بسم الله الرحمن الرحیم

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

۱

مقدمه

امنیت

توازن آسیب و تهدید

امنیت حاصل از توازن میان آسیب و تهدید است.

امنیت

آسیب

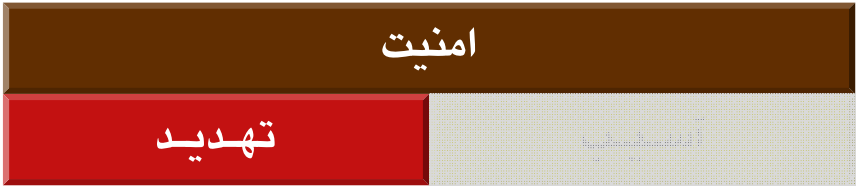
امنیت

آسیب

آسیب، یک پدیده‌ی **درون** سیستم است که ممکن است به‌عنوان نقطه‌ضعف آن استفاده شود.

امنیت

تهدید



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

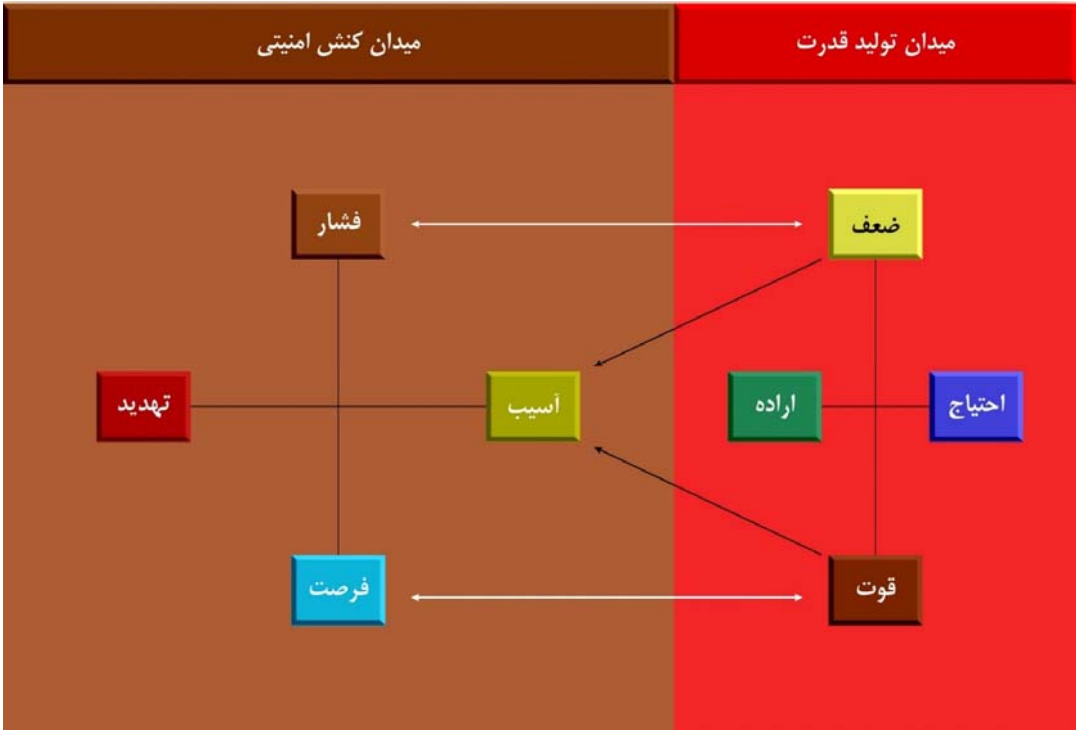
امنیت

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

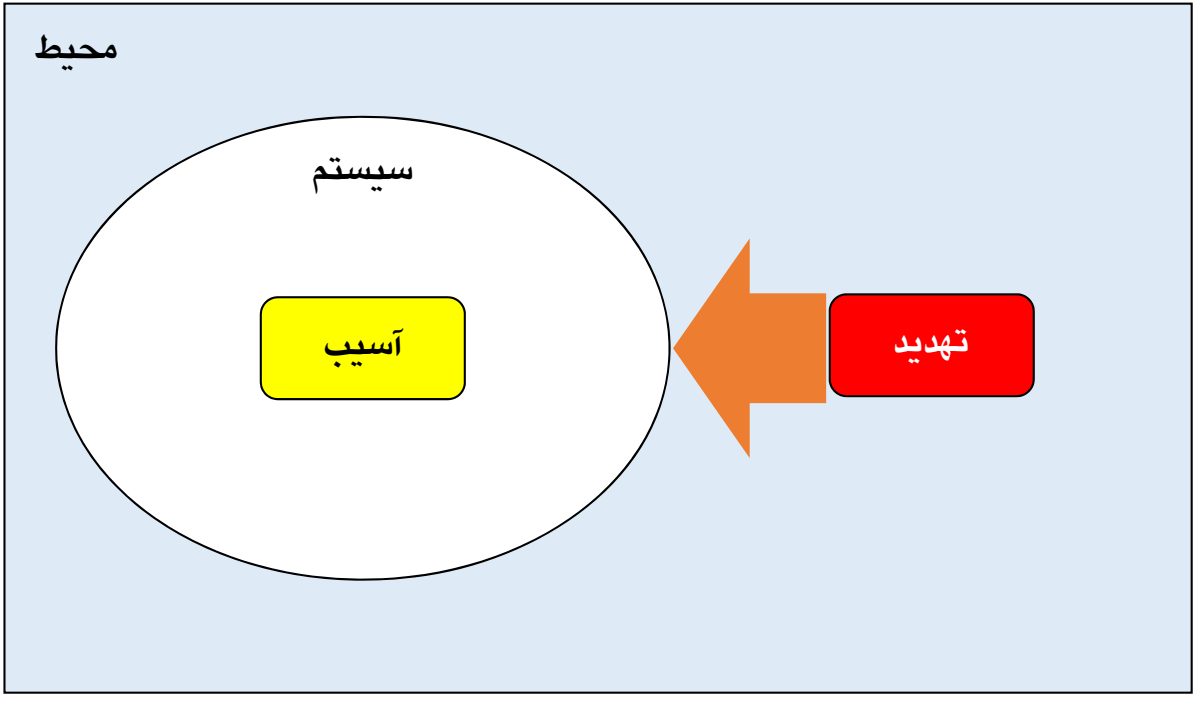
قدرت ارگانیکی		حوزه‌ی قدرت	آماج – میدان عمل		روش	جهت	دکترین قدرت اقدام
			تصرف	سیادت			
	قدرت سخت	نظامی	تصرف سرزمین	——	خشونت	بود و نبود	قهری
			——	سیادت بر اقیانوس – دریا	خشونت	بود و نبود	قهری
			——	سیادت بر فضا – هوا	خشونت	بود و نبود	قهری
	قدرت نیمه سخت	سیاسی اقتصادی اجتماعی	تصرف حکومت	سیادت بر حاکمیت	حذف – رقابت	منفعت نفع و ضرر	تشویقی تنبیهی
			تصرف بازار	سیادت بر منابع اقتصادی	حذف – رقابت	منفعت نفع و ضرر	تشویقی تنبیهی
			تصرف اجتماعی	سیادت بر جامعه	حذف – رقابت	منفعت نفع و ضرر	تشویقی تنبیهی
	قدرت نرم	فرهنگی روانی اطلاعاتی	تصرف قلب ها	——	حب و بغض	ولایت و برائت	ارضایی
			——	سیادت بر مغزها	شک و یقین	حق و باطل	اقناعی

طیف قدرت

بر مبنای سیستم سایبرنتیکی

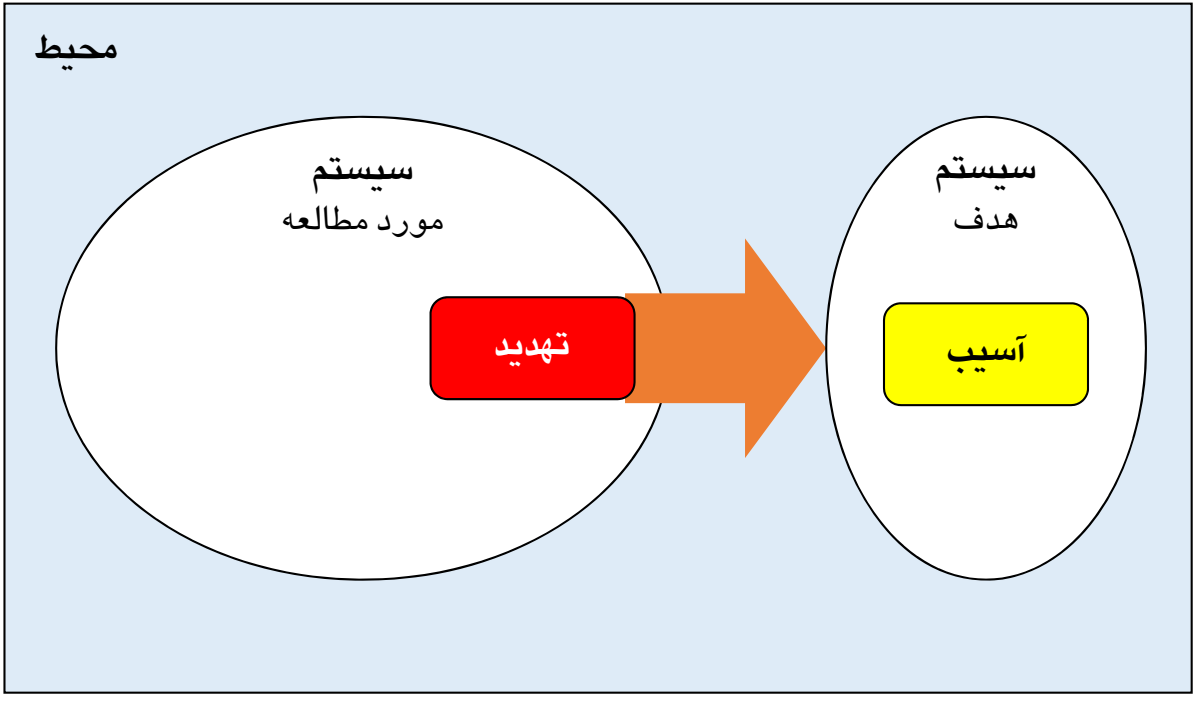
		حوزه‌ی قدرت	میدان عمل - آماج	روش	جهت	دکترین قدرت اقدام
قدرت سایبرنتیکی	قدرت سخت	انرژی	نیرو	تبدیل حالت ماده	سکون یا حرکت	توان یا ناتوانی
	قدرت نیمه سخت	سایبر	کنترل	وابستگی و یکپارچگی	مهار و فرمان	حرکت از قوه به فعل
	قدرت نرم	اطلاعات	آگاهی	گردآوری دسته‌بندی انتشار	دروازه بانی خبر	بی‌اطلاع نگه داشتن یا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

به‌عنوان یک خاصیت غیرکارکردی سیستم

امنیت یک خاصیت غیرکارکردی یک سیستم است.

یعنی یک جزء سیستمی متولی تولید و حفظ آن نیست

بلکه کل سیستم به‌مثابه یک کل واجد این خاصیت می‌شود.

نظریه‌های امنیت ذیل نظریه‌ی سیستم‌ها تعریف می‌شوند.

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

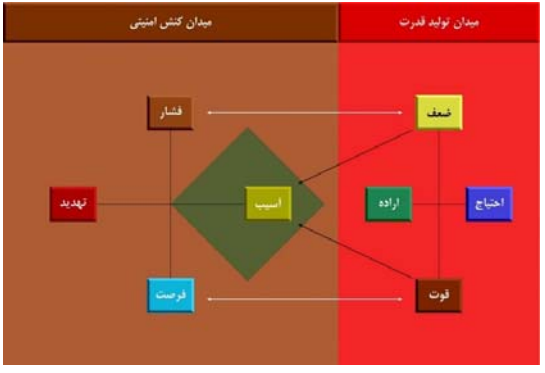
امنیت حاصل از توازن میان آسیب و تهدید است.

چگونگی ایجاد این توازن، مکاتب مختلف امنیتی را پدید می‌آورد.

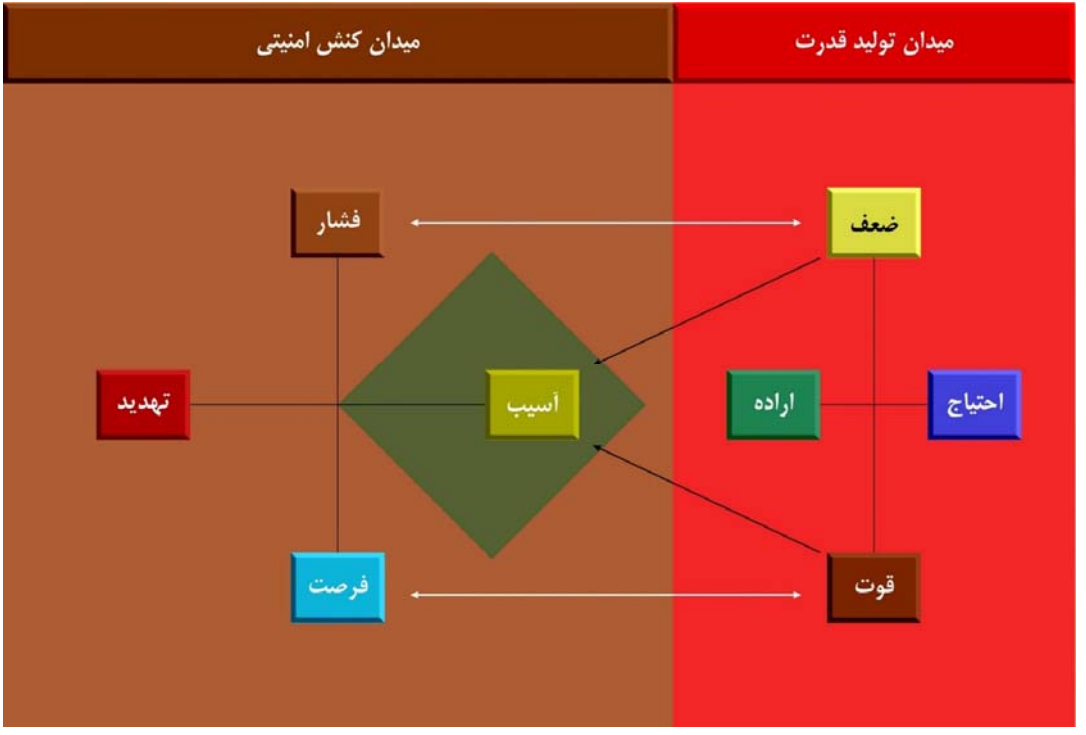
مکتب آسیب‌محور

دکترین مکتب امنیتی آسیب‌محور

باید آسیب‌ها را پوشش داد.



مکتب آسیب‌محور

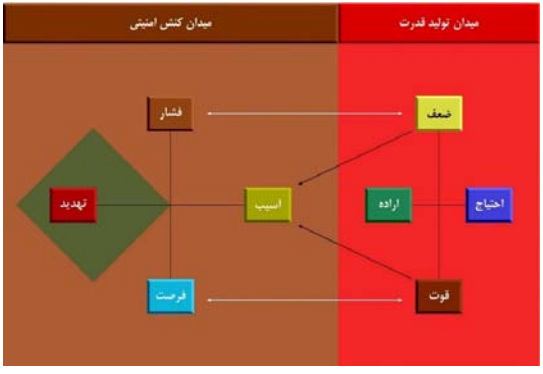


در این مکتب، مبتنی بر نقاط قوت سیستم، اصالت با تلاش برای پوشاندن آسیب است نه از میان برداشتن تهدید.

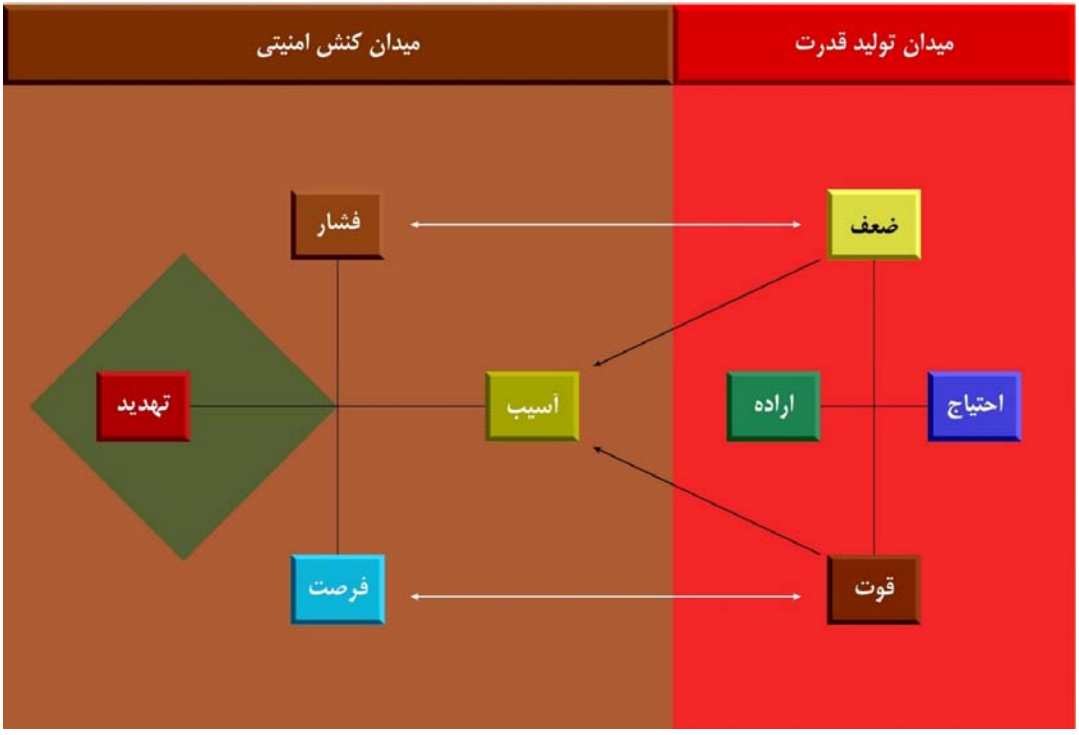
مکتب تهدیدمحور

دکترین مکتب امنیتی تهدیدمحور

باید تهدید را از منشأ نابود کرد.



مکتب تهدیدمحور

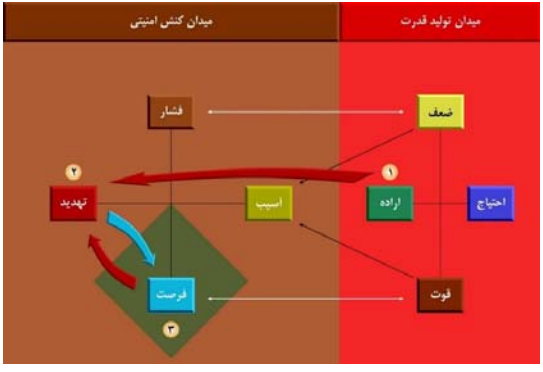


در این مکتب، امکان کاهش آسیب از درون وجود ندارد، بلکه باید تهدید را در بیرون خنثی کرد.

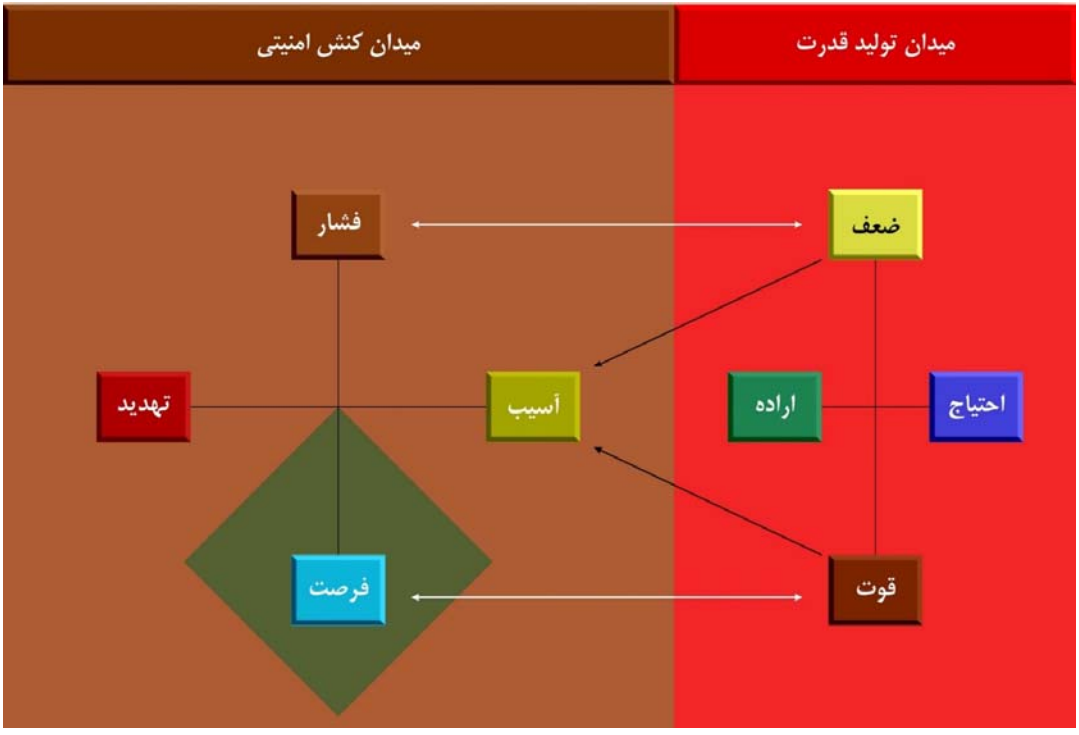
مکتب فرصت‌طلب

دکترین مکتب امنیتی فرصت‌طلب

باید تهدید را به فرصت تبدیل کرد.



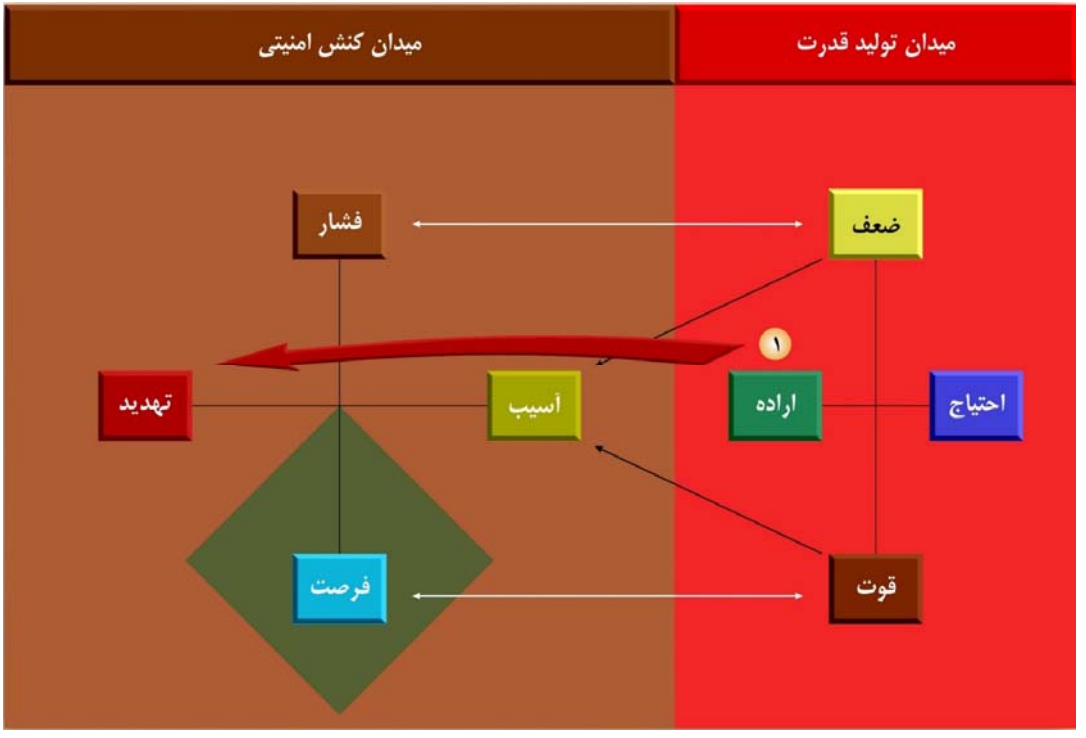
مکتب فرصت‌طلب



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

مکتب فرصت‌طلب

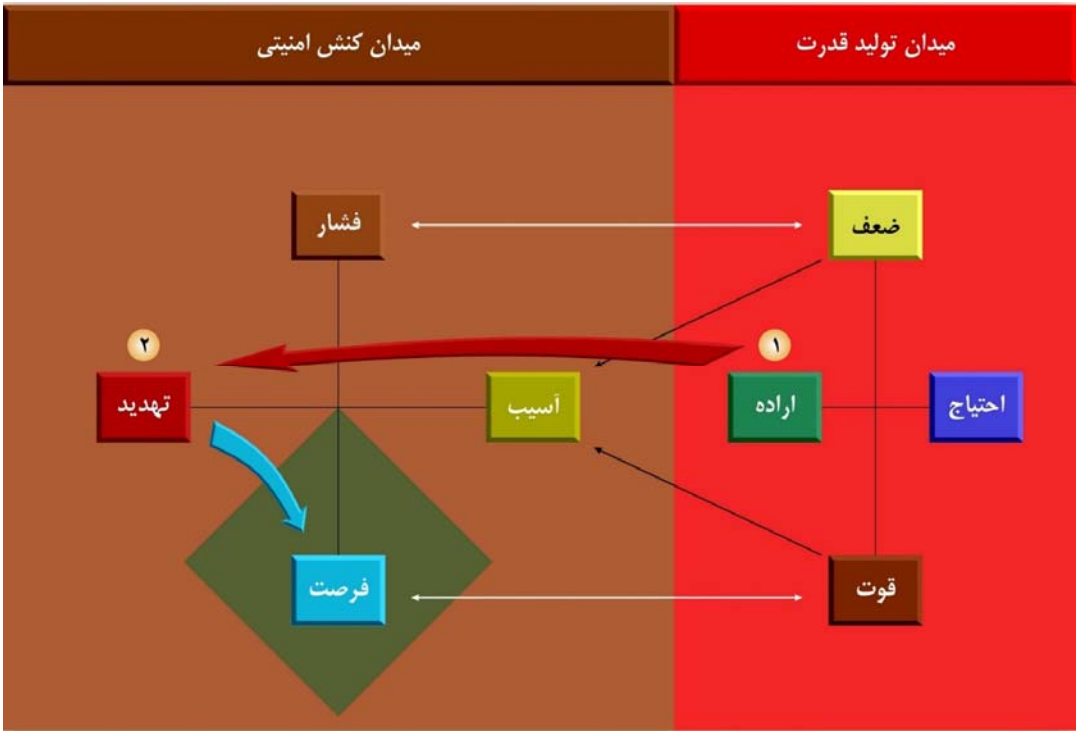
گام یکم پروژه در مکتب امنیتی فرصت‌طلب: تولید تهدید



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

مکتب فرصت‌طلب

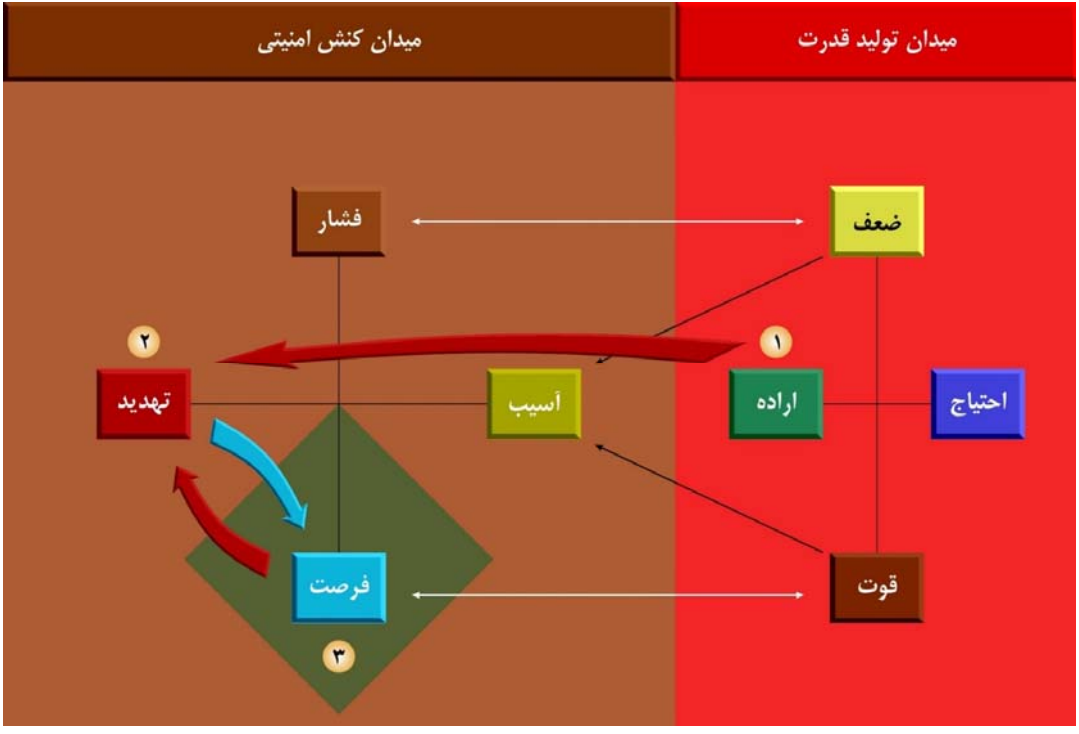
گام دوم پروژه در مکتب امنیتی فرصت‌طلب: تبدیل تهدید به فرصت



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

مکتب فرصت‌طلب

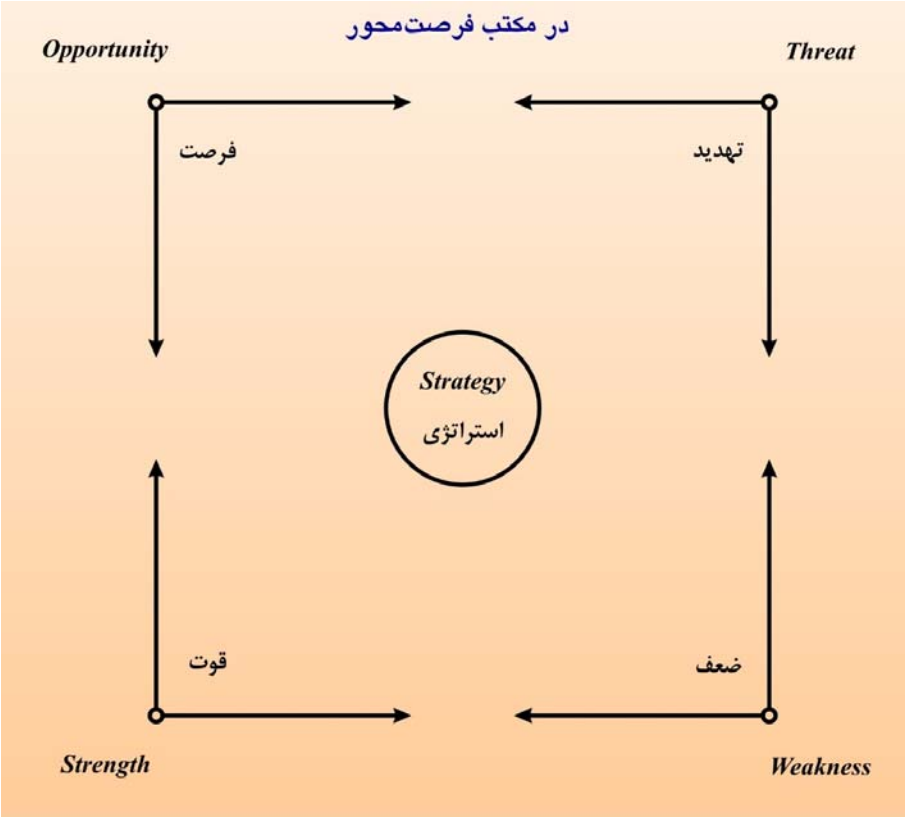
گام سوم پروژه در مکتب امنیتی فرصت‌طلب: خنثی شدن تهدید



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

مکتب فرصت‌طلب

تحلیل SWOT

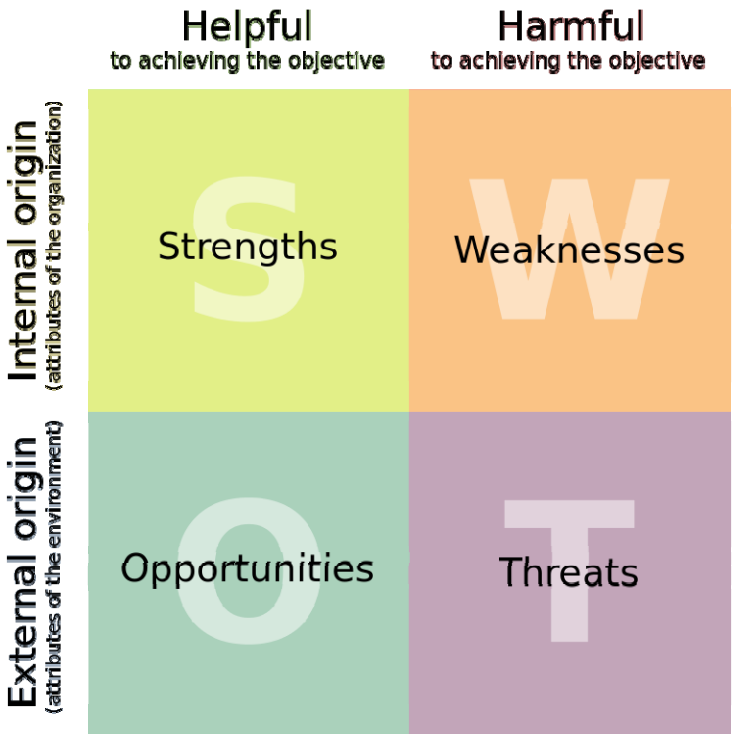



Threats
Opportunities


Threat
Opportunity


Threat
Opportunity

SWOT ANALYSIS



SWOT ANALYSIS

Internal		External	
Strengths	Weaknesses	Opportunities	Threats

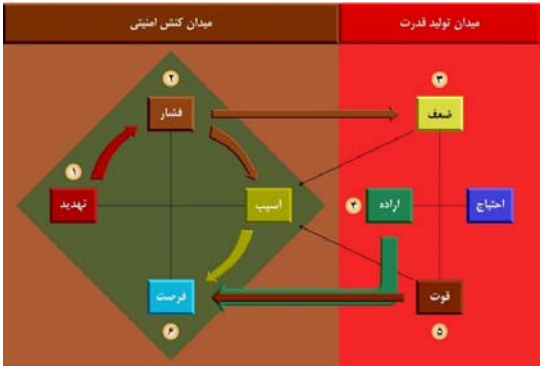
SWOT ANALYSIS

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

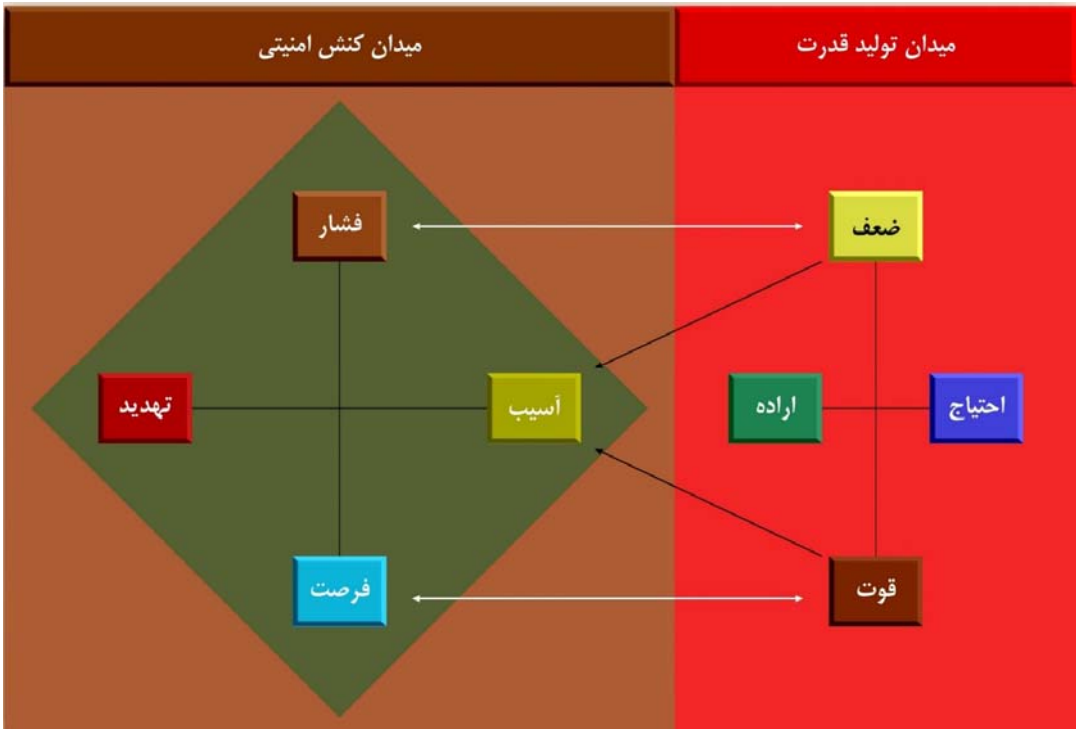
مکتب موقعیت‌طلب

دکترین مکتب امنیتی موقعیت‌طلب

باید از تهدید موقعیت متعالی به‌دست آورد.



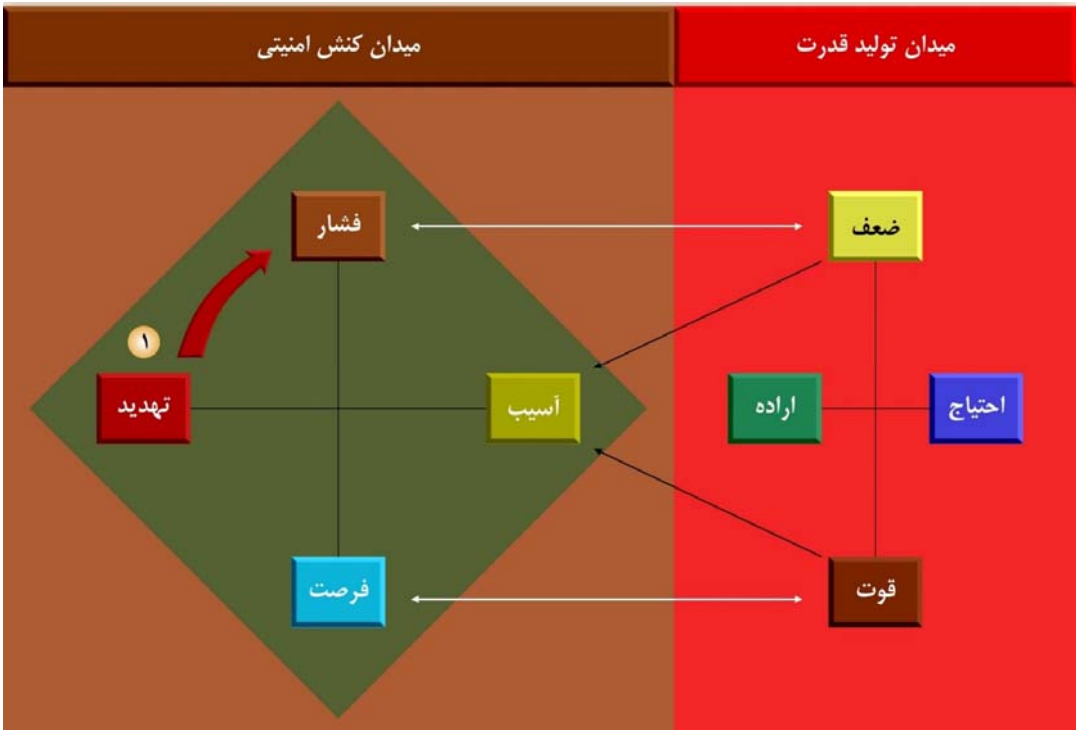
مکتب موقعیت‌طلب



در این مکتب، امنیت از طریق تبیین تهدید، و مصادره و هضم آن برای ایجاد موقعیت متعالی‌تر سیستم شکل می‌گیرد.

مکتب موقعیت‌طلب

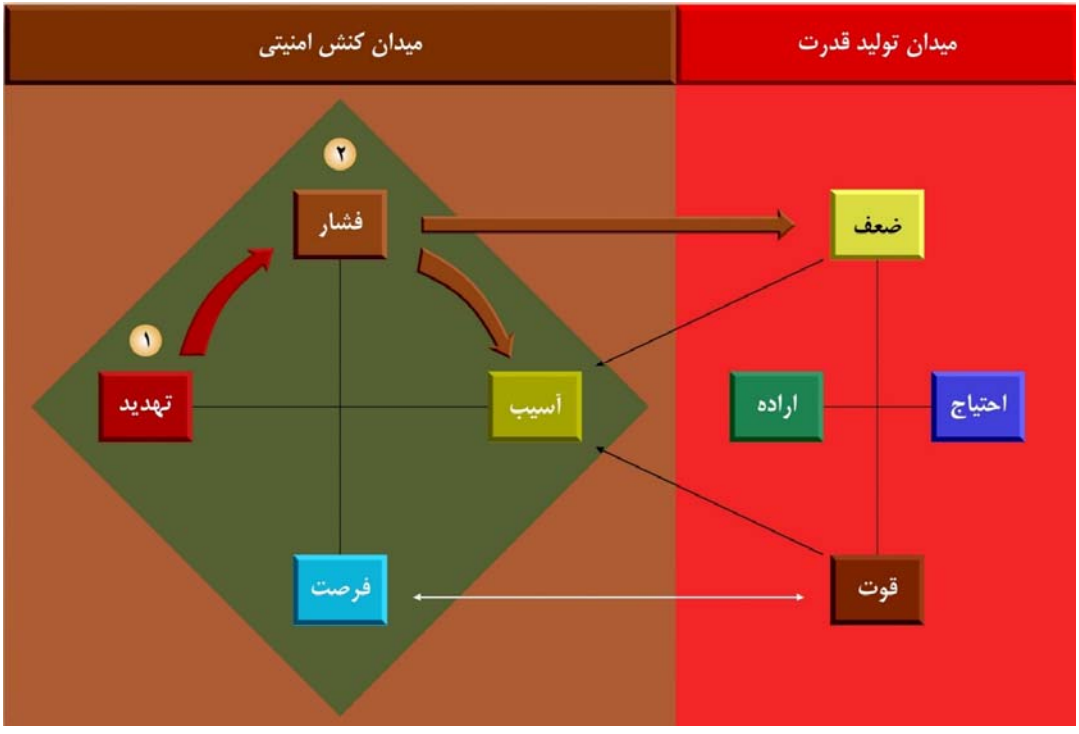
گام اول پروسه در مکتب امنیتی موقعیت‌طلب: روند اعمال تهدید



۱) در میدان کنشی امنیتی، **تهدیدی** به‌وجود می‌آید.

مکتب موقعیت‌طلب

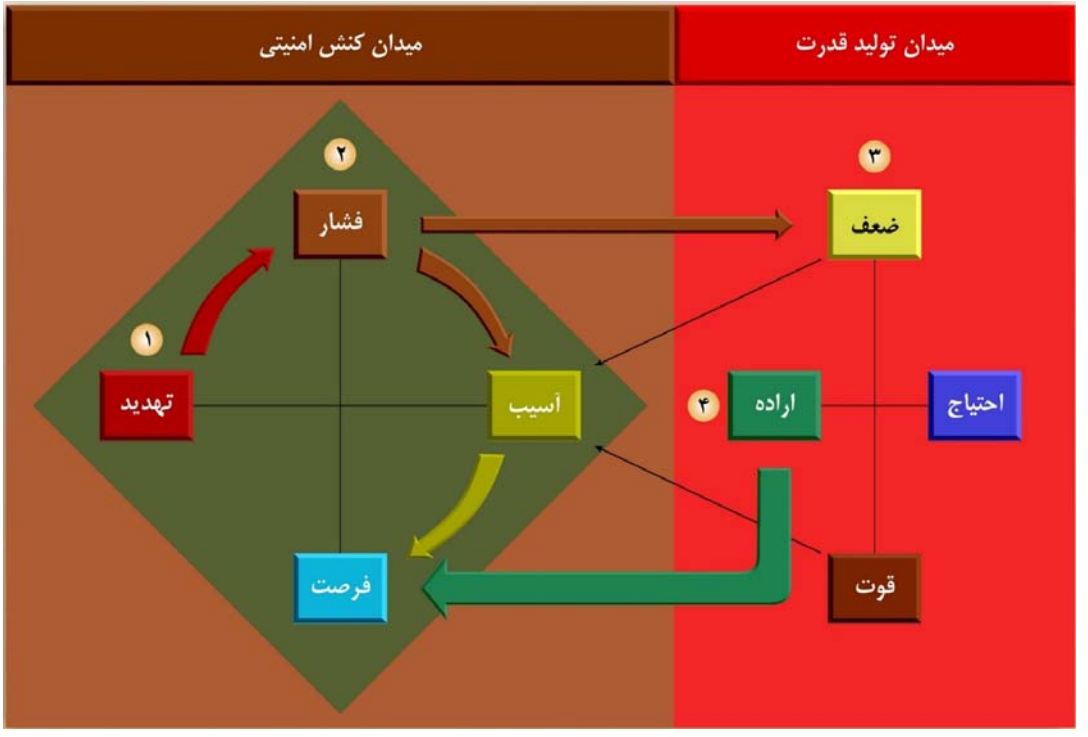
گام دوم پروسه در مکتب امنیتی موقعیت‌طلب: روند اعمال فشار



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

مکتب موقعیت‌طلب

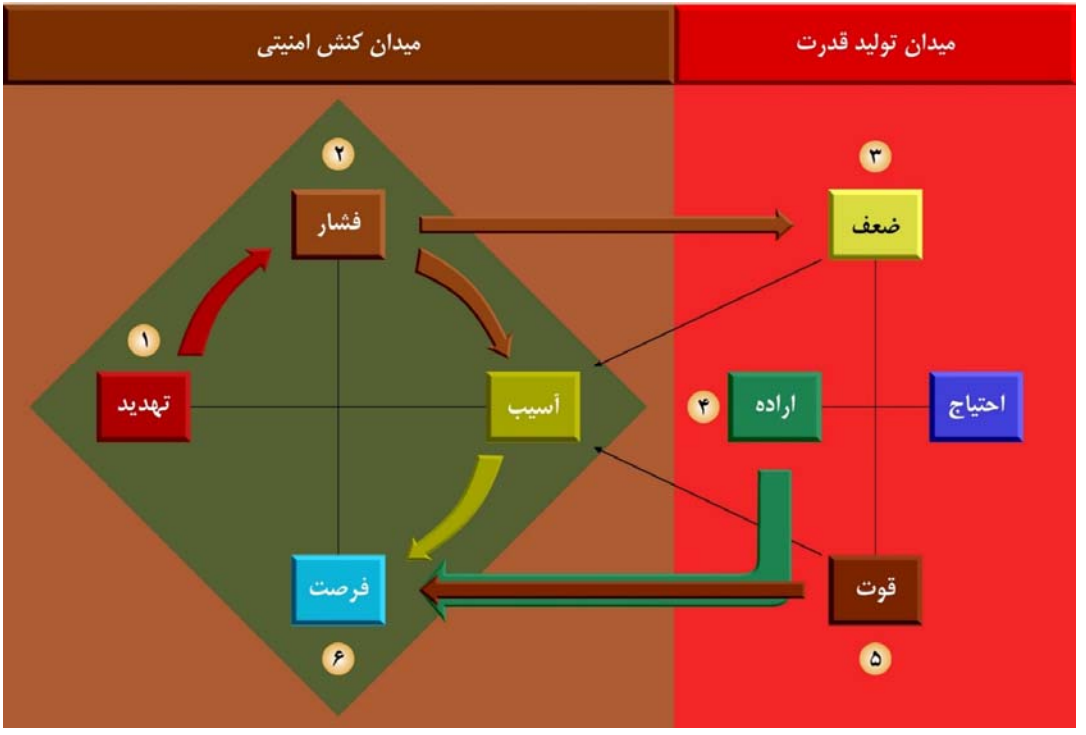
گام سوم پروسه در مکتب امنیتی موقعیت‌طلب: روند اعمال اراده



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

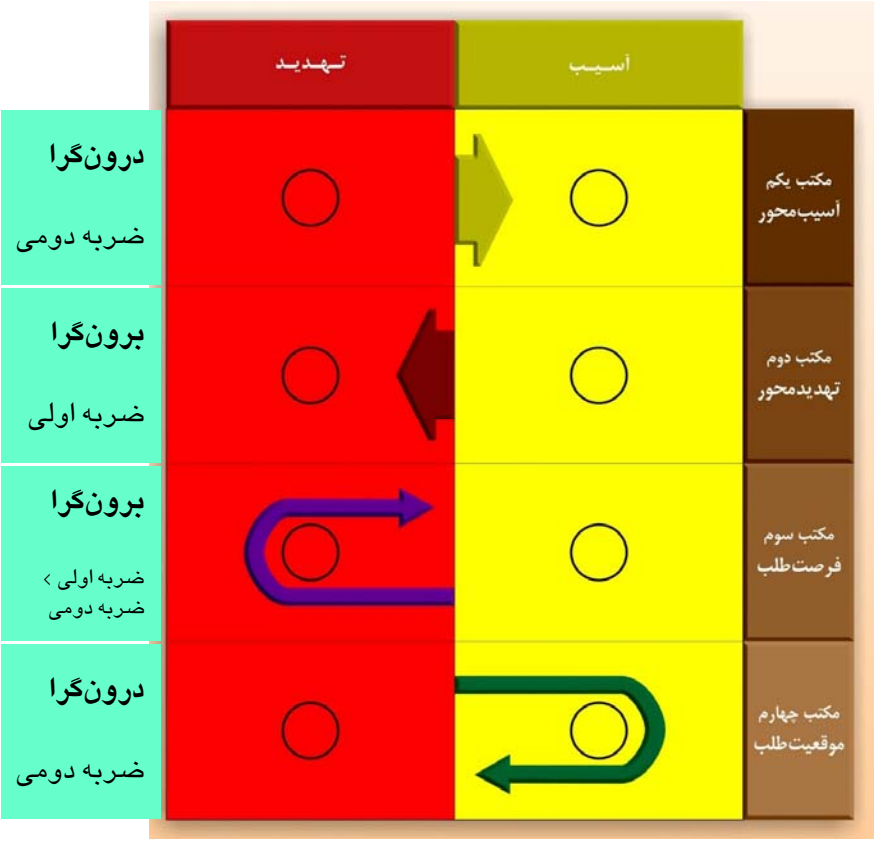
مکتب موقعیت‌طلب

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



۴) قوت و توانایی ذاتی سیستم، سبب می‌شود 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

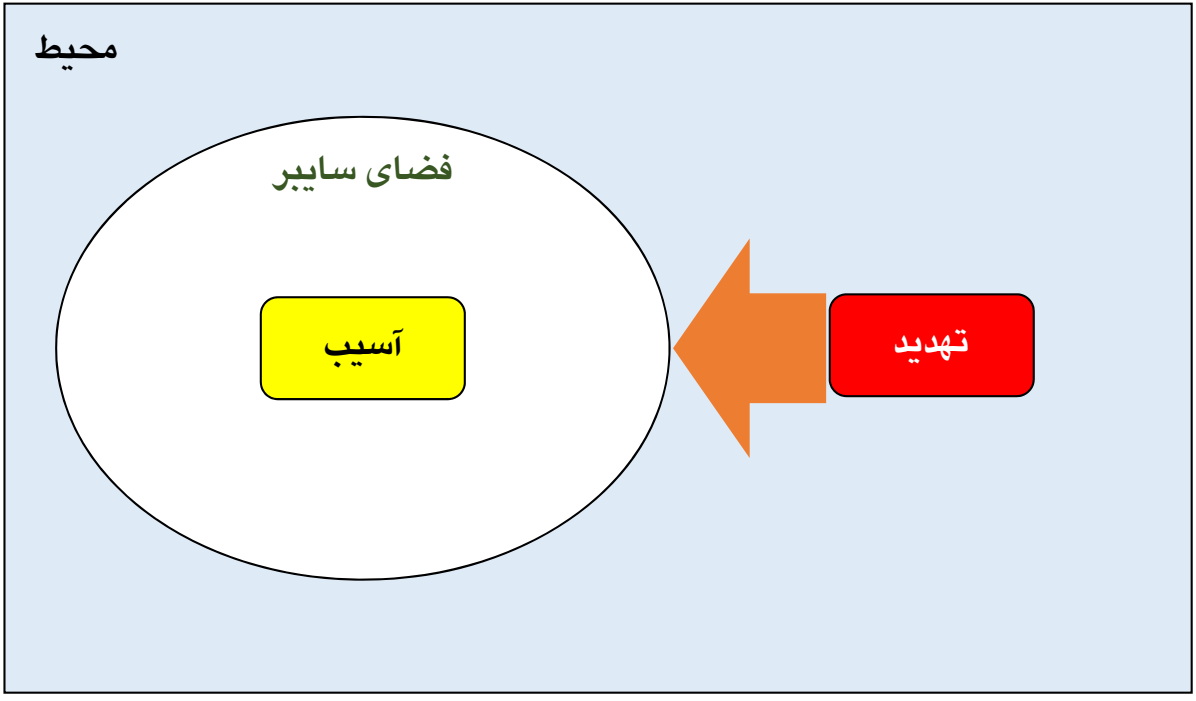
	آسیب	تهدید
مکتب اول آسیب محور	باید آسیب‌ها را پوشش داد.	باید جلو پوشش آسیب پذیری‌های دشمن را گرفت.
مکتب دوم تهدید محور	باید تهدیدها را از منشاء نابود کرد.	به نیت نابودی دشمن، باید تهدیدی جدی علیه او شد.
مکتب سوم فرصت طلب	باید تهدیدها رابه فرصت تبدیل کرد.	نباید اجازه داد دشمن، تهدید بودن ما را به فرصت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

فضای سایبر و امنیت

۳

امنیت فضای سایبر

امنیت فضای سایبر

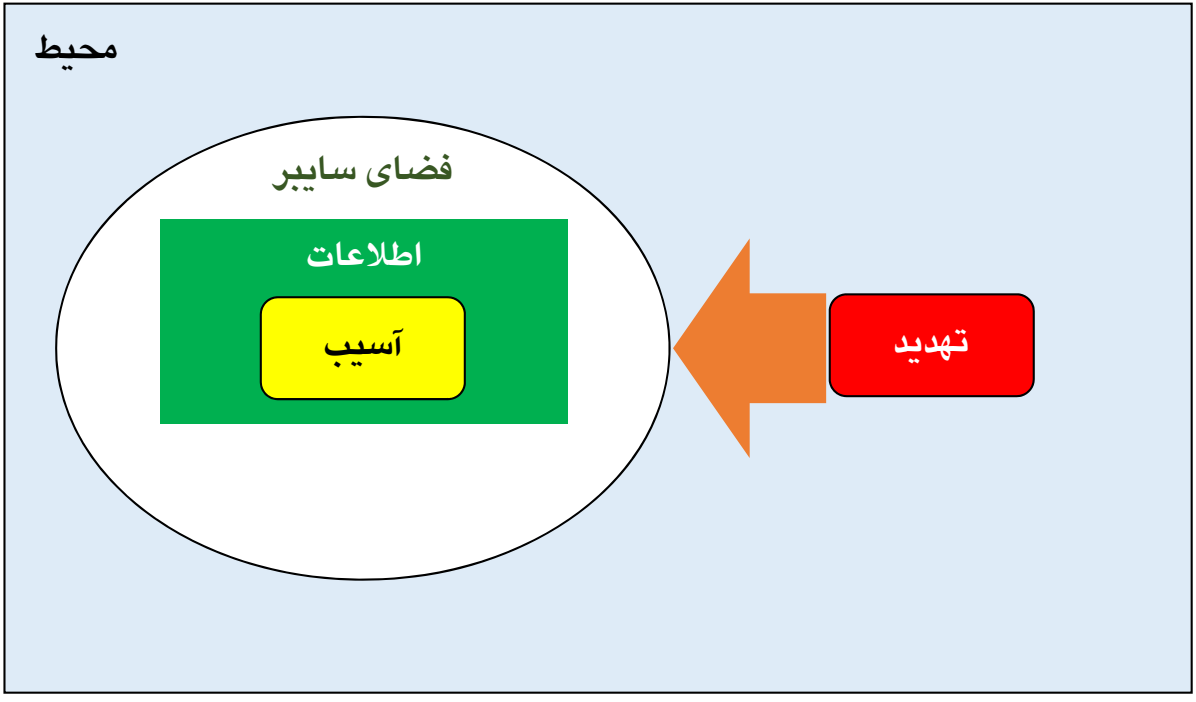


مسئله، امنیت خود زیرساخت و کاربرد فضای سایبر است.

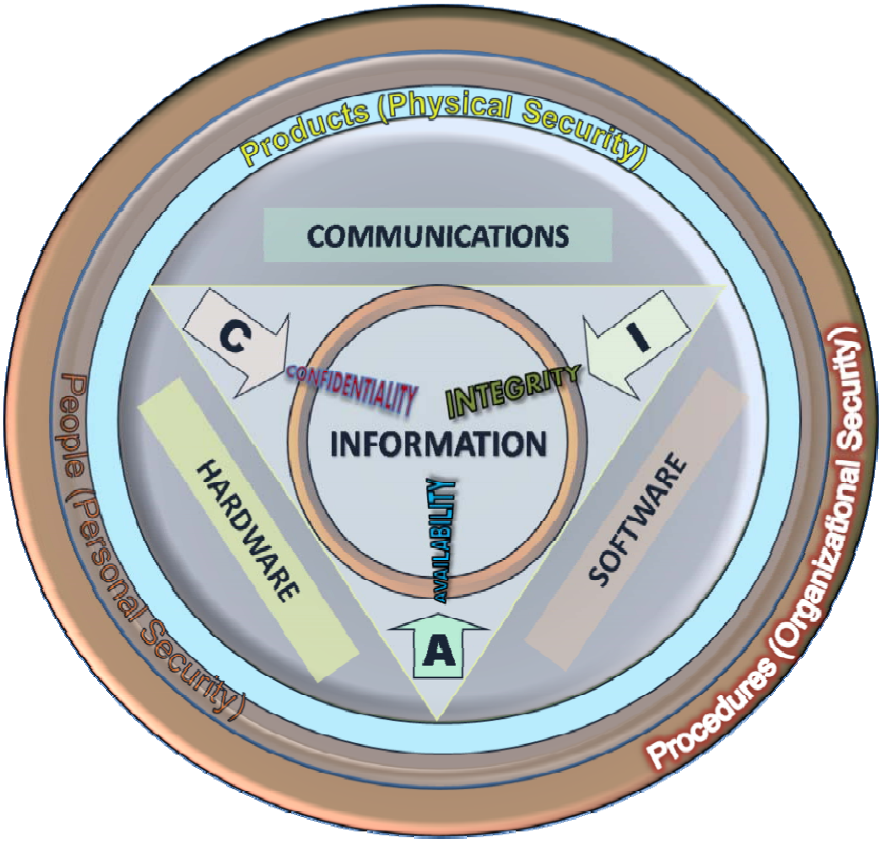
امنیت زیرساخت و کاربرد فضای سایبر

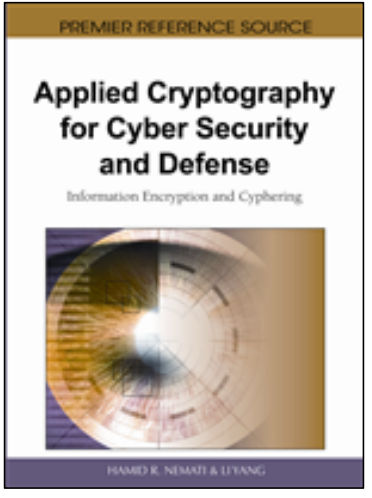
امنیت فضای سایبر

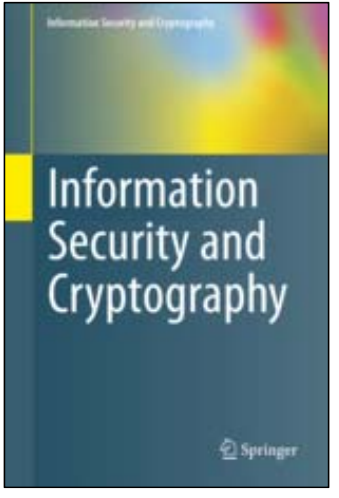
امنیت اطلاعات



امنیت لایه‌ی اطلاعات

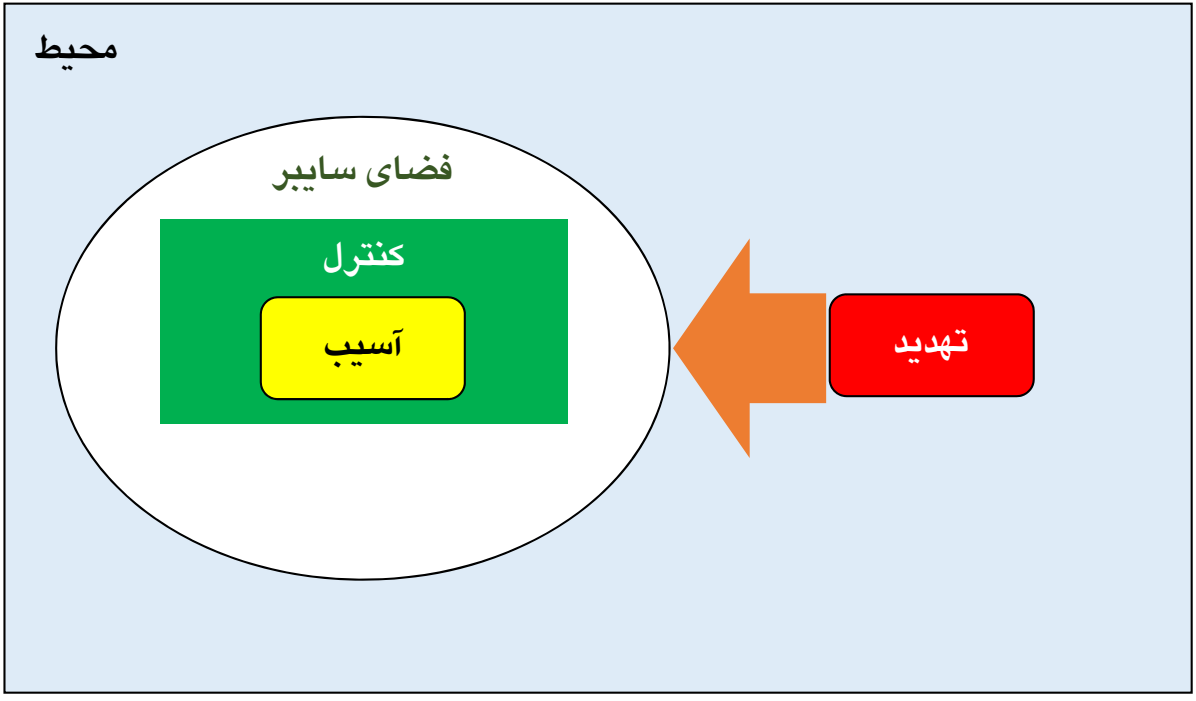

Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
AVAILABILITY
A
HARDWARE
SOFTWARE
People (Personal Security)
Procedures (Organizational Security)


PREMIER REFERENCE SOURCE
Applied Cryptography for Cyber Security and Defense
Information Encryption and Cyphering
HAMID R. NEMATI & LI YANG


Information Security and Cryptography
Springer

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

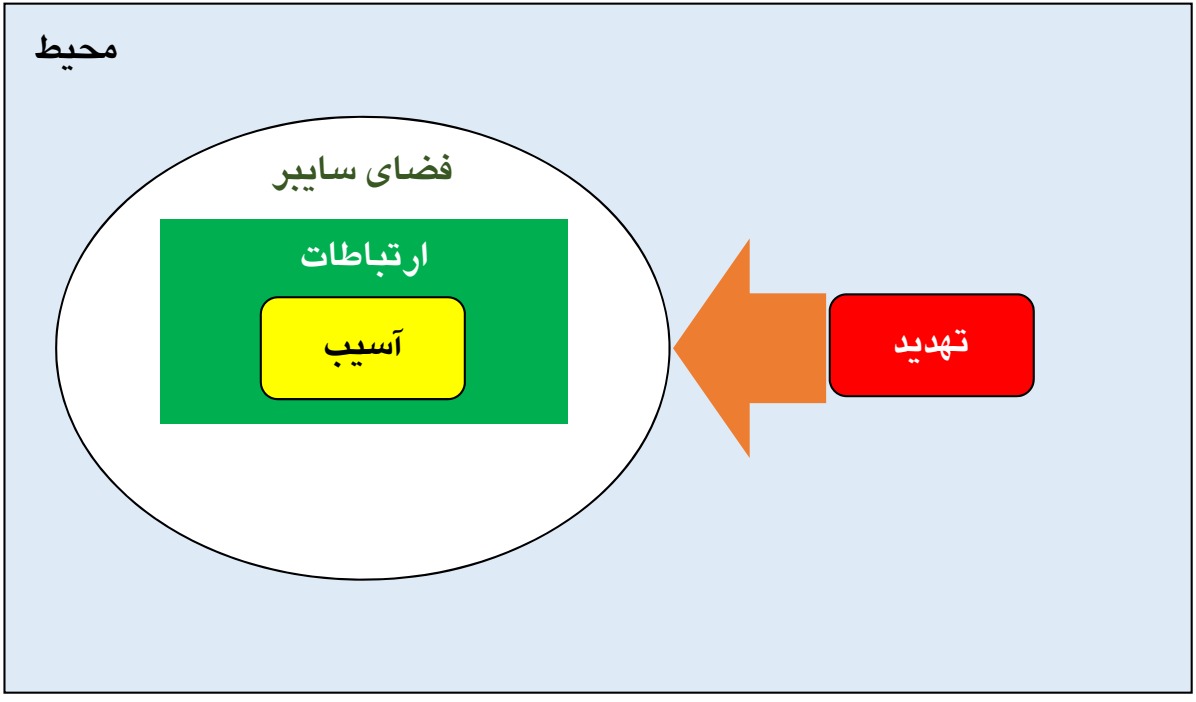
Security

- 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.

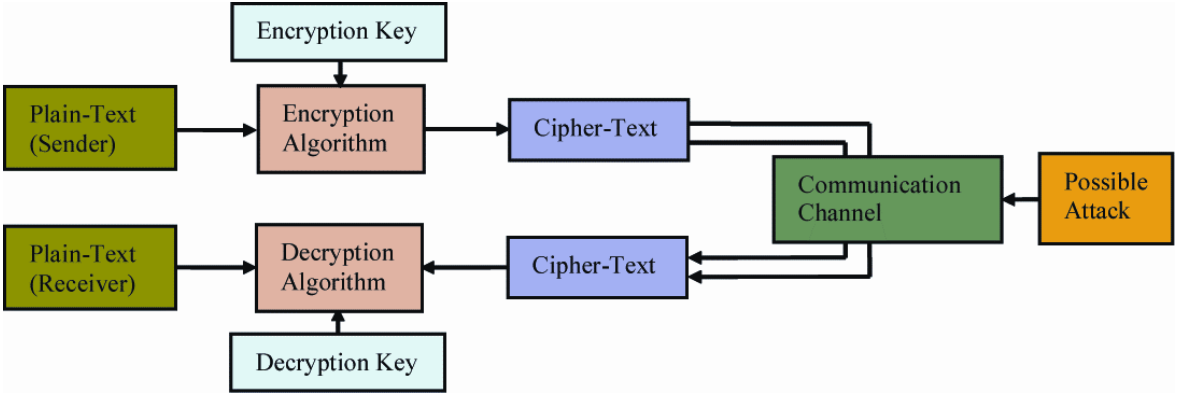
- The physical security of the system is essential. Threats can come through the Web, but they can also come from a physical terminal. Even if the Web access is very secure, if an attacker obtains physical access to a server, breaking into a system is much easier.

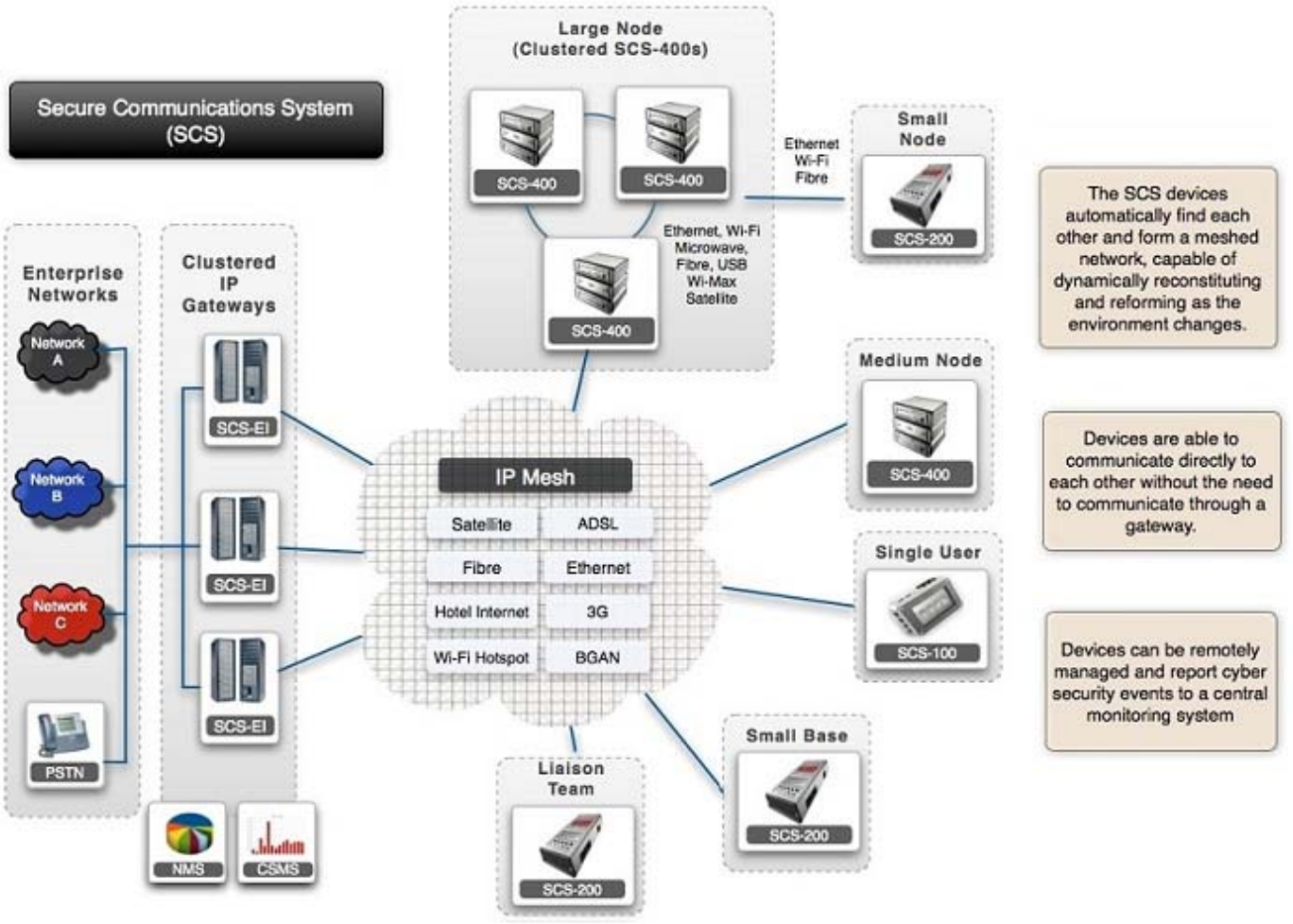
امنیت فضای سایبر

امنیت ارتباطات



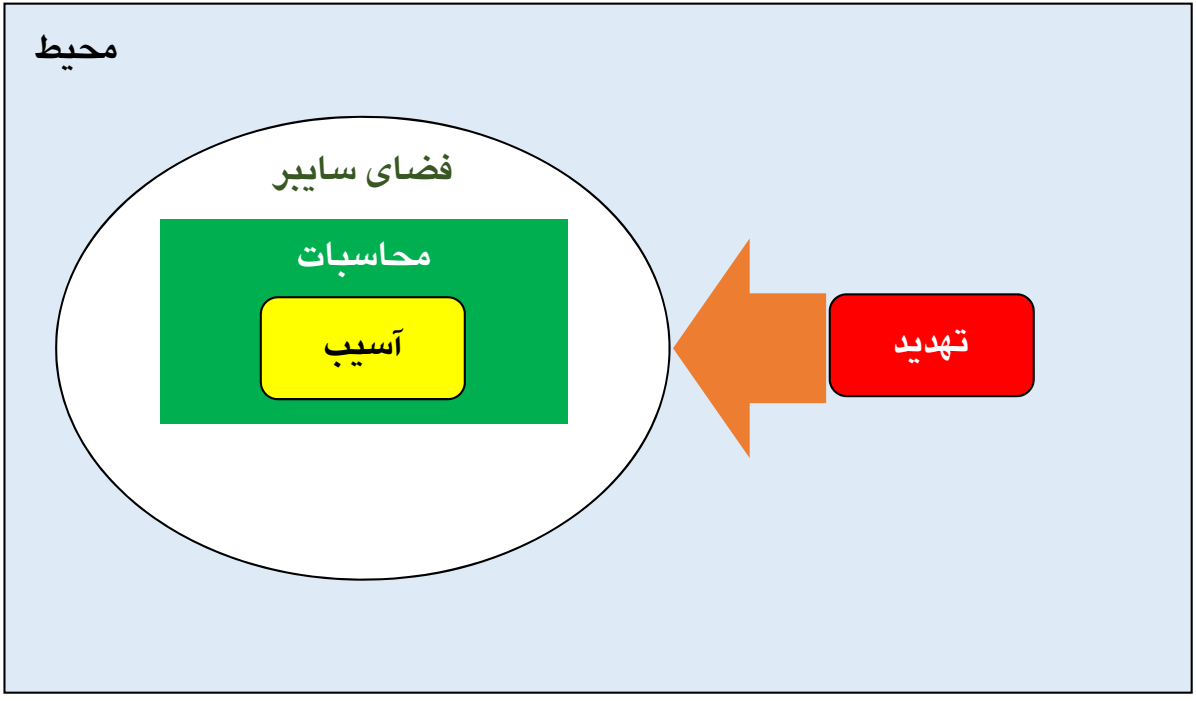
امنیت لایه‌ی ارتباطات


Encryption Key
Plain-Text (Sender)
Encryption Algorithm
Cipher-Text
Communication Channel
Possible Attack
Plain-Text (Receiver)
Decryption Algorithm
Cipher-Text
Decryption Key


Secure Communications System (SCS)
Large Node (Clustered SCS-400s)
SCS-400
SCS-400
SCS-400
Ethernet Wi-Fi Fibre
Small Node
SCS-200
Ethernet, Wi-Fi Microwave, Fibre, USB Wi-Max Satellite
Enterprise Networks
Network A
Network B
Network C
PSTN
Clustered IP Gateways
SCS-EI
SCS-EI
SCS-EI
NMS
CSMS
IP Mesh
Satellite
ADSL
Fibre
Ethernet
Hotel Internet
3G
Wi-Fi Hotspot
BGAN
Medium Node
SCS-400
Single User
SCS-100
Small Base
SCS-200
Liaison Team
SCS-200
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

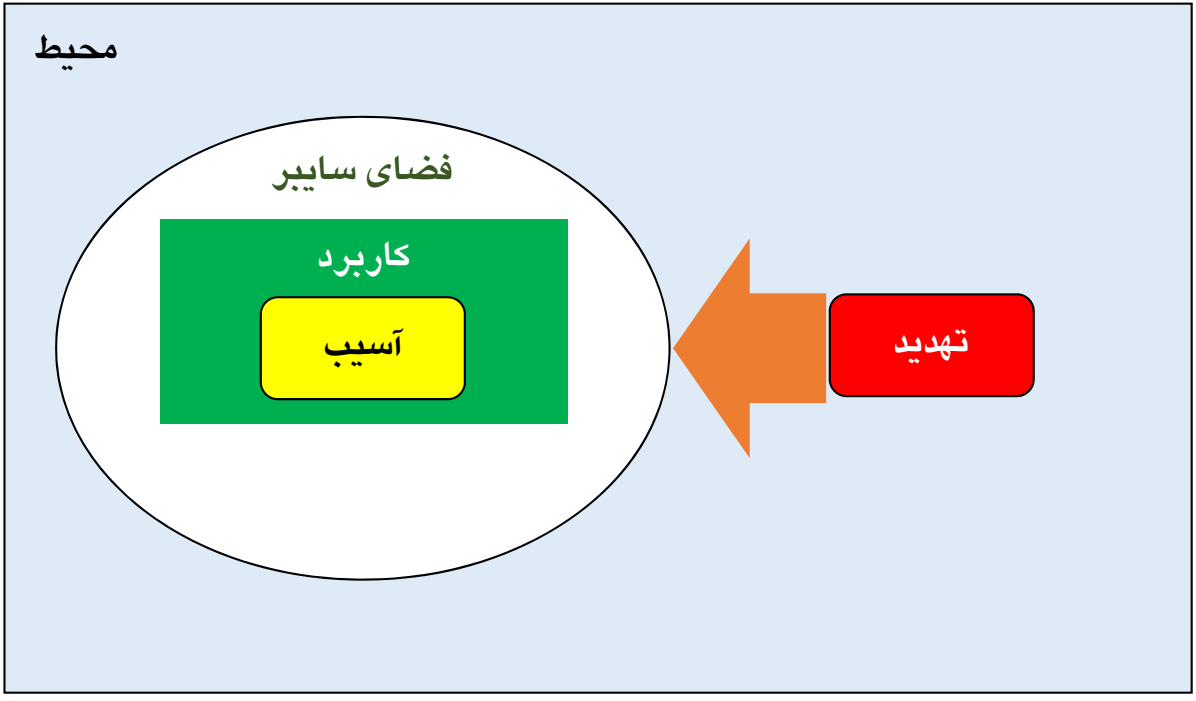


امنیت لایه‌ی محاسبات

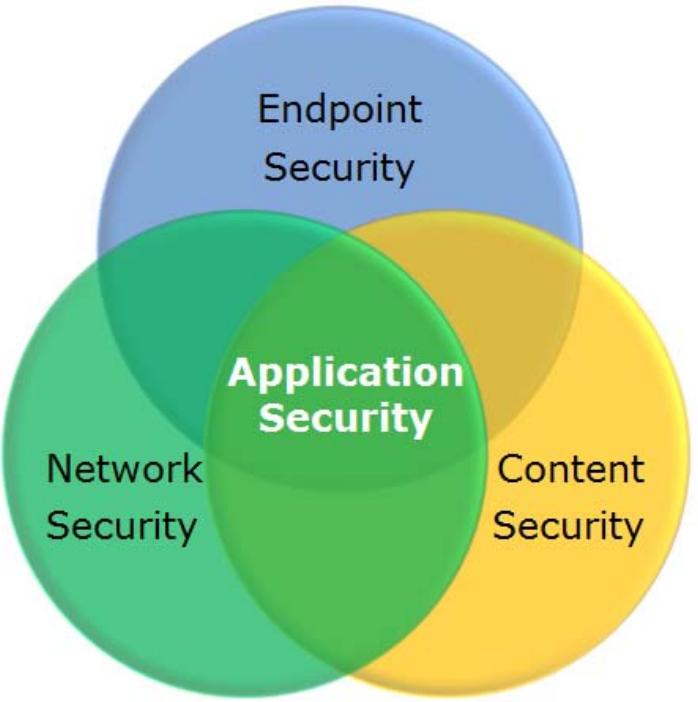
Ninh V. Nguyen
ninh.nv@gmail.com

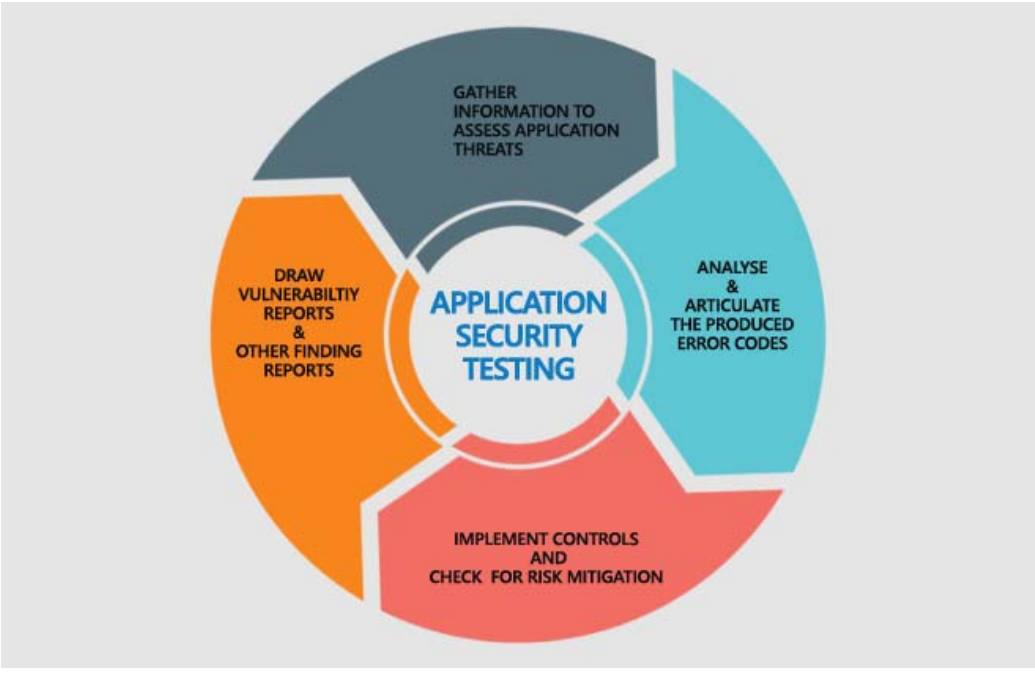
امنیت فضای سایبر

امنیت کاربرد

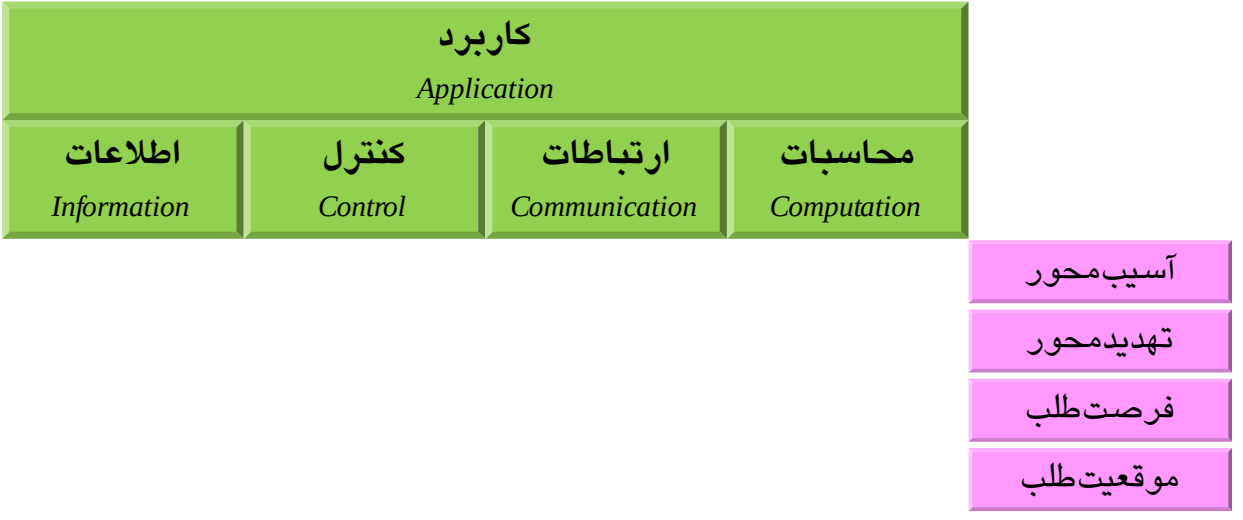


امنیت لایه‌ی کاربرد


Endpoint
Security
Application
Security
Network
Security
Content
Security


GATHER INFORMATION TO ASSESS APPLICATION THREATS
ANALYSE & ARTICULATE THE PRODUCED ERROR CODES
IMPLEMENT CONTROLS AND CHECK FOR RISK MITIGATION
DRAW VULNERABILTIY REPORTS & OTHER FINDING REPORTS
APPLICATION SECURITY TESTING

امنیت فضای سایبر با در نظر گرفتن مکاتب امنیتی



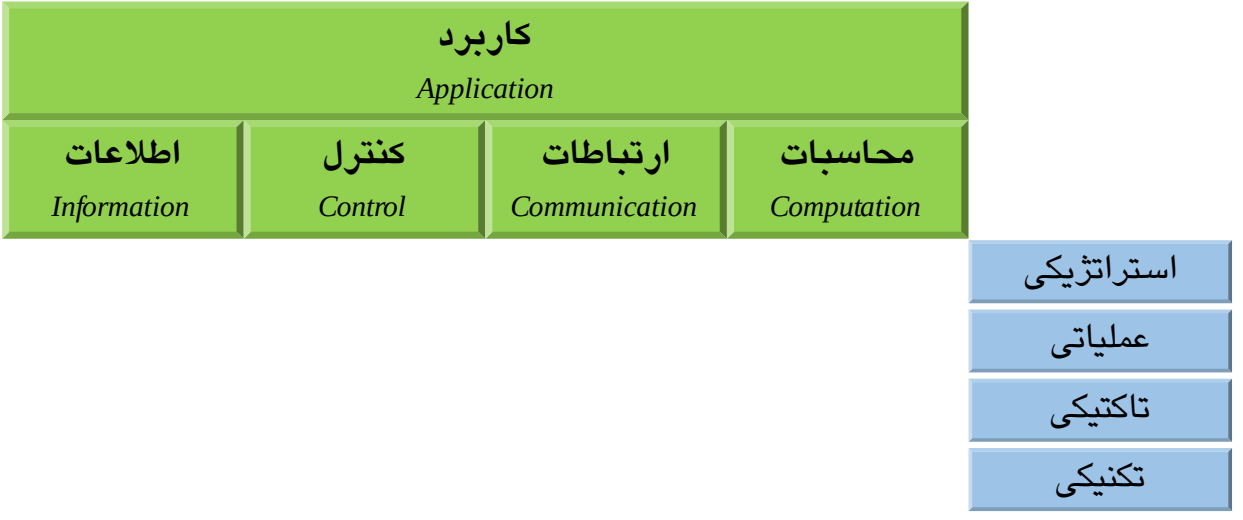
مثال:

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.

شماره: ۲-۴	**آسیب:** **احراز هویت در پروتکل EIGRP هنگام ایجاد عبارت MD5 تنها بخش‌های خاصی از بسته را در نظر می‌گیرد.**	**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.**
استراتژی امنیت با مکتب آسیب محور	پوشش دادن تمام بخش‌های بسته EIGRP در احراز هویت و همچنین امضای بسته‌ها با استفاده از روش MAC	
استراتژی امنیت با مکتب تهدید محور	طراحی و پیاده‌سازی سیاست‌های امنیت فیزیکی و اعمال کنترل دسترسی دقیق	
استراتژی امنیت با مکتب فرصت 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 موقعیت 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	

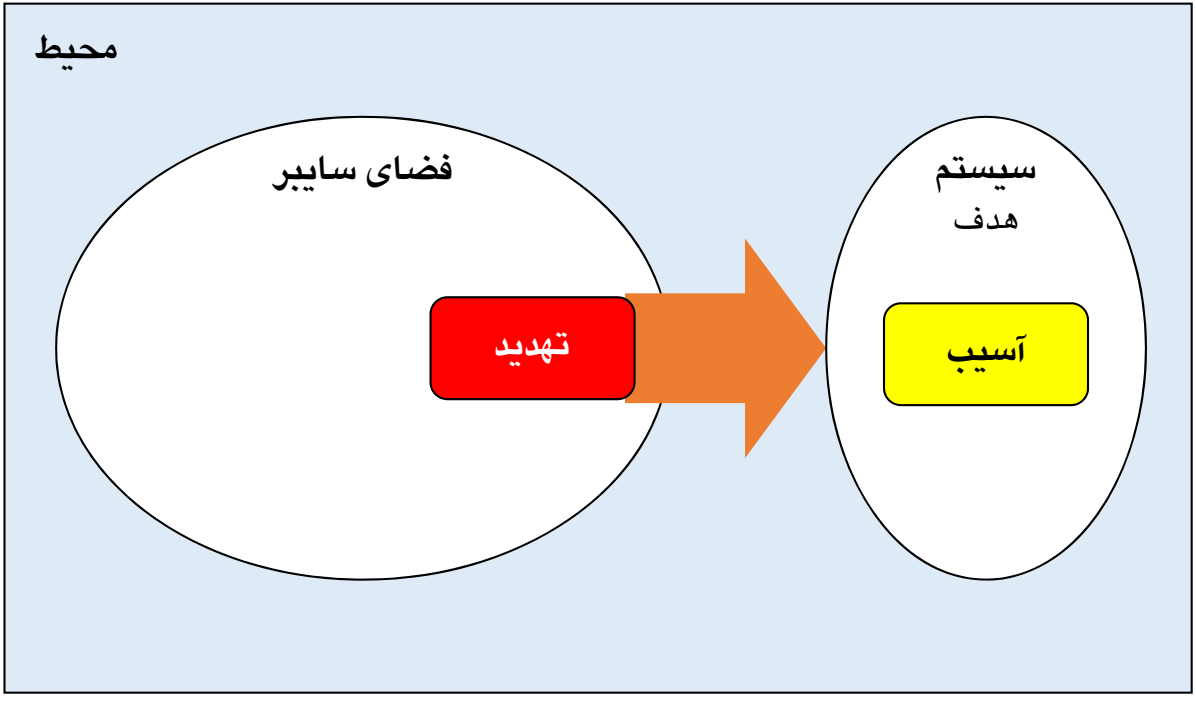
امنیت فضای سایبر با در نظر گرفتن سطوح اقدام



۴

امنیت متأثر از فضای سایبر

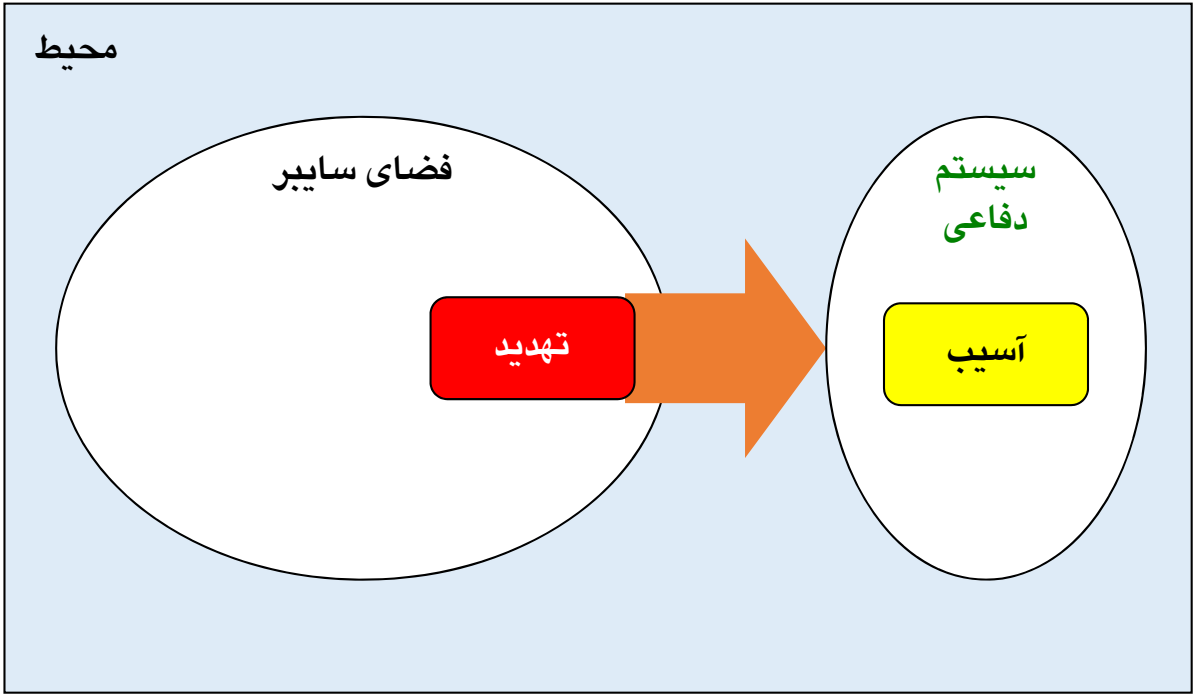
امنیت متأثر از فضای سایبر



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

امنیت متأثر از فضای سایبر

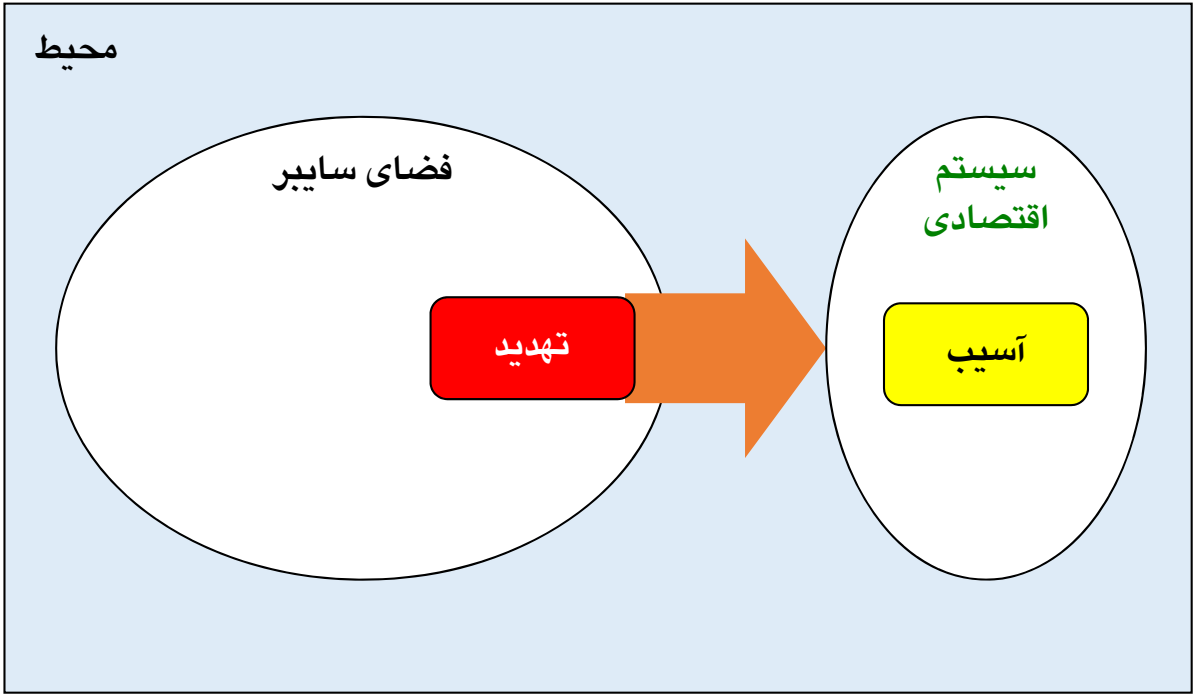
امنیت دفاعی



امنیت دفاعی: امنیت سیستم دفاعی

امنیت متأثر از فضای سایبر

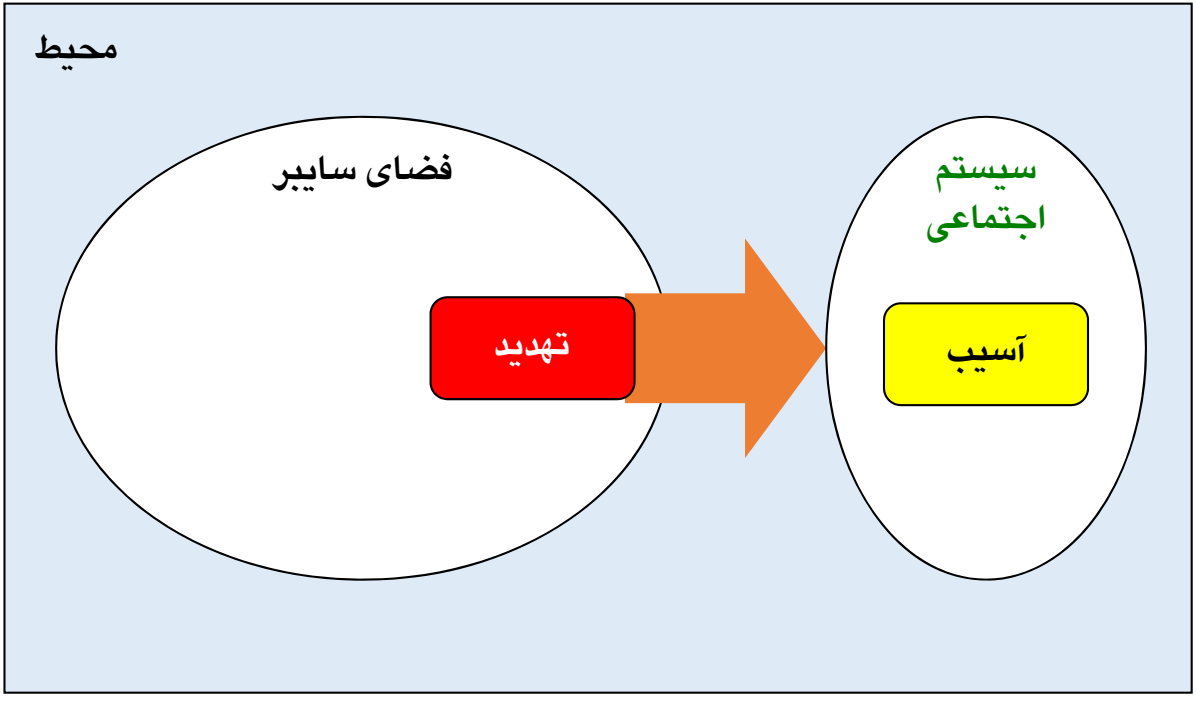
امنیت اقتصادی



امنیت اقتصادی: امنیت سیستم اقتصادی

امنیت متأثر از فضای سایبر

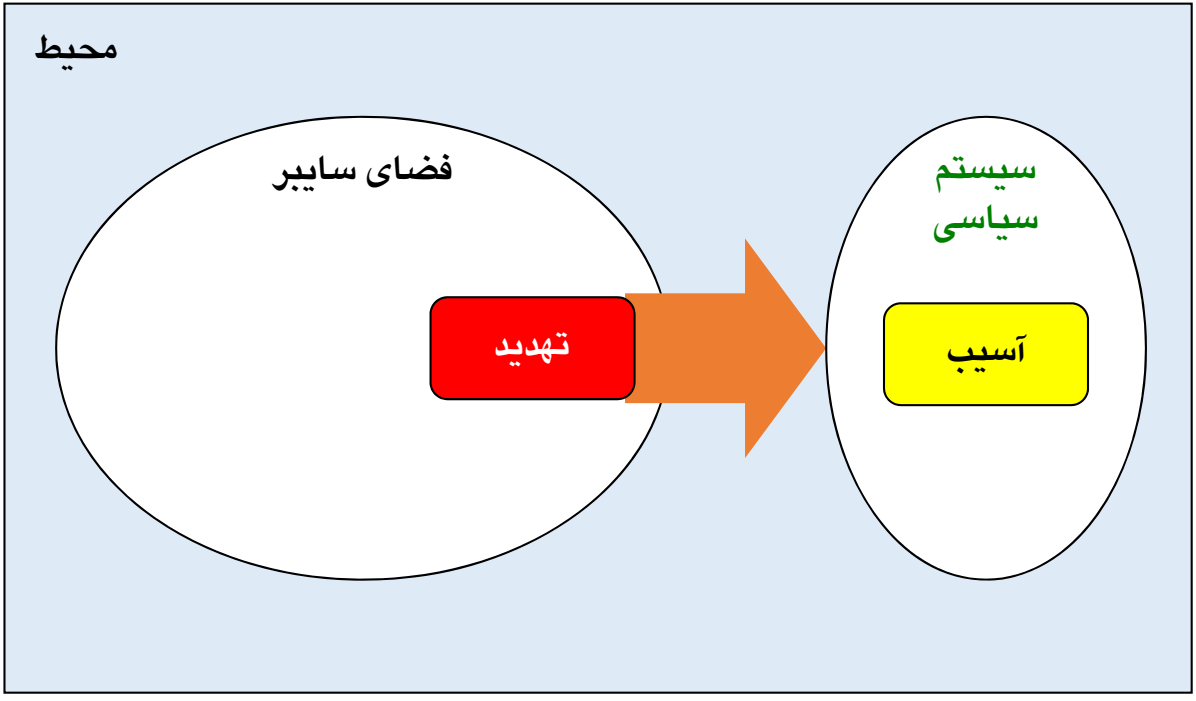
امنیت اجتماعی



امنیت اجتماعی: امنیت سیستم اجتماعی

امنیت متأثر از فضای سایبر

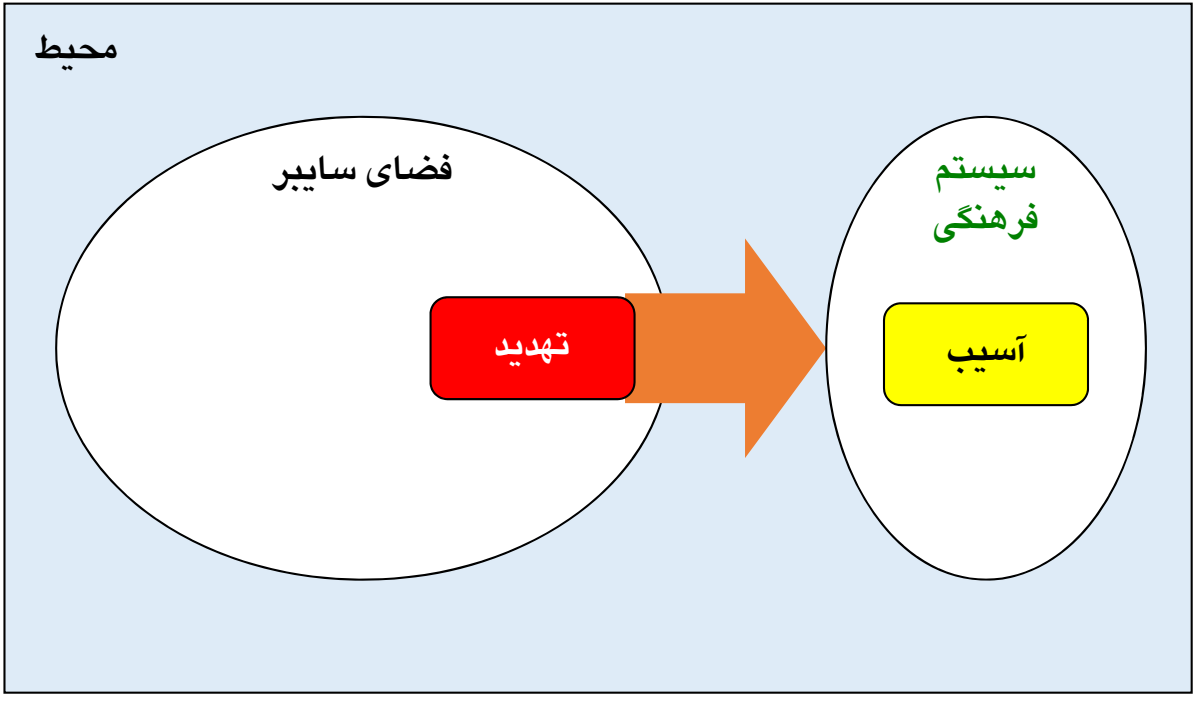
امنیت سیاسی



امنیت سیاسی: امنیت سیستم سیاسی

امنیت متأثر از فضای سایبر

امنیت فرهنگی



امنیت فرهنگی: امنیت سیستم فرهنگی