

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



مباحث ویژه پیرامون فضای سایبر

فضای سایبر و امنیت

Cyberspace and Security

کاظم فولادی
دانشکده مهندسی برق و کامپیوتر
دانشگاه تهران

<http://courses.fouladi.ir/cyber>

فضای سایبر و امنیت



مقدمه

امنیت

توازن آسیب و تهدید



امنیت حاصل از توازن میان آسیب و تهدید است.

امنیت

آسیب



آسیب، یک پدیده‌ی درون سیستم
است که ممکن است به عنوان
نقطه ضعف آن استفاده شود.

امنیت

تهدید

امنیت

تهدید

تهدید، یک پدیده‌ی بیرون سیستم
است و انگیزه‌ای است که ممکن
است ثبات و بقای سیستم را دچار
اختلال کند.

امنیت

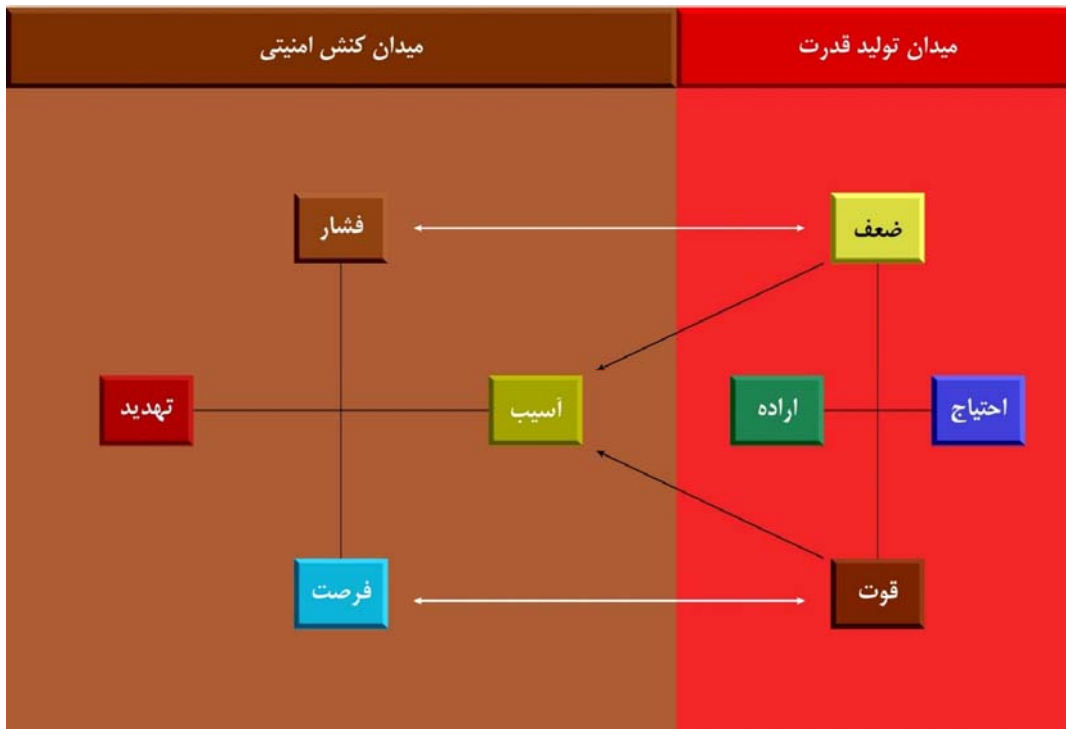
توازن آسیب و تهدید



امنیت حاصل از توازن میان **آسیب** و **تهدید** است.

این توازن در **میدان کنش امنیتی** شکل می‌گیرد
که خود متأثر از **میدان تولید قدرت** است.

میدان کنش امنیتی



توازن آسیب و تهدید در **میدان کنش امنیتی** شکل می‌گیرد که خود متأثر از **میدان تولید قدرت** است.

طیف قدرت

بر مبنای سیستم ارگانیکی

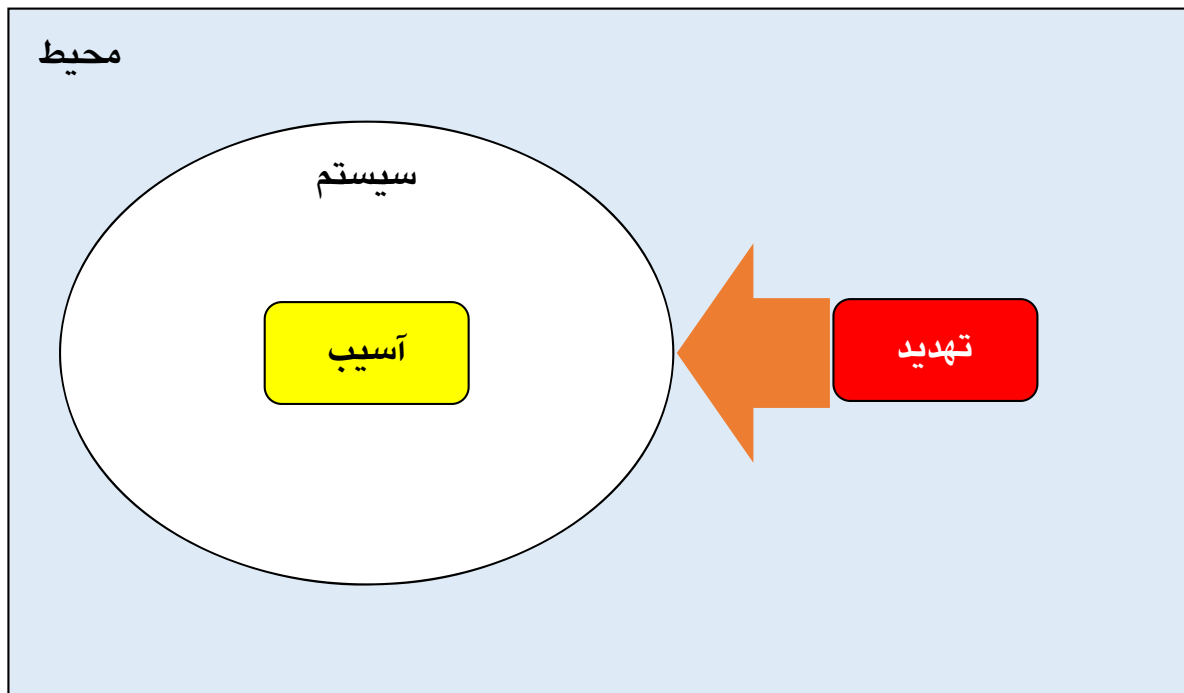
حوزه‌ی قدرت	آماج - میدان عمل		روش	جهت	دکترین قدرت اقدام
	سیادت	تصرف			
قدرت سخت	نظامی	تصرف سرزمین	_____	بود و نبود	قهری
		_____	سیادت بر اقیانوس - دریا	بود و نبود	قهری
		_____	سیادت بر فضا - هوا	بود و نبود	قهری
قدرت نیمه سخت	سیاسی اقتصادی اجتماعی	تصرف حکومت	سیادت بر حاکمیت	منفعت نفع و ضرر	تشویقی تنبیهی
		تصرف بازار	سیادت بر منابع اقتصادی	منفعت نفع و ضرر	تشویقی تنبیهی
		تصرف اجتماعی	سیادت بر جامعه	منفعت نفع و ضرر	تشویقی تنبیهی
قدرت نرم	فرهنگی روانی اطلاعاتی	تصرف قلب‌ها	_____	ولایت و برانیت	ارضایی
		_____	سیادت بر مغزها	حق و باطل	اقتناعی

طیف قدرت

بر مبنای سیستم سایبرنتیکی

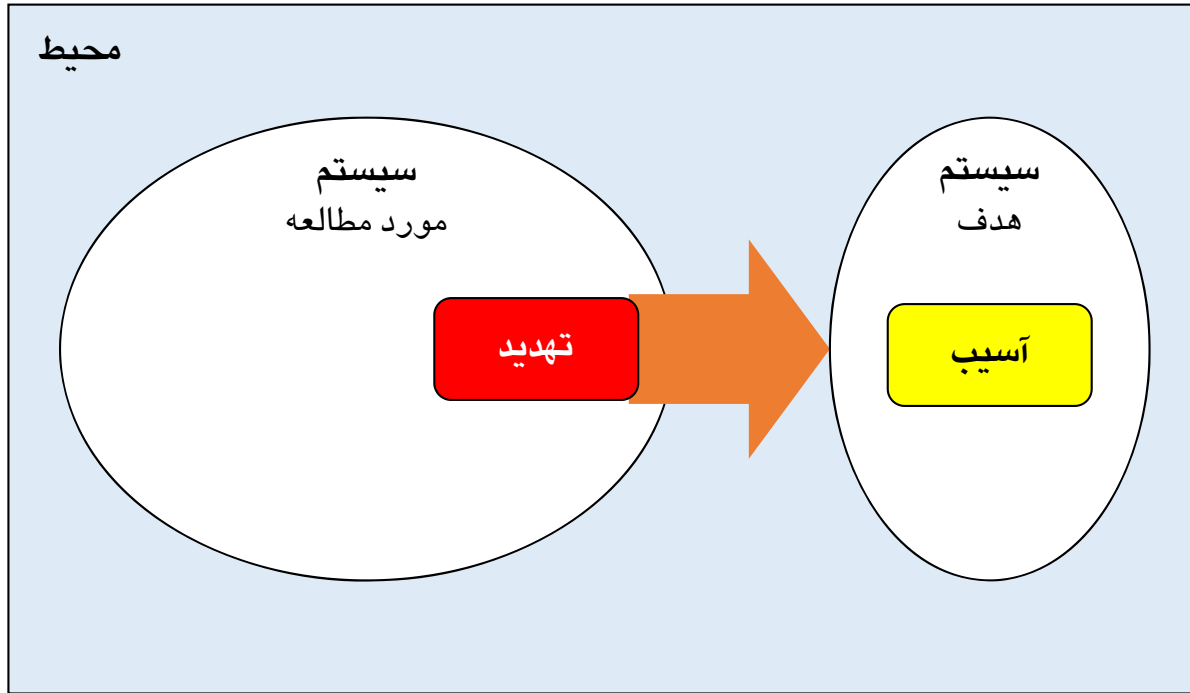
		حوزه‌ی قدرت	میدان عمل - آماج	روش	جهت	دکترین قدرت اقدام
قدرت سایبرنتیکی	قدرت سخت	انرژی	نیرو	تبدیل حالت ماده	سکون یا حرکت	توان یا ناتوانی
	قدرت نیمه سخت	سایبر	کنترل	وابستگی و یکپارچگی	مهار و فرمان	حرکت از قوه به فعل
	قدرت نرم	اطلاعات	آگاهی	گردآوری دسته‌بندی انتشار	دروازه بانی خبر	بی اطلاع نگه داشتن یا مطلع سازی

امنیت یک سیستم



مسئله، امنیت خود سیستم است.

امنیت متأثر از یک سیستم



مسئله امنیت سیستم دیگر (سیستم هدف) است که با تهدیدی از سوی سیستم مورد مطالعه مواجه می‌شود.

امنیت

به عنوان یک خاصیت غیرکارکردی سیستم

امنیت یک خاصیت غیرکارکردی یک سیستم است.

یعنی یک جزء سیستمی متولی تولید و حفظ آن نیست
بلکه کل سیستم به مثابه یک کل واجد این خاصیت می شود.

نظریه های امنیت ذیل نظریه ی سیستم ها تعریف می شوند.

امنیت فضای سایبر

فراتر از امنیت اطلاعات و امنیت شبکه

امنیت فضای سایبر
چیزی فراتر از امنیت اطلاعات و امنیت شبکه است.

فضای سایبر و امنیت

۲

مکتب‌های
امنیتی

امنیت

مکاتب امنیتی



امنیت حاصل از توازن میان **آسیب** و **تهدید** است.

چگونگی ایجاد این توازن، مکاتب مختلف امنیتی را پدید می آورد.

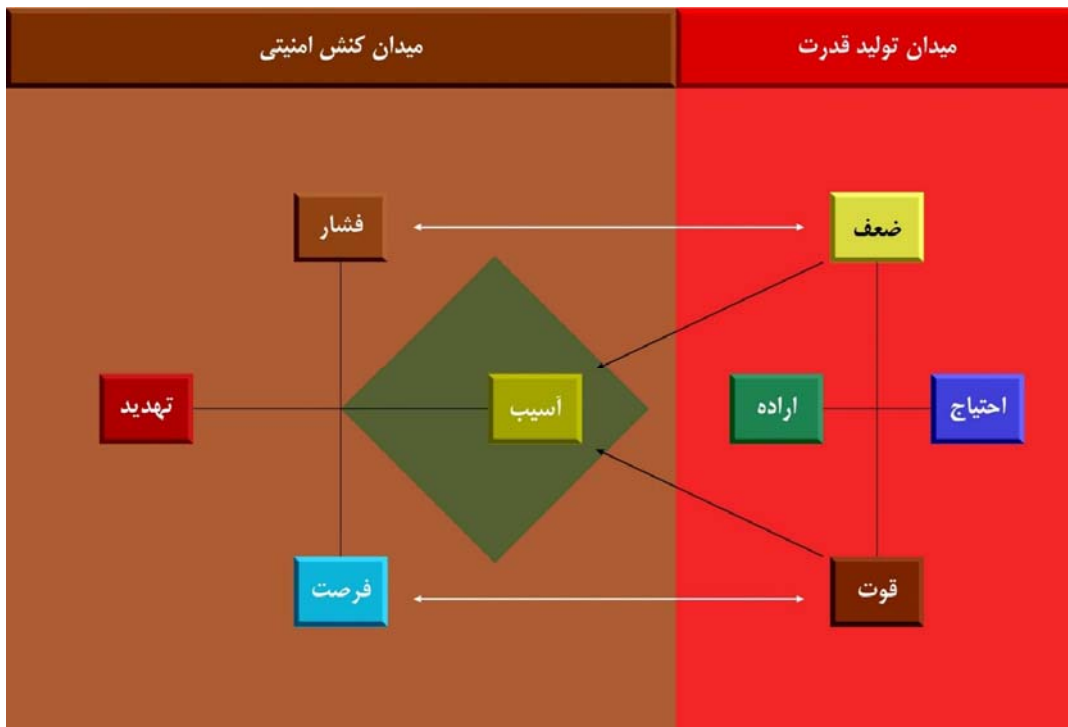
مکتب آسیب محور

دکترین مکتب امنیتی آسیب محور

باید آسیب‌ها را پوشش داد.



مکتب آسیب محور



در این مکتب، مبتنی بر نقاط قوت سیستم، اصالت با تلاش برای پوشاندن آسیب است نه از میان برداشتن تهدید.

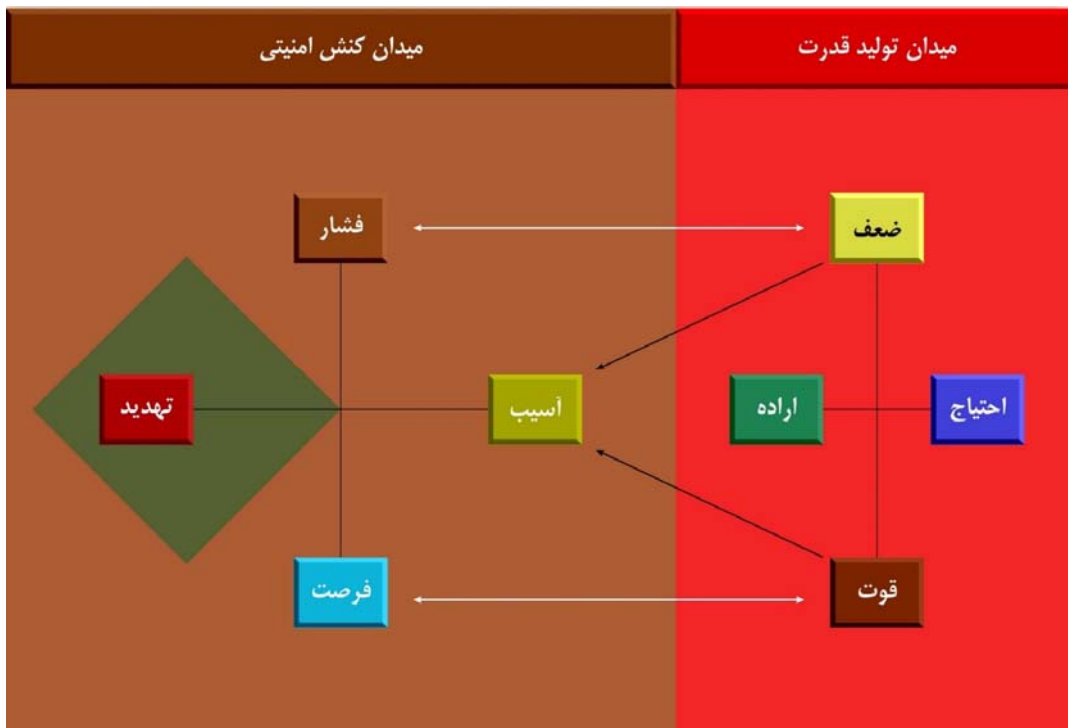
مکتب تهدیدمحور

دکترین مکتب امنیتی تهدیدمحور

باید تهدید را از منشأ نابود کرد.



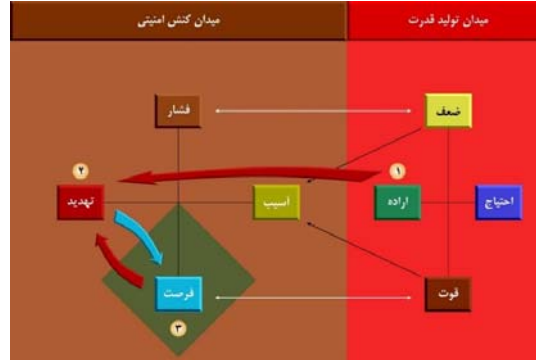
مکتب تهدیدمحور



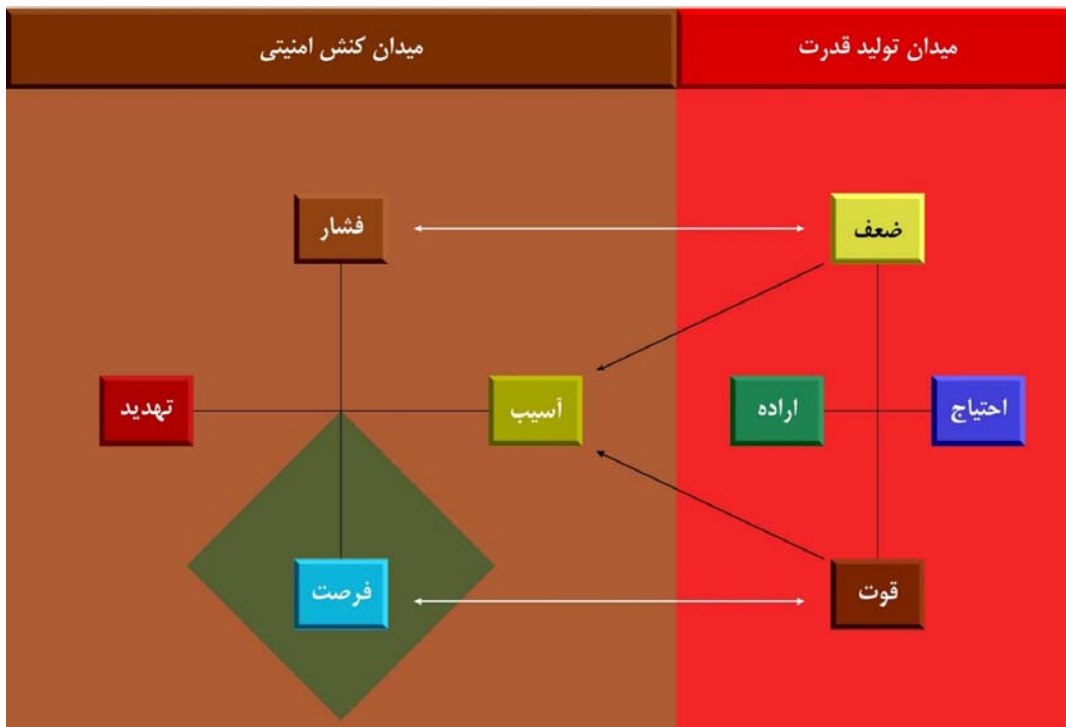
در این مکتب، امکان کاهش آسیب از درون وجود ندارد، بلکه باید تهدید را در بیرون خنثی کرد.

دکترین مکتب امنیتی فرصت طلب

باید تهدید را به فرصت تبدیل کرد.



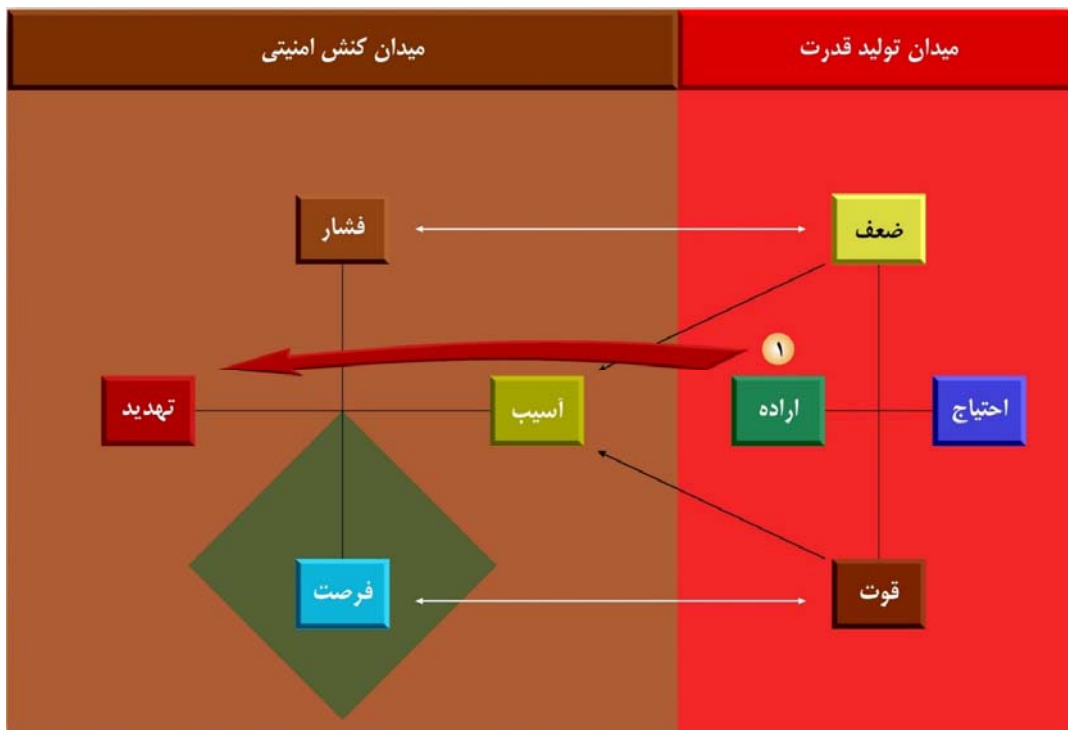
مکتب فرصت طلب



در این مکتب، ابتدا تهدید برآورد می‌شود و سپس آن را به فرصت تبدیل می‌کنند.

مکتب فرصت طلب

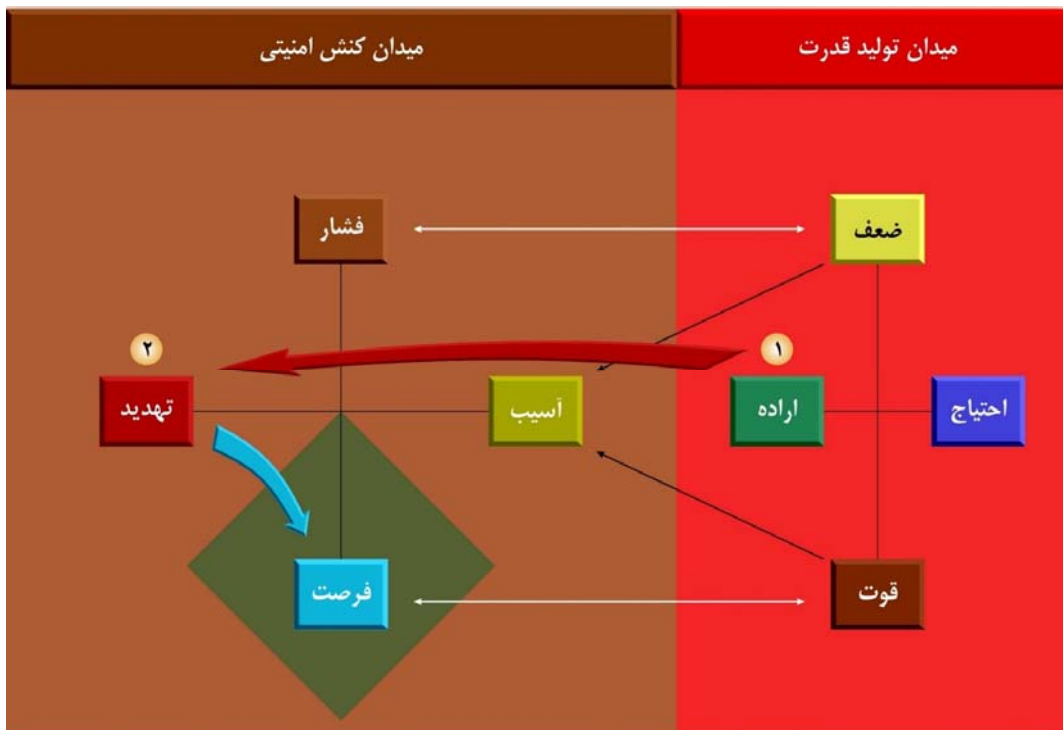
گام یکم پروژه در مکتب امنیتی فرصت طلب: تولید تهدید



۱) ابتدا به ساکن، **اراده‌ای** به صورت **تهدید** علیه سیستم به وجود می‌آید: باید تهدید را تبیین و تدقیق نمود.

مکتب فرصت طلب

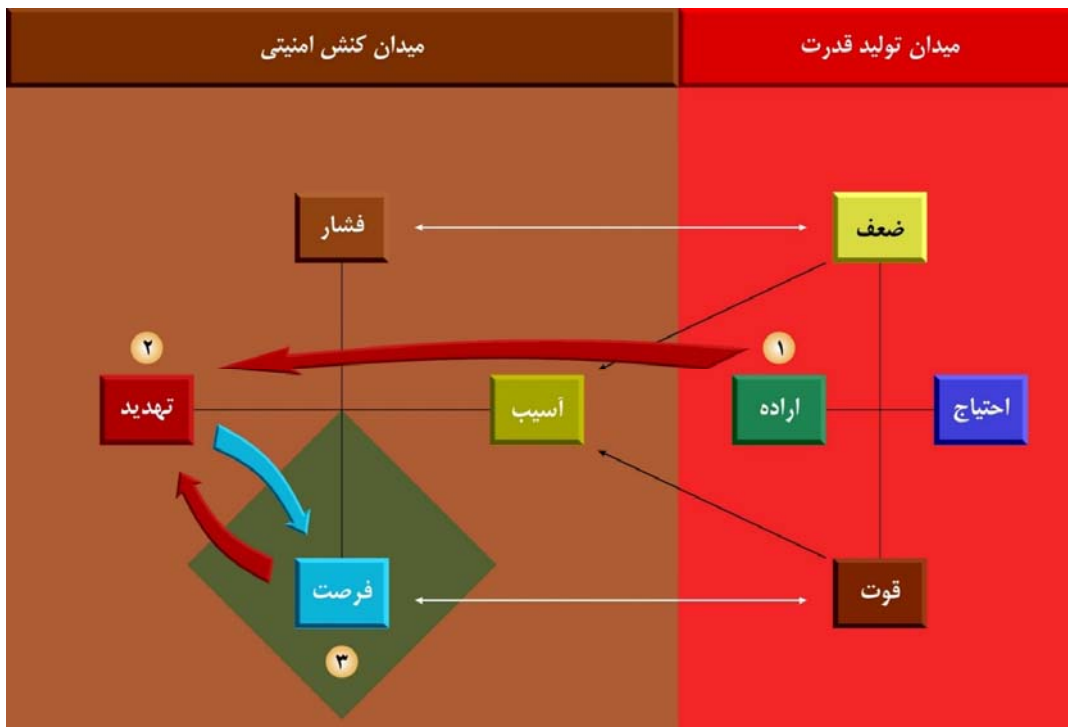
گام دوم پروژه در مکتب امنیتی فرصت طلب: تبدیل تهدید به فرصت



(۲) در گام بعدی، با توجه به ماهیت تهدید، فرصتی تعریف می‌شود که معطوف به **قوت** سیستم خواهد بود.

مکتب فرصت طلب

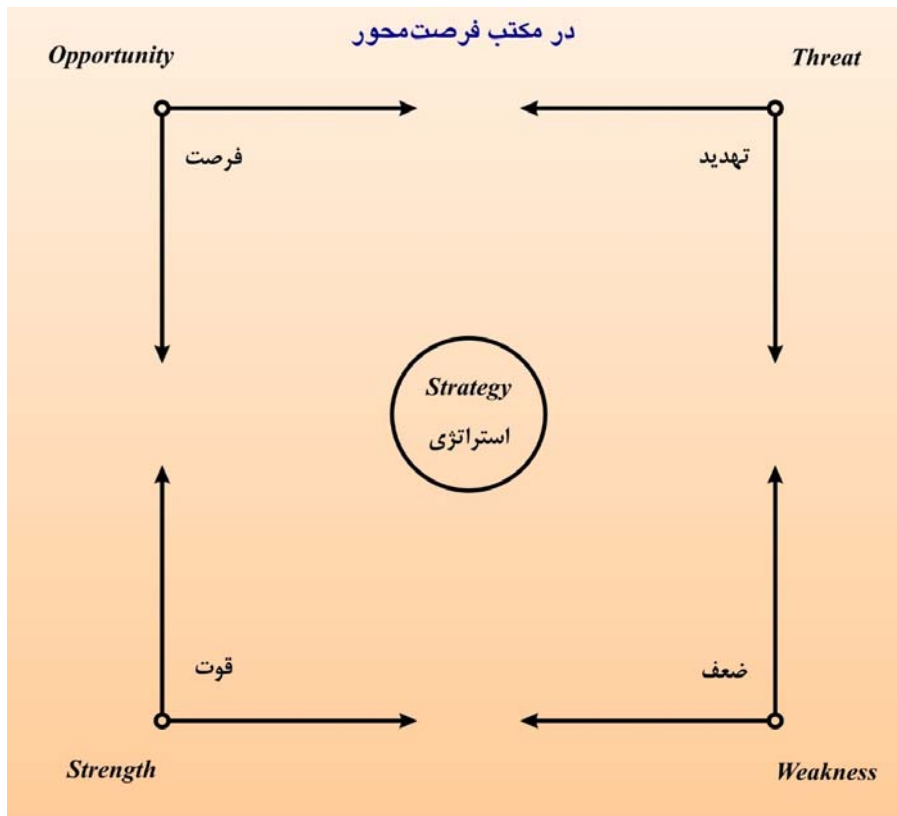
گام سوم پروژه در مکتب امنیتی فرصت طلب: خنثی شدن تهدید



۳) در نهایت، تهدید خنثی می‌شود و فرصت ایجاد شده برای سیستم سبب تقویت آن می‌شود.

مکتب فرصت طلب

تحلیل SWOT







SWOT ANALYSIS



SWOT ANALYSIS

Internal		External	
Strengths	Weaknesses	Opportunities	Threats



SWOT ANALYSIS

	Strengths 1. 2. 3. 4.	Weaknesses 1. 2. 3. 4.
Opportunities 1. 2. 3. 4.	Opportunity-Strength strategies <i>Use strengths to take advantage of opportunities</i> 1. 2.	Opportunity-Weakness strategies <i>Overcome weaknesses by taking advantage of opportunities</i> 1. 2.
Threats 1. 2. 3. 4.	Threat-Strength strategies <i>Use strengths to avoid threats</i> 1. 2.	Threat-Weakness Strategies <i>Minimize weaknesses and avoid threats</i> 1. 2.



مکتب موقعیت طلب

دکترین مکتب امنیتی موقعیت طلب

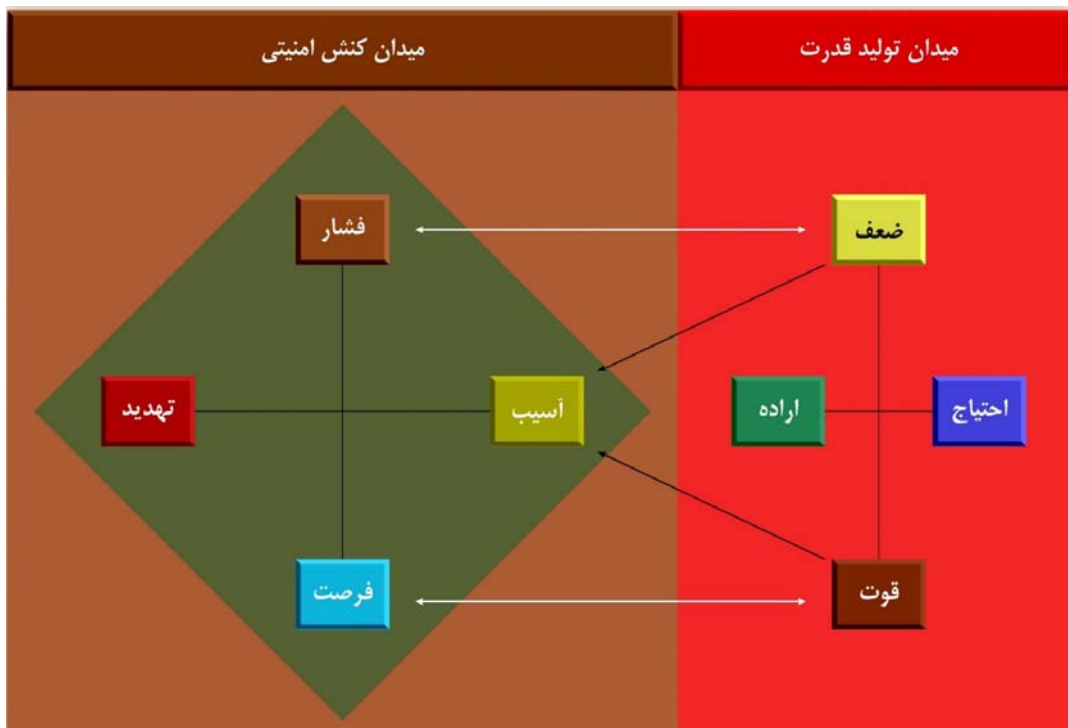
باید از تهدید موقعیت متعالی به دست آورد.







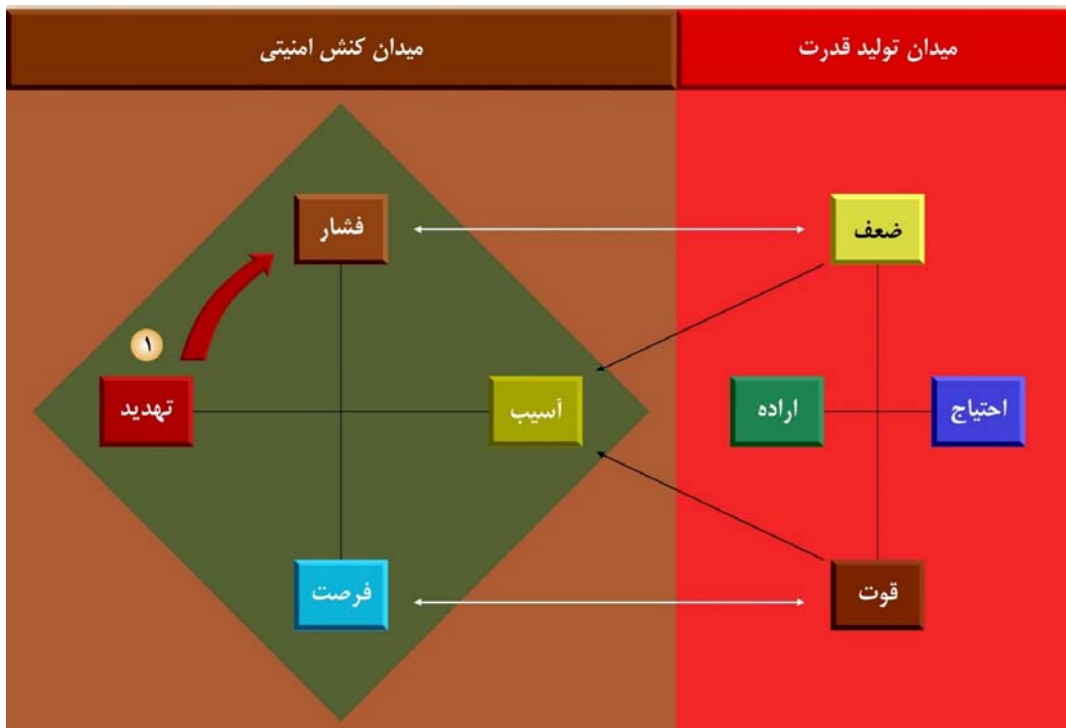
مکتب موقعیت طلب



در این مکتب، امنیت از طریق تبیین تهدید، و مصادره و هضم آن برای ایجاد موقعیت متعالی تر سیستم شکل می گیرد.

مکتب موقعیت طلب

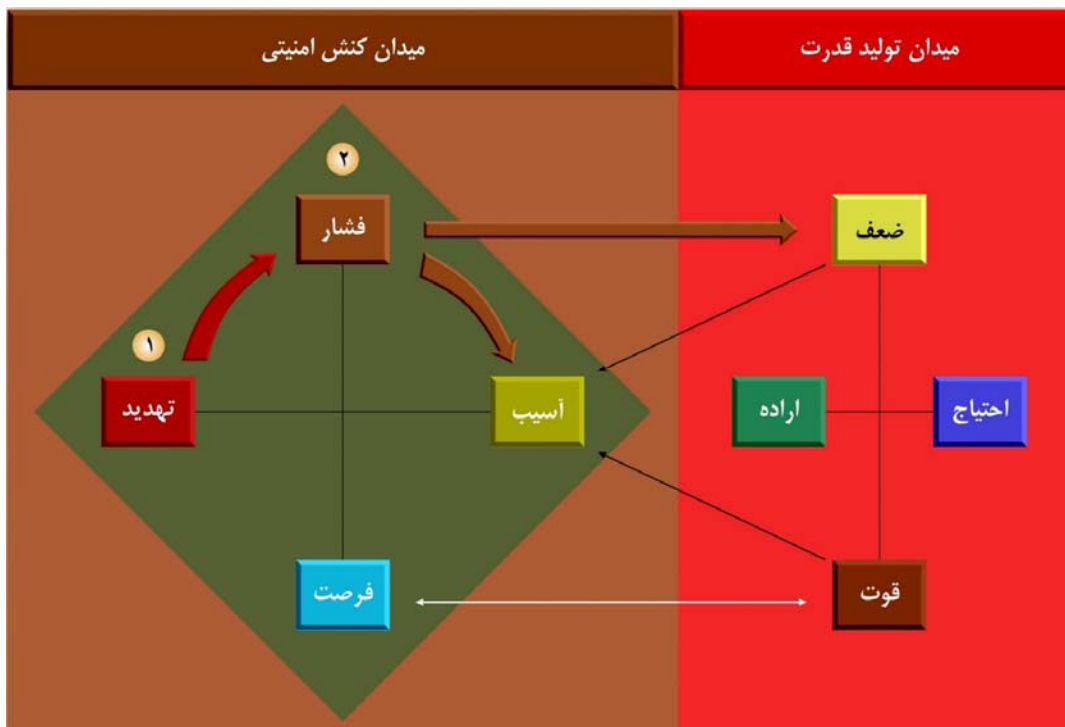
گام اول پروسه در مکتب امنیتی موقعیت طلب: روند اعمال تهدید



(۱) در میدان کنشی امنیتی، تهدیدی به وجود می آید.

مکتب موقعیت طلب

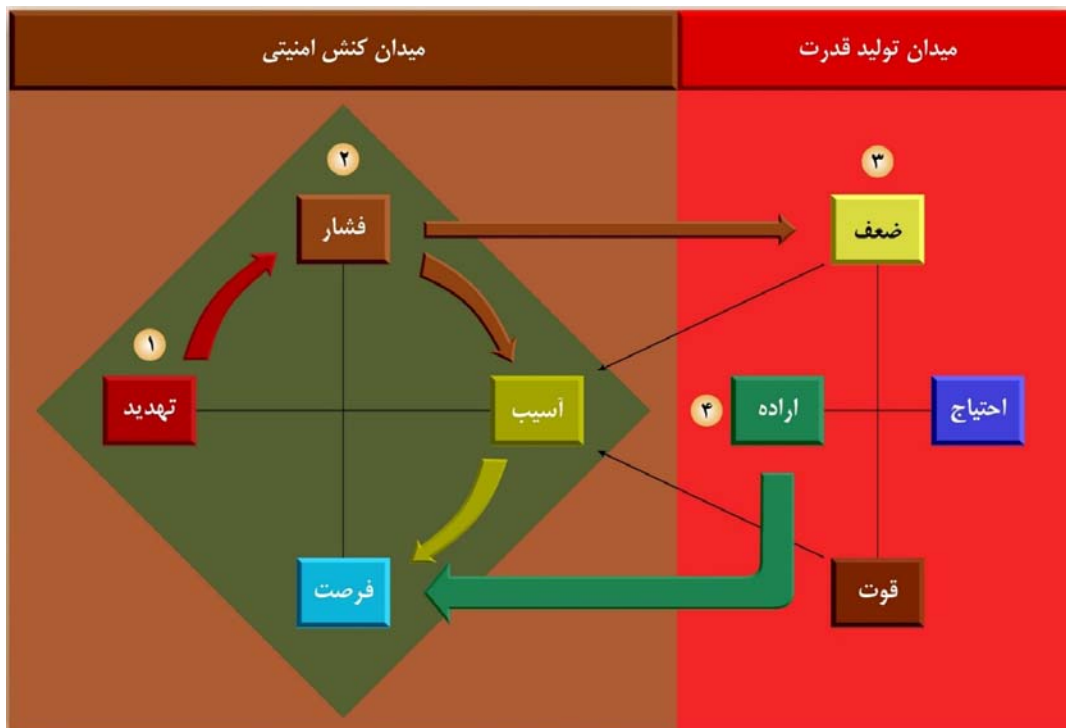
گام دوم پروسه در مکتب امنیتی موقعیت طلب: روند اعمال فشار



(۲) تهدید بیرونی، از سویی سبب ایجاد فشار بر نقاط ضعف سیستم می شود و از سوی دیگر موجب آسیب می شود.

مکتب موقعیت طلب

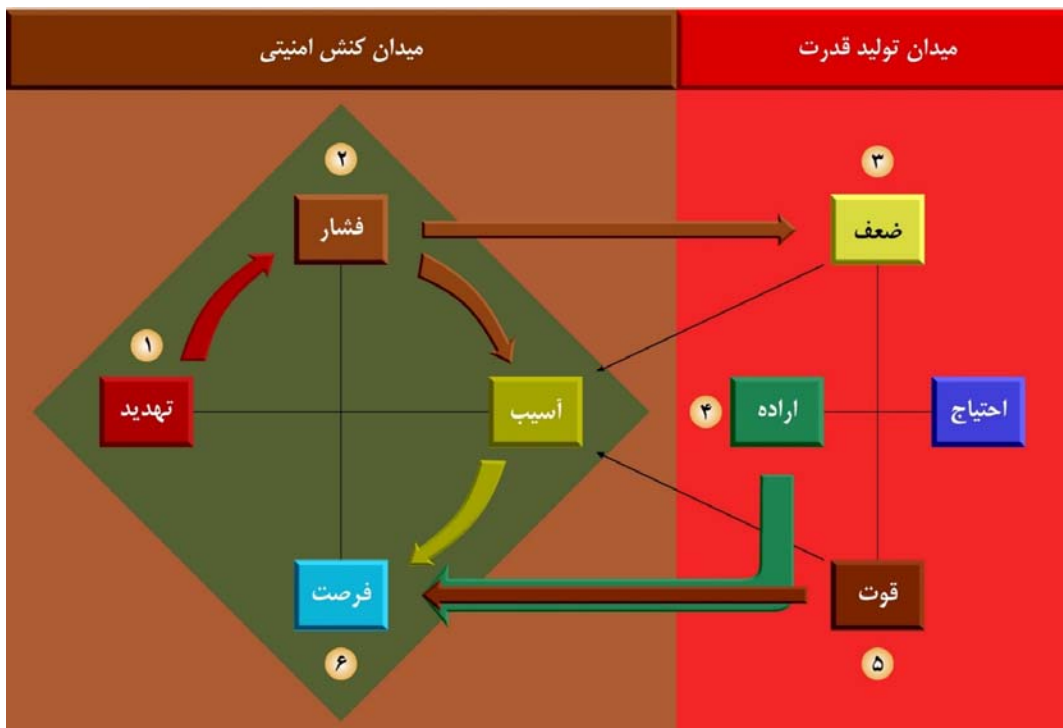
گام سوم پروسه در مکتب امنیتی موقعیت طلب: روند اعمال اراده



۳) آسیب صورت گرفته، اراده‌ی سیستم را برای واکنش علیه تهدید صورت گرفته، شکل می‌دهد.

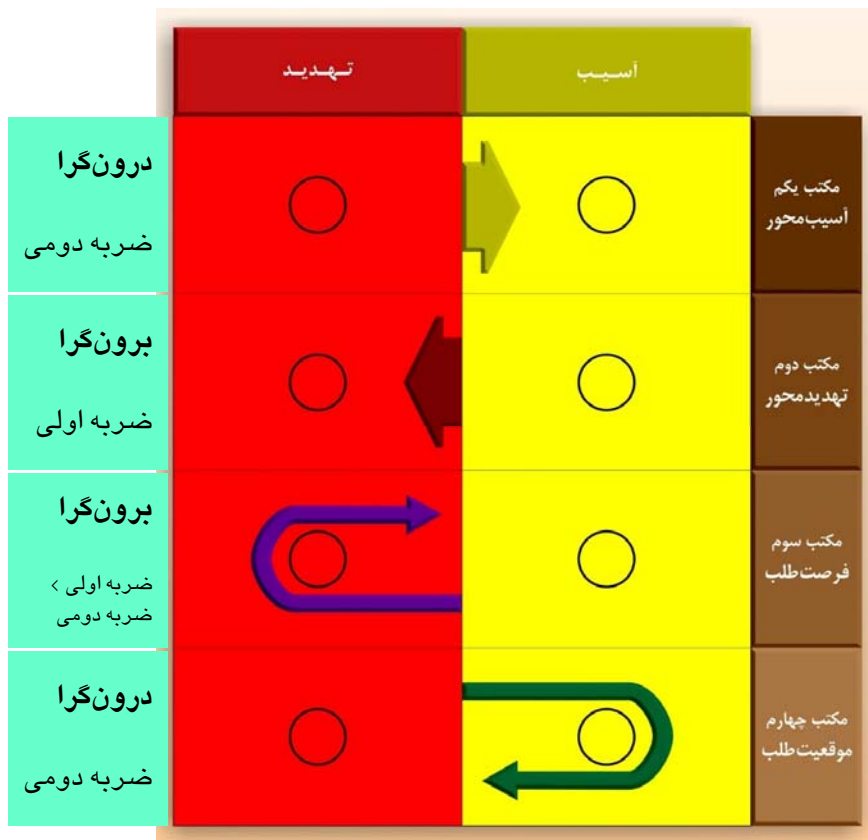
مکتب موقعیت طلب

گام چهارم پروسه در مکتب امنیتی موقعیت طلب: روند اعمال قدرت مبتنی بر قوت



۴) قوت و توانایی ذاتی سیستم، سبب می شود ارزش و موقعیت سیستم در مواجهه با تهدید بیرونی با هضم آن تهدید بالاتر رود. (با وجود ایجاد آسیب)

صورت‌بندی مکاتب امنیتی



دکترین امنیت در نسبت با مکاتب امنیتی

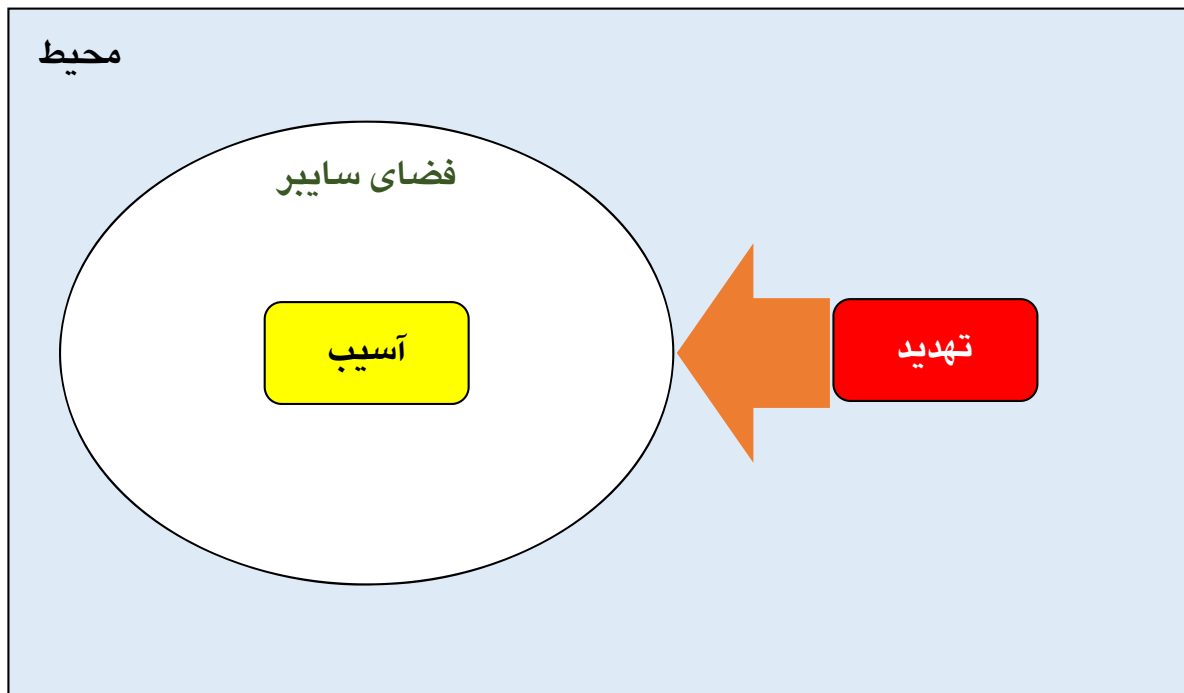
تهدید	آسیب	
باید جلو پوشش آسیب پذیری های دشمن را گرفت.	باید آسیب ها را پوشش داد.	مکتب اول آسیب محور
به نیت نابودی دشمن، باید تهدیدی جدی علیه او شد.	باید تهدیدها را از منشاء نابود کرد.	مکتب دوم تهدید محور
نباید اجازه داد دشمن، تهدید بودن ما را به فرصت تبدیل کند.	باید تهدیدها را به فرصت تبدیل کرد.	مکتب سوم فرصت طلب
نباید اجازه داد دشمن، تهدید بودن ما را به موقعیت برتر خود تبدیل کند.	باید از تهدیدها موقعیت متعالی پدید آورد.	مکتب چهارم موقعیت طلب

فضای سایبر و امنیت

۳

امنیت
فضای
سایبر

امنیت فضای سایبر



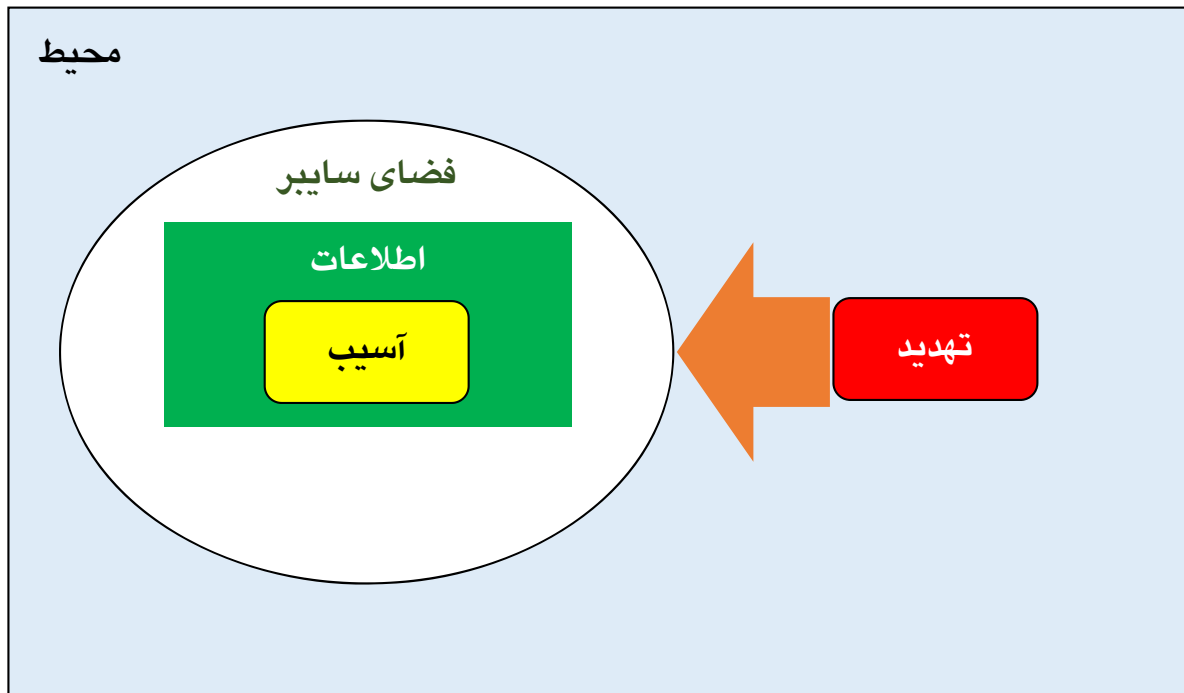
مسئله، امنیت خود زیرساخت و کاربرد فضای سایبر است.

امنیت زیرساخت و کاربرد فضای سایبر

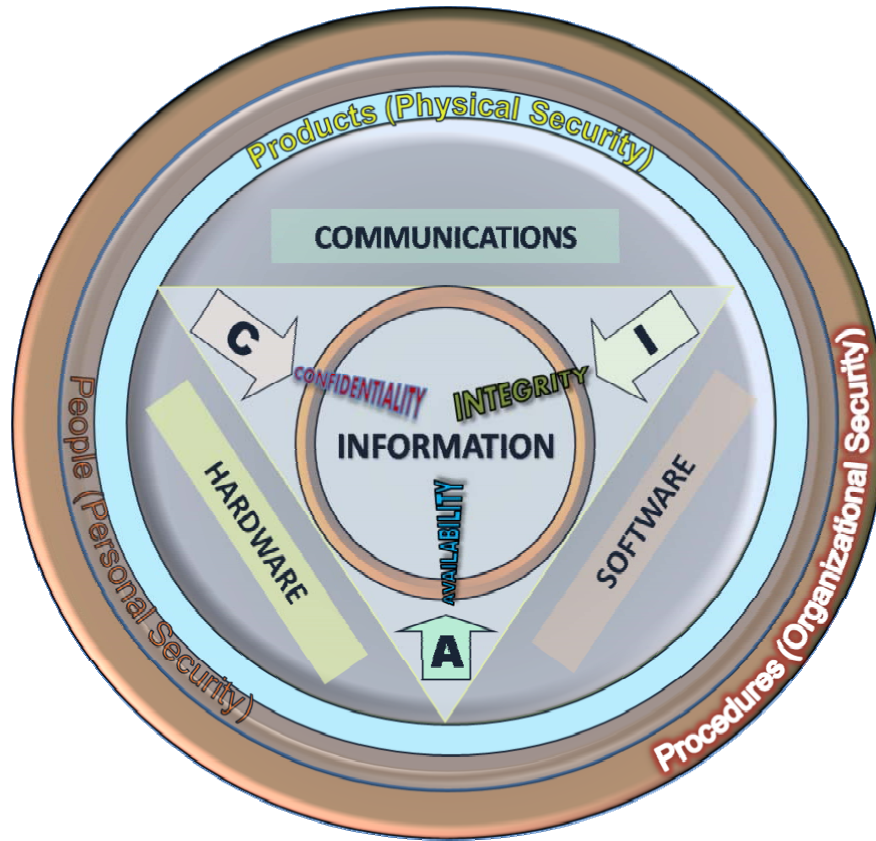


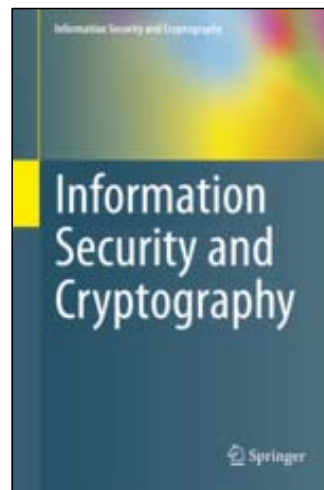
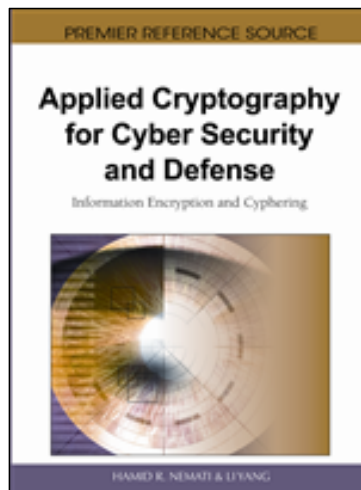
امنیت فضای سایبر

امنیت اطلاعات



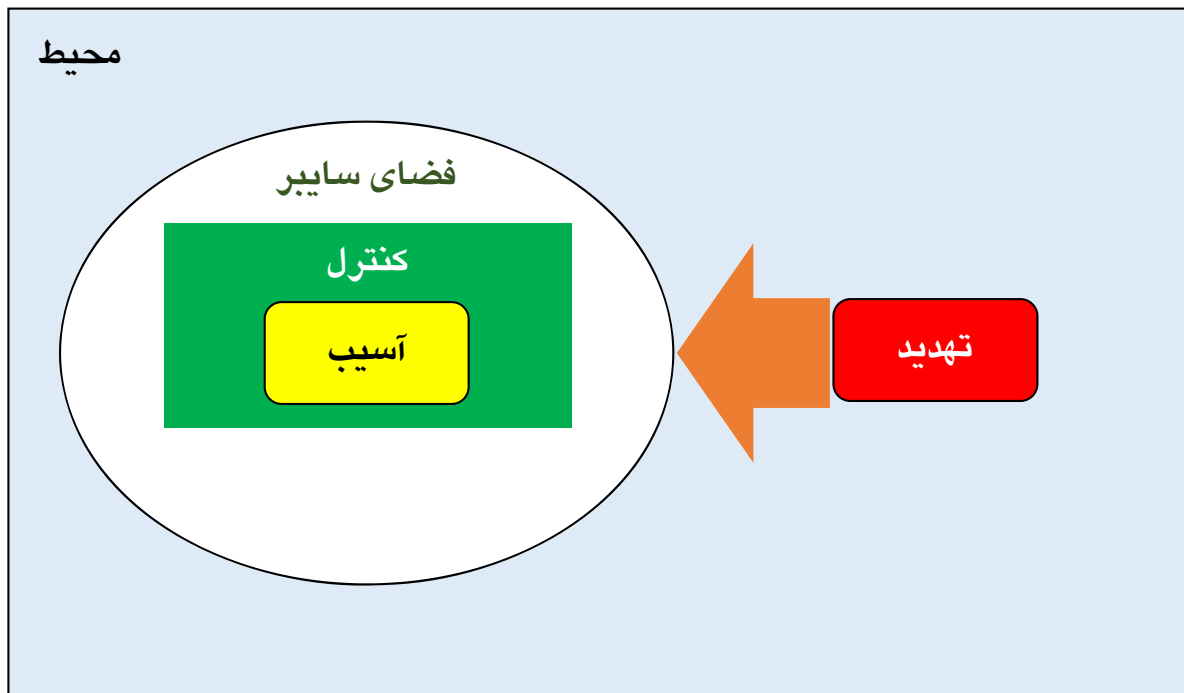
امنیت لایه‌ی اطلاعات





امنیت فضای سایبر

امنیت کنترل



امنیت لایه‌ی کنترل

Operating Systems Security

Lesson Preview

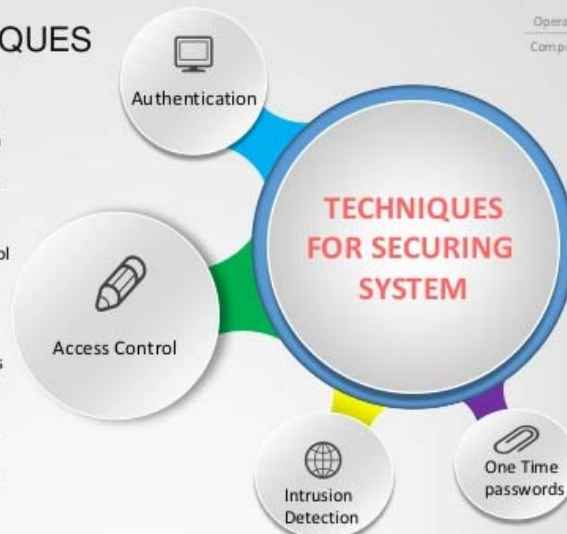
- Understand the important role an **operating system** plays in computer security
 - Learn about the **need for hardware support** for isolating OS from untrusted user/application code
 - Understand **key trusted computing** base concepts
-

SECURITY TECHNIQUES

Security

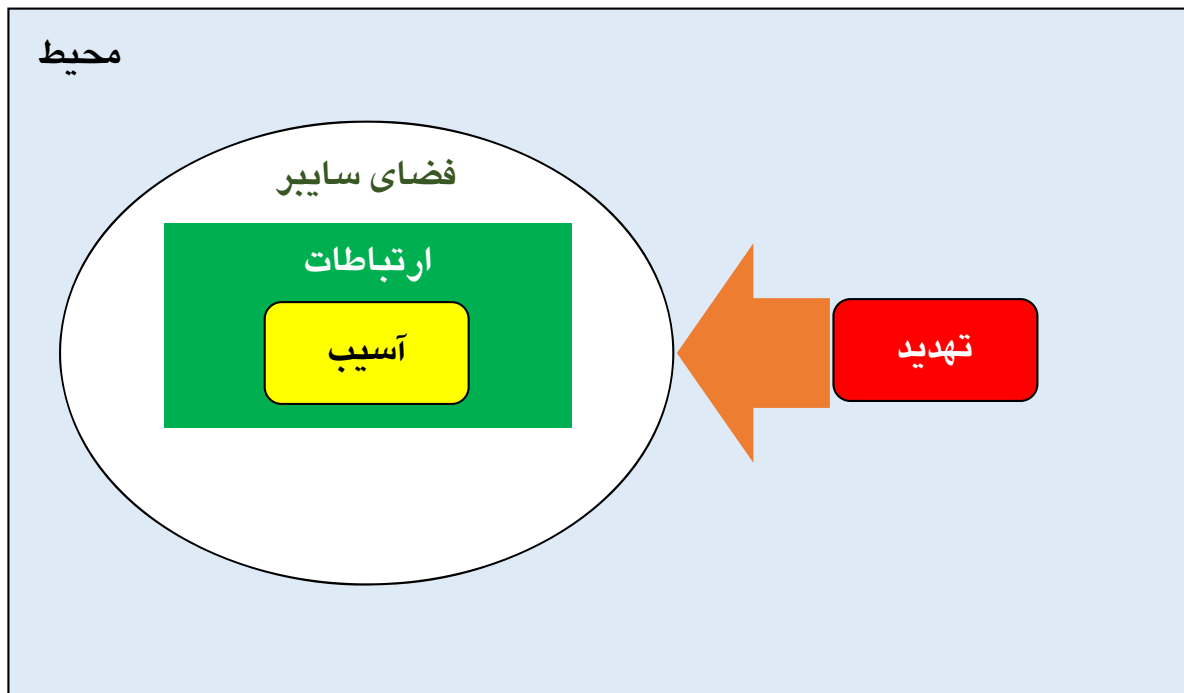
Operating System
Computer Security

- The operating system is the physical environment where your application runs. Any vulnerability in the operating system could compromise the security of the application. By securing the operating system, you make the environment stable, control access to resources, and control external access to the environment.
- The physical security of the system is essential. Threats can come through the Web, but they can also come from a physical terminal. Even if the Web access is very secure, if an attacker obtains physical access to a server, breaking into a system is much easier.

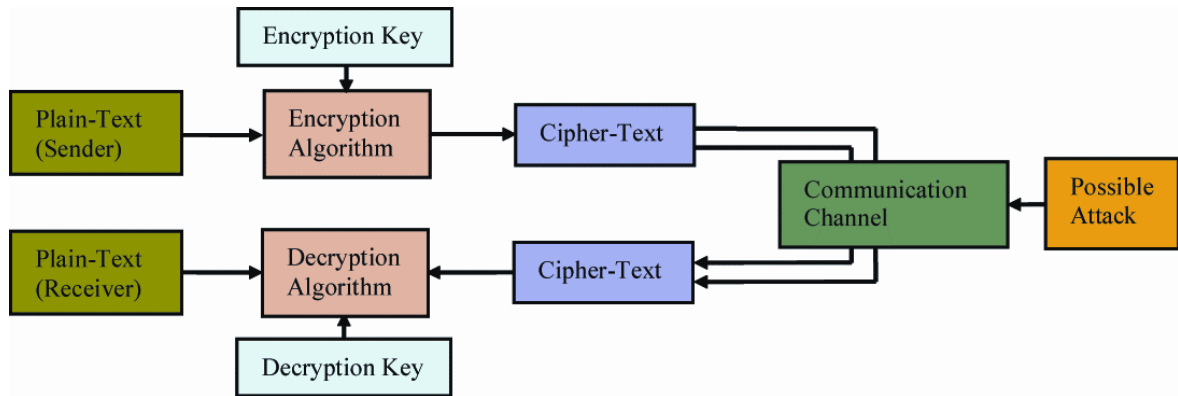


امنیت فضای سایبر

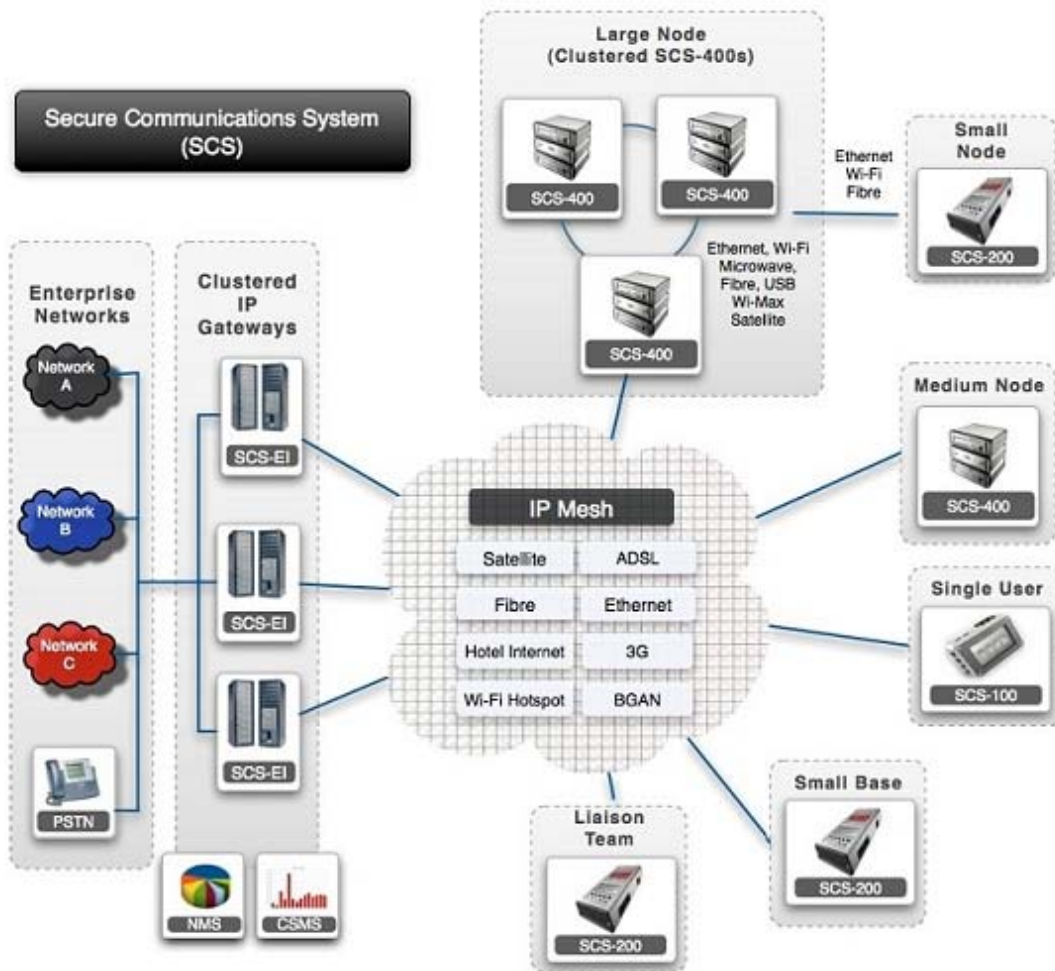
امنیت ارتباطات



امنیت لایه‌ی ارتباطات



Secure Communications System (SCS)



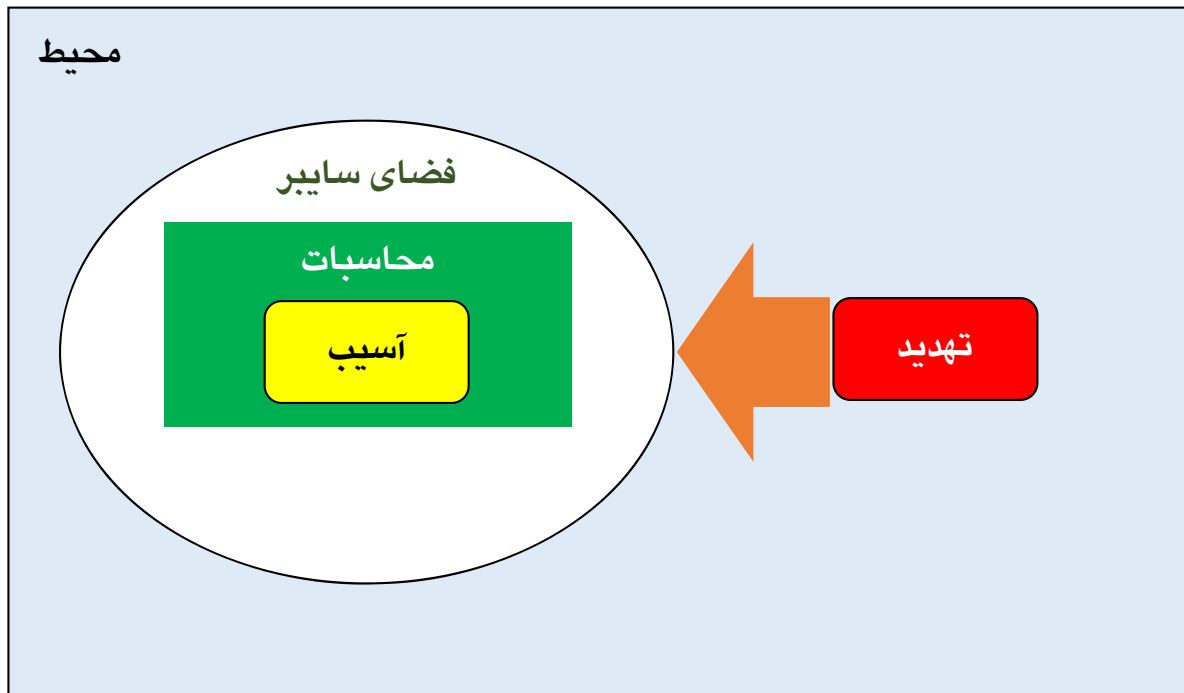
The SCS devices automatically find each other and form a meshed network, capable of dynamically reconstituting and reforming as the environment changes.

Devices are able to communicate directly to each other without the need to communicate through a gateway.

Devices can be remotely managed and report cyber security events to a central monitoring system

امنیت فضای سایبر

امنیت محاسبات



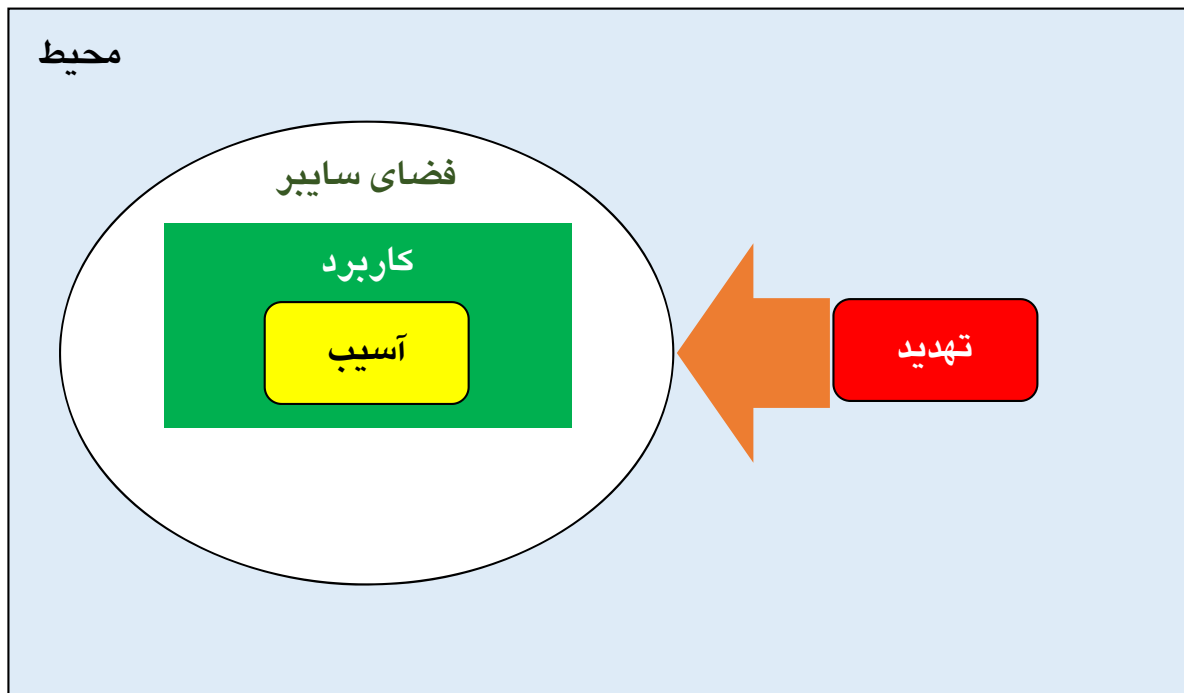
امنیت لایه‌ی محاسبات



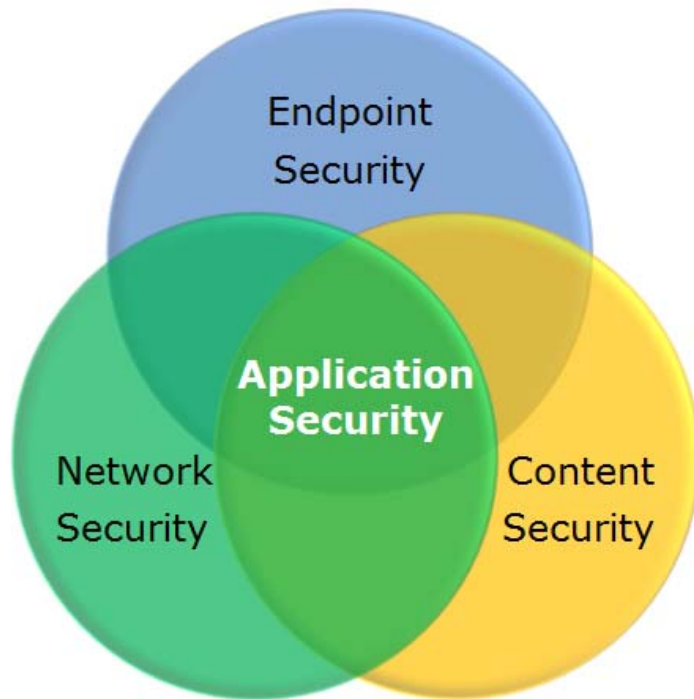
Ninh V. Nguyen
ninh.nv@gmail.com

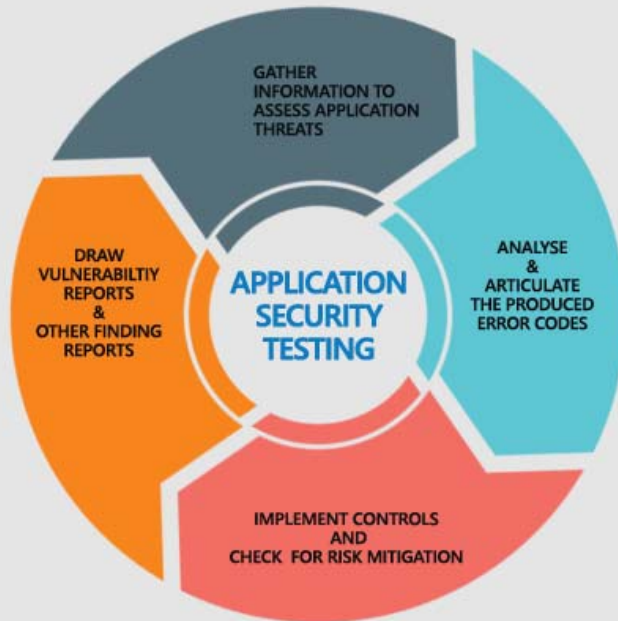
امنیت فضای سایبر

امنیت کاربرد



امنیت لایه‌ی کاربرد





امنیت فضای سایبر با در نظر گرفتن مکاتب امنیتی



مثال:

آسیب‌ها و تهدیدهای پروتکل EIGRP

شماره	آسیب	تهدید
۴-۱	مسیریاب اگر تعداد زیادی از بسته‌های اعلان همسایگی را به طور همزمان دریافت کند نمی‌تواند آن‌ها را پردازش نماید.	ارسال تعداد زیادی از بسته‌های اعلان همسایگی به طور همزمان، عملکرد مسیریاب قربانی را مختل خواهد کرد.
۴-۲	احراز هویت در پروتکل EIGRP هنگام ایجاد عبارت MD5 تنها بخش‌های خاصی از بسته را در نظر می‌گیرد.	مهاجم می‌تواند با شنود یک بسته Hello قانونی از عبارت MD5 همراه آن استفاده کرده و همراه یک بسته Hello که خود آن را ایجاد کرده است ارسال و در شبکه اختلال ایجاد نماید.
۴-۳	در صورت ارسال بسته‌های تقلبی Goodbye و یا بسته‌هایی با مقادیر متفاوت ضرایب K عملکرد مسیریاب موقتاً مختل خواهد شد.	مهاجم با ارسال این بسته‌ها به صورت مداوم باعث ایجاد اختلال دائمی در عملکرد مسیریاب قربانی می‌شود.

تهدید: مهاجم می‌تواند با شنود یک بسته Hello قانونی از عبارت MD5 همراه آن استفاده کرده و همراه یک بسته Hello که خود آن را ایجاد کرده است ارسال و در شبکه اختلال ایجاد نماید.	آسیب: احراز هویت در پروتکل EIGRP هنگام ایجاد عبارت MD5 تنها بخش‌های خاصی از بسته را در نظر می‌گیرد.	شماره: ۲-۴
پوشش دادن تمام بخش‌های بسته EIGRP در احراز هویت و همچنین امضای بسته‌ها با استفاده از روش MAC		استراتژی امنیت با مکتب آسیب محور
طراحی و پیاده‌سازی سیاست‌های امنیت فیزیکی و اعمال کنترل دسترسی دقیق		استراتژی امنیت با مکتب تهدید محور
با محدود و مشخص نمودن همسایه‌های هر مسیریاب به صورت دستی علاوه بر این که تهدید مذکور ناکارآمد می‌شود، پیامدهای حاصل از اشتباهات مدیریتی در شبکه نیز کاهش می‌یابد.		استراتژی امنیت با مکتب فرصت محور
با وقوع چنین حملاتی مدیران انگیزه لازم را به منظور حمایت بیشتر از توسعه سیاست‌های سازمانی و ارتقاء پروتکل‌های مورد استفاده به دست می‌آورند و به این ترتیب علاوه بر هضم تهدید، یک سیستم پیشرفته‌تر خواهیم داشت که ارزش آن بیشتر از سیستم قدیمی است		استراتژی امنیت با مکتب موقعیت محور

امنیت فضای سایبر با در نظر گرفتن سطوح اقدام

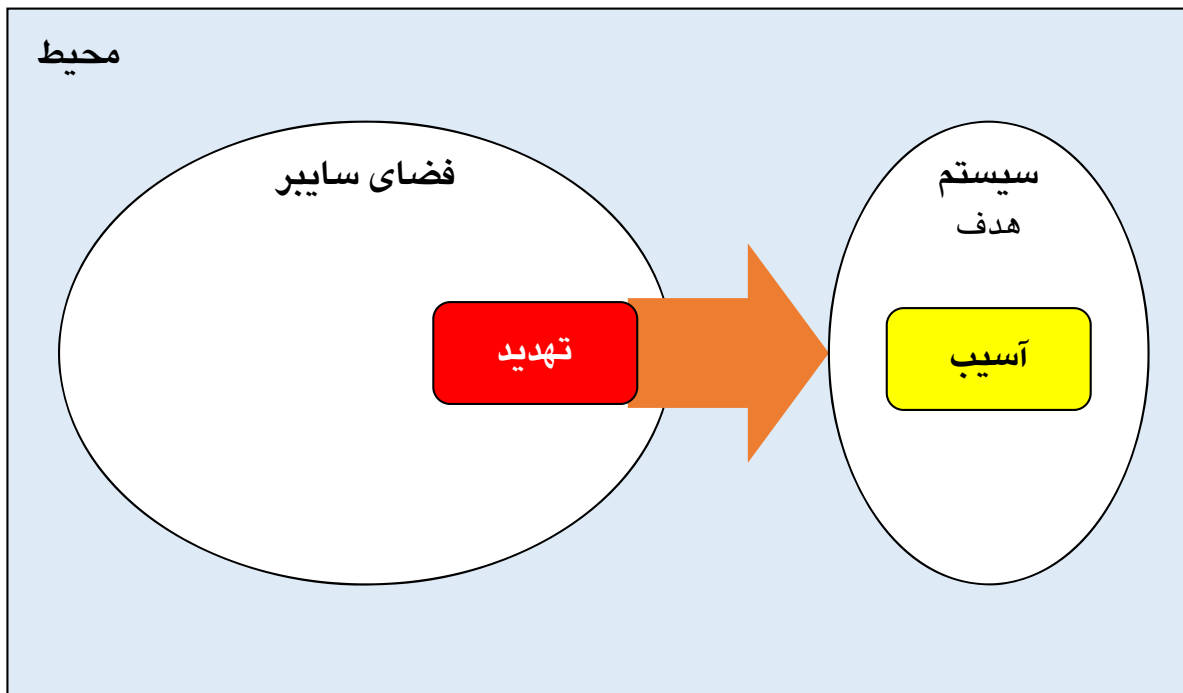


فضای سایبر و امنیت

۴

امنیت
متأثر از
فضای
سایبر

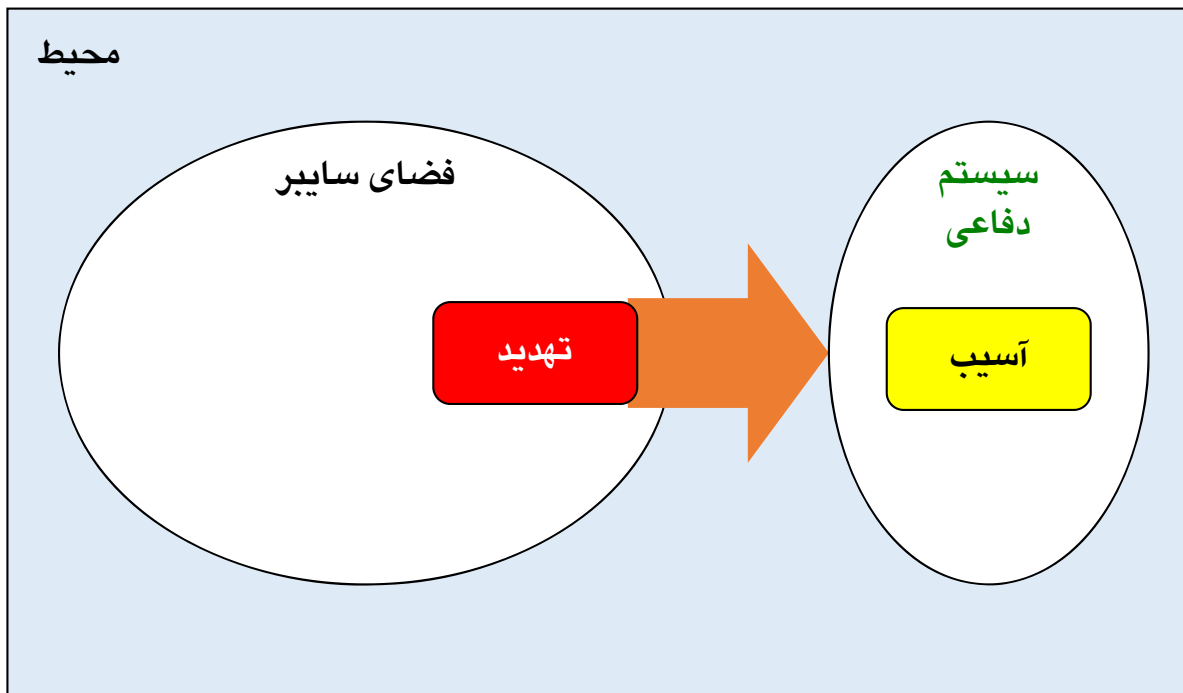
امنیت متأثر از فضای سایبر



مسئله امنیت سیستم دیگر (سیستم هدف) است که با تهدیدی از سوی فضای سایبر مواجه می شود.

امنیت متأثر از فضای سایبر

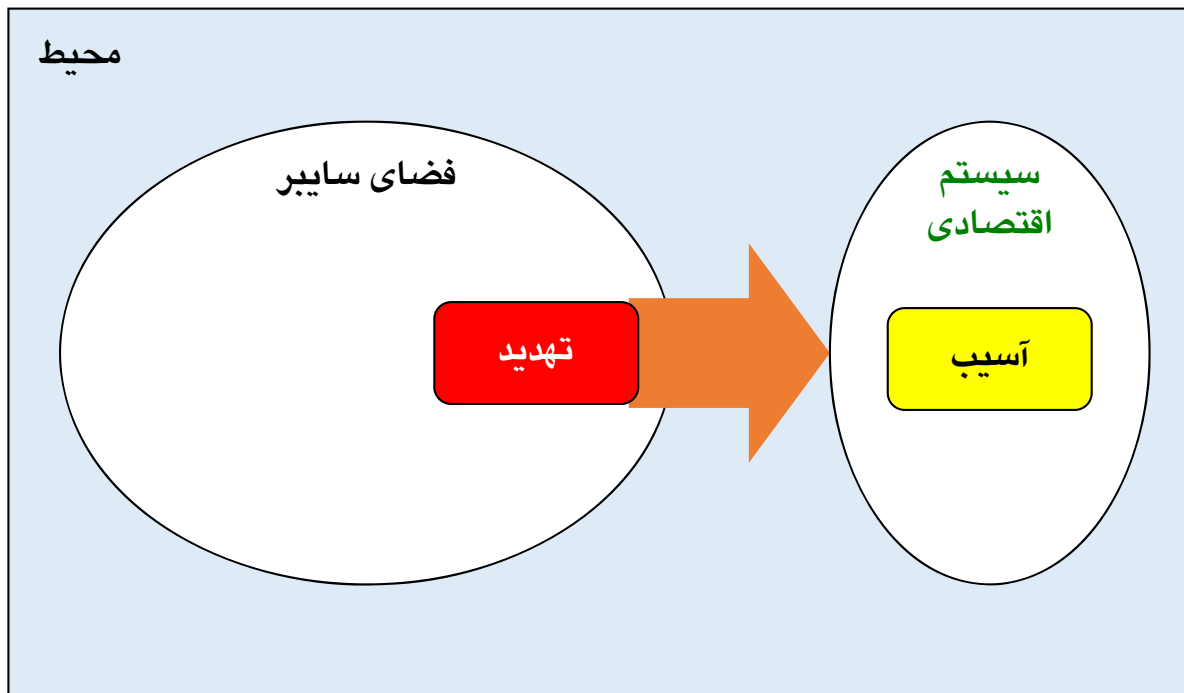
امنیت دفاعی



امنیت دفاعی : امنیت سیستم دفاعی

امنیت متأثر از فضای سایبر

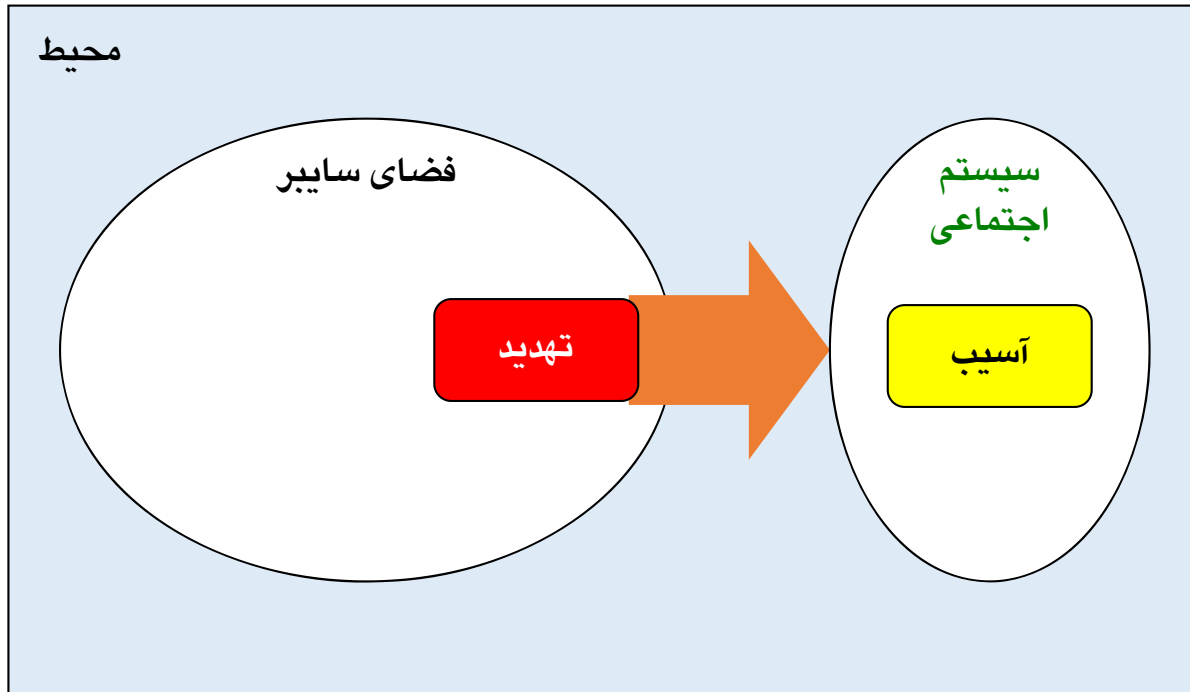
امنیت اقتصادی



امنیت اقتصادی: امنیت سیستم اقتصادی

امنیت متأثر از فضای سایبر

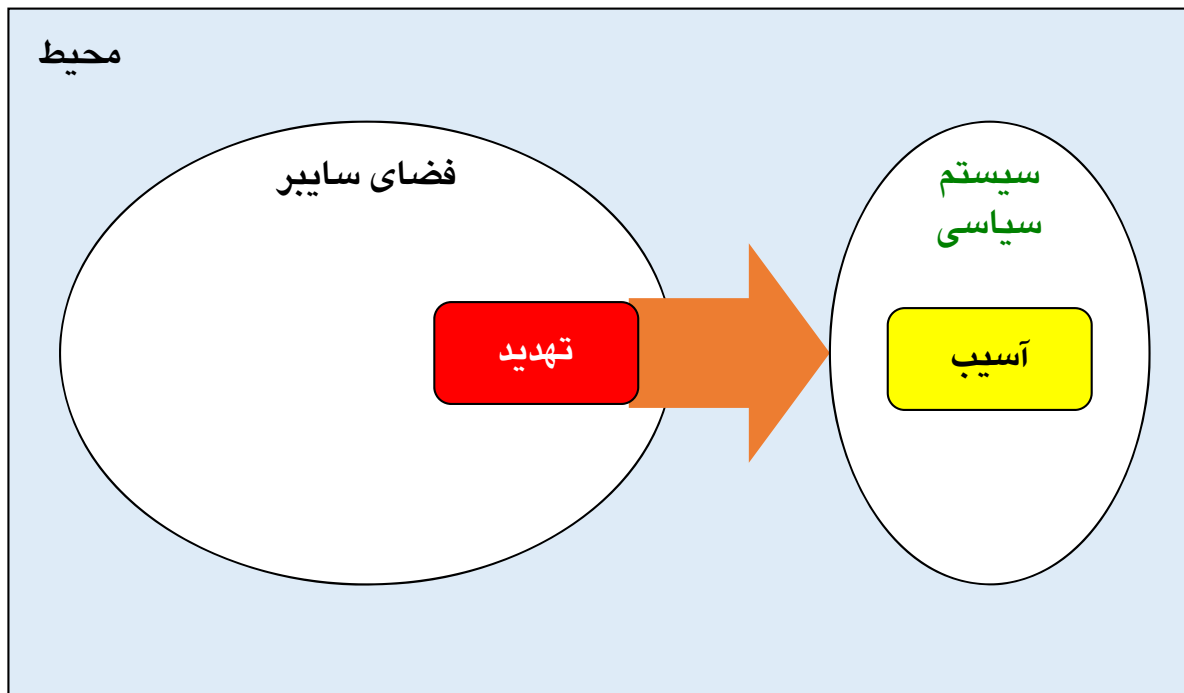
امنیت اجتماعی



امنیت اجتماعی: امنیت سیستم اجتماعی

امنیت متأثر از فضای سایبر

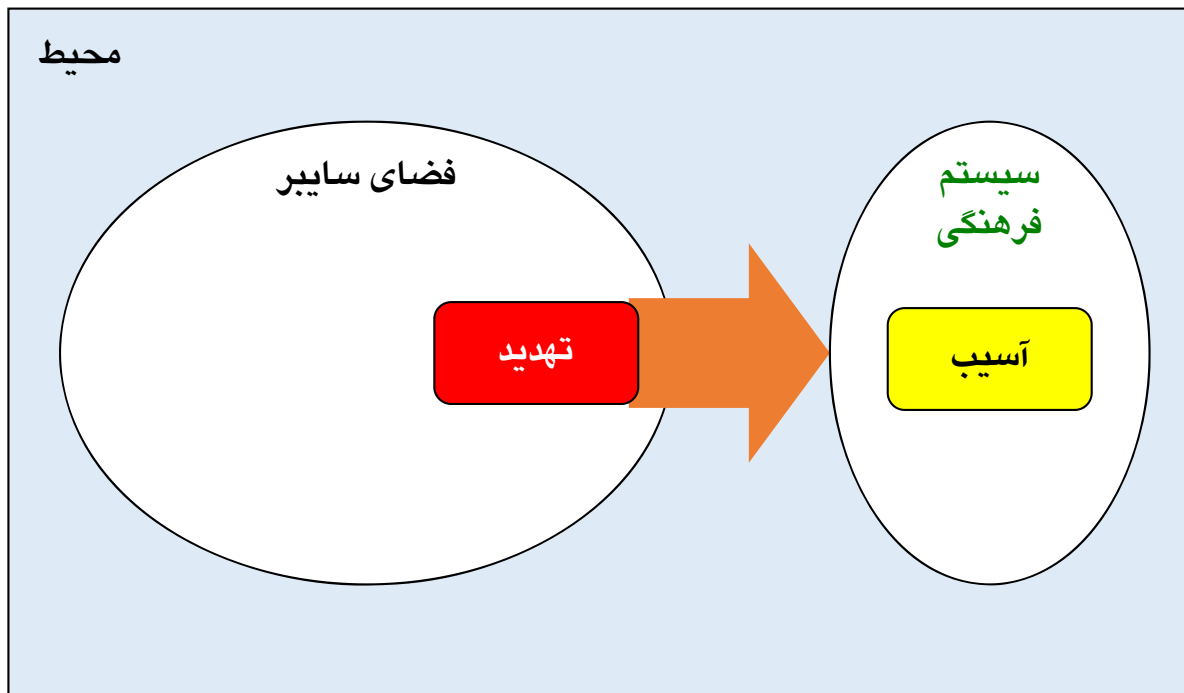
امنیت سیاسی



امنیت سیاسی: امنیت سیستم سیاسی

امنیت متأثر از فضای سایبر

امنیت فرهنگی



امنیت فرهنگی : امنیت سیستم فرهنگی