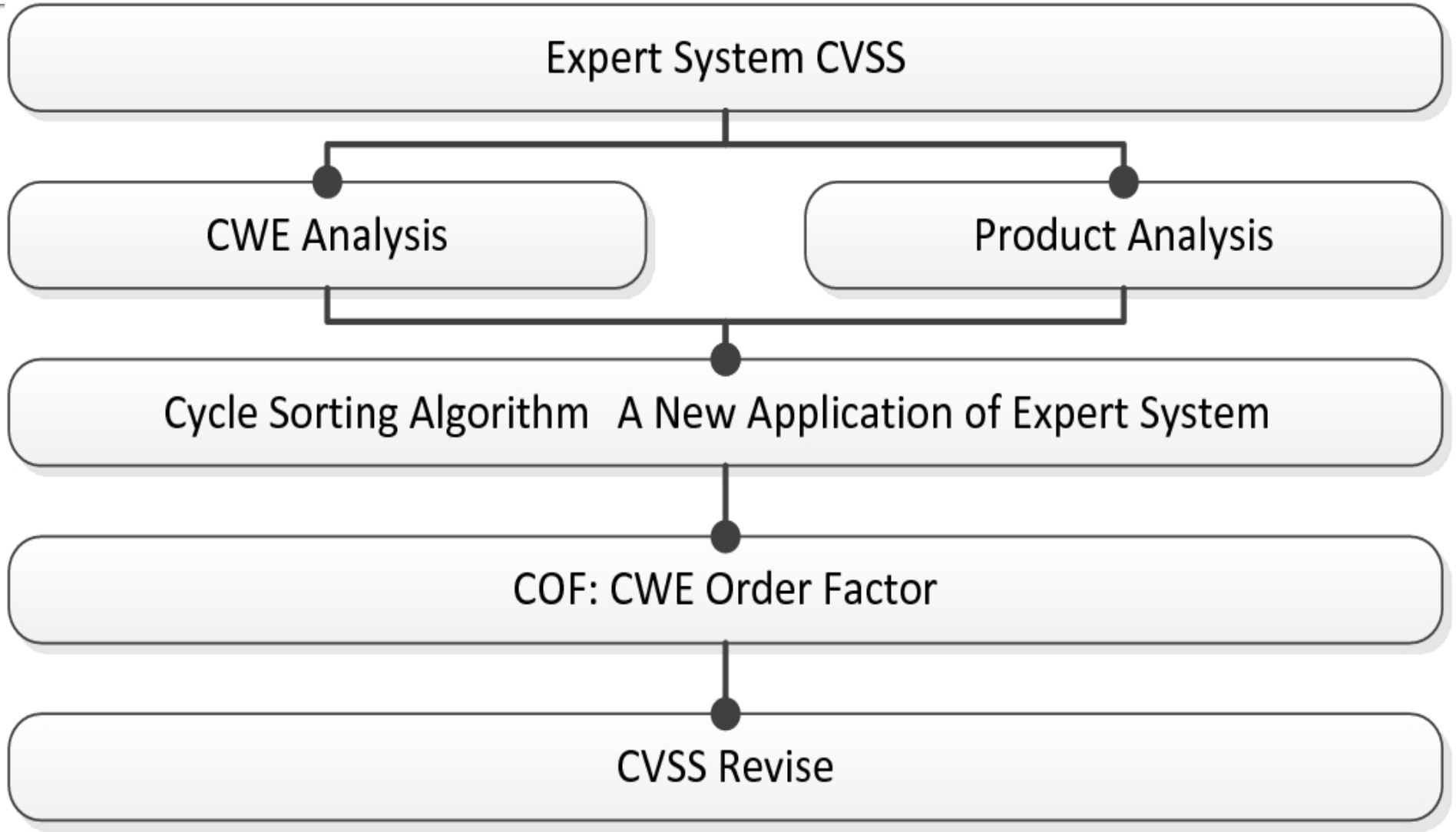


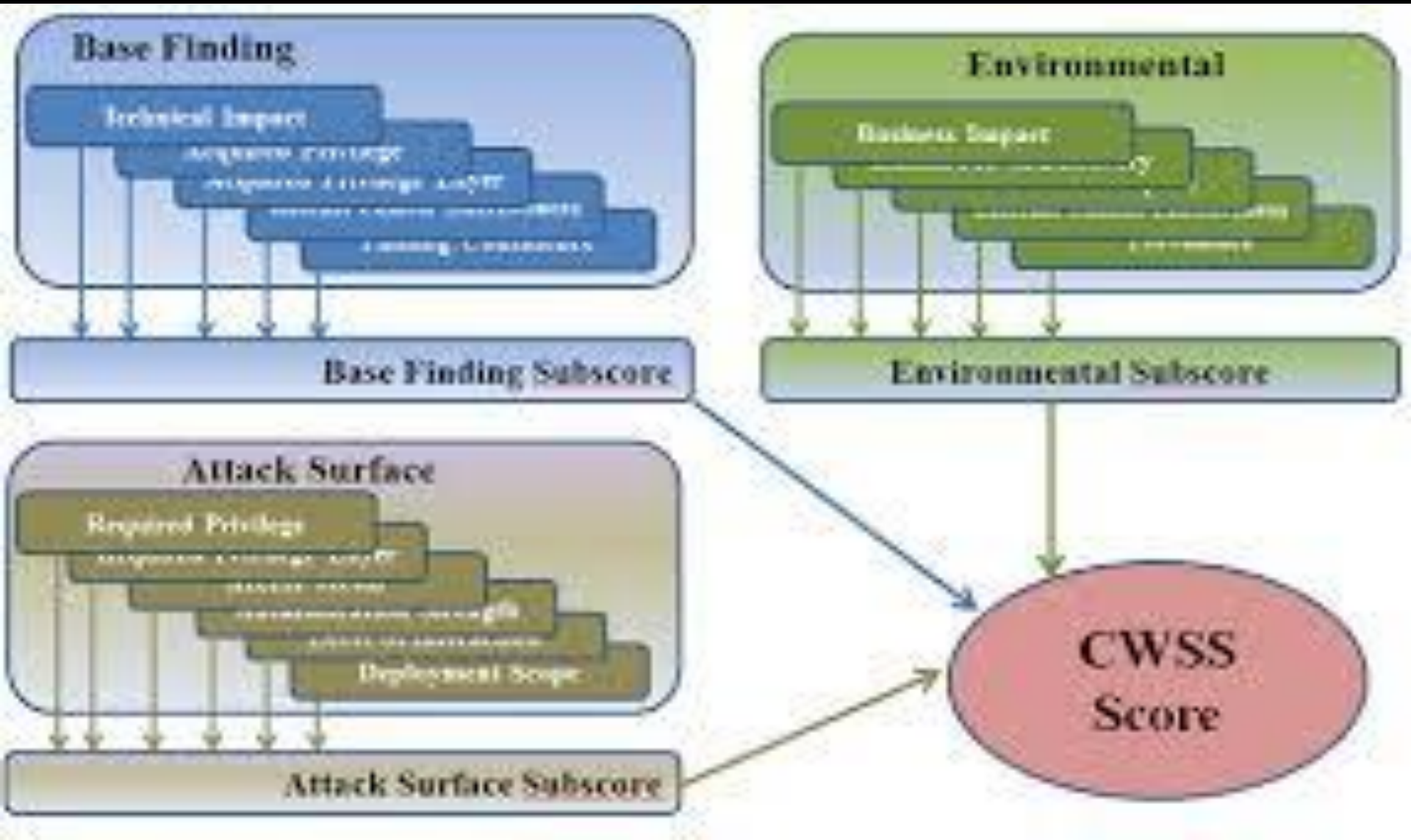
Source: CSA (1997)

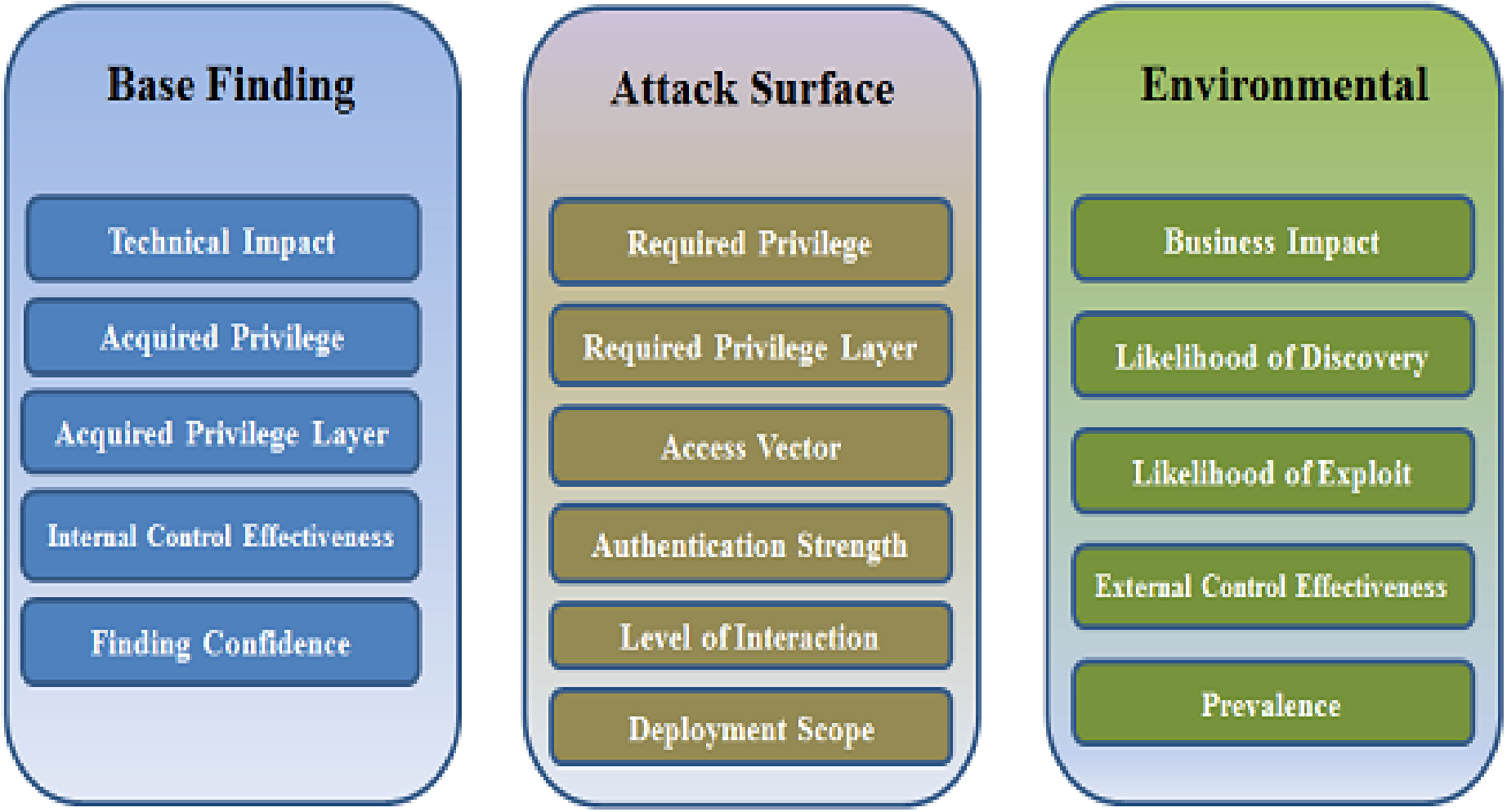

Firewall Access
Firewall Vulnerable
Address Available
Personal Data
Exploit Firewall (0.27,5,{2})
Send MW Email (0.23,2,{3})
Create Dictionary (1.0,11,{})
Database Vulnerable
Net Access +100
Dictionary
Remote Exploit (0.45,5,{1})
Pwd Brute Force (0.21,9,{1})
Access DB +1000

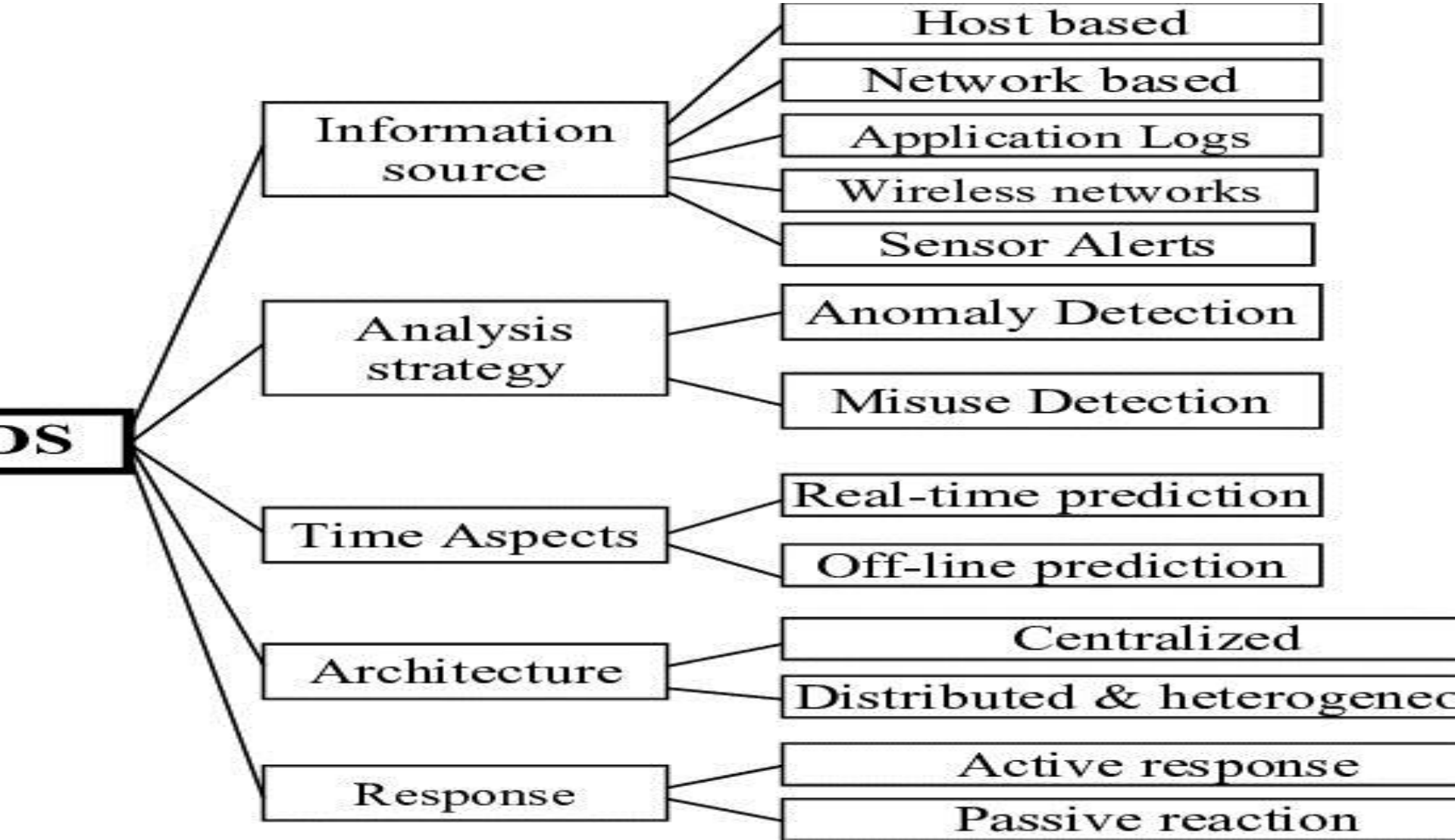

1. Define Objectives
Identify Business Objectives
Identify Security and Compliance Requirements
Business Impact Analysis
2. Define Technical Scope
Capture the Boundaries of the Technical Environment
Capture Infrastructure | Application | Software Dependencies
3. Application Decomposition
Identify Use Cases | Define App. Entry Points & Trust Levels
Identify Actors | Assets | Services | Roles | Data Sources
Data Flow Diagramming (DFDs) | Trust Boundaries
4. Threat Analysis
Probabilistic Attack Scenarios Analysis
Regression Analysis on Security Events
Threat Intelligence Correlation and Analytics
5. Vulnerability & Weaknesses Analysis
Queries of Existing Vulnerability Reports & Issues Tracking
Threat to Existing Vulnerability Mapping Using Threat Trees
Design Flaw Analysis Using Use and Abuse Cases
Scorings (CVSS/CWSS) | Enumerations (CWE/CVE)
6. Attack Modeling
Attack Surface Analysis
Attack Tree Development | Attack Library Mgt.
Attack to Vulnerability & Exploit Analysis Using Attack Trees
7. Risk & Impact Analysis
Qualify & Quantify Business Impact
Countermeasure Identification and Residual Risk Analysis
ID Risk Mitigation Strategies


Stage II - Definition of the Technical Scope (DTS)
Stage III - Application Decomposition and Analysis (ADA)
Stage IV - Threat Analysis (TA)
Stage V - Weakness and Vulnerability Analysis (WVA)
Stage VI - Attack Modeling & Simulation (AMS)


Expert System CVSS
CWE Analysis
Product Analysis
Cycle Sorting Algorithm A New Application of Expert System
COF: CWE Order Factor
CVSS Revise


Base Finding
Base Finding Subscore
Environmental
Environmental Subscore
Attack Surface
Required Privilege
Deployment Scope
Attack Surface Subscore
CWSS
Score


Base Finding
Technical Impact
Acquired Privilege
Acquired Privilege Layer
Internal Control Effectiveness
Finding Confidence
Attack Surface
Required Privilege
Required Privilege Layer
Access Vector
Authentication Strength
Level of Interaction
Deployment Scope
Environmental
Business Impact
Likelihood of Discovery
Likelihood of Exploit
External Control Effectiveness
Prevalence


DS
Information source
Host based
Network based
Application Logs
Wireless networks
Sensor Alerts
Analysis strategy
Anomaly Detection
Misuse Detection
Time Aspects
Real-time prediction
Off-line prediction
Architecture
Centralized
Distributed & heterogenec
Response
Active response
Passive reaction