دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

مرکز پژوهشی آپا
دانشگاه صنعتی امیرکبیر

آگاهی از وضعیت امنیت سایبری با ابزار CyGraph

ارائه دهنده
مطهره دهقان

آبان ۹۹

مقدمه


لزوم آگاهی از وضعیت امنیت سایبری
تصمیم گیری بهتر در صورت آگاهی بهتر از وضعیت
آگاهی ناقص یا ناکافی از وضعیت
آگاهی و فهم موقعیت در مقیاس بزرگ بعنوان یک چالش
افزایش تعداد فعالیت های موذی سایبری

سناریوهای کاربردی

سناریو ۱- برج مراقبت

سناریو ۲- رانندگی

آگاهی از وضعیت

- مدل اِندزلی: آگاهی از وضعیت (SA) عبارتست از درک عناصر محیط در یک فضا و زمان مشخص، فهم معانی (منظور) آن ها و پیش بینی یا تخمین وضعیت آن ها در آینده نزدیک.

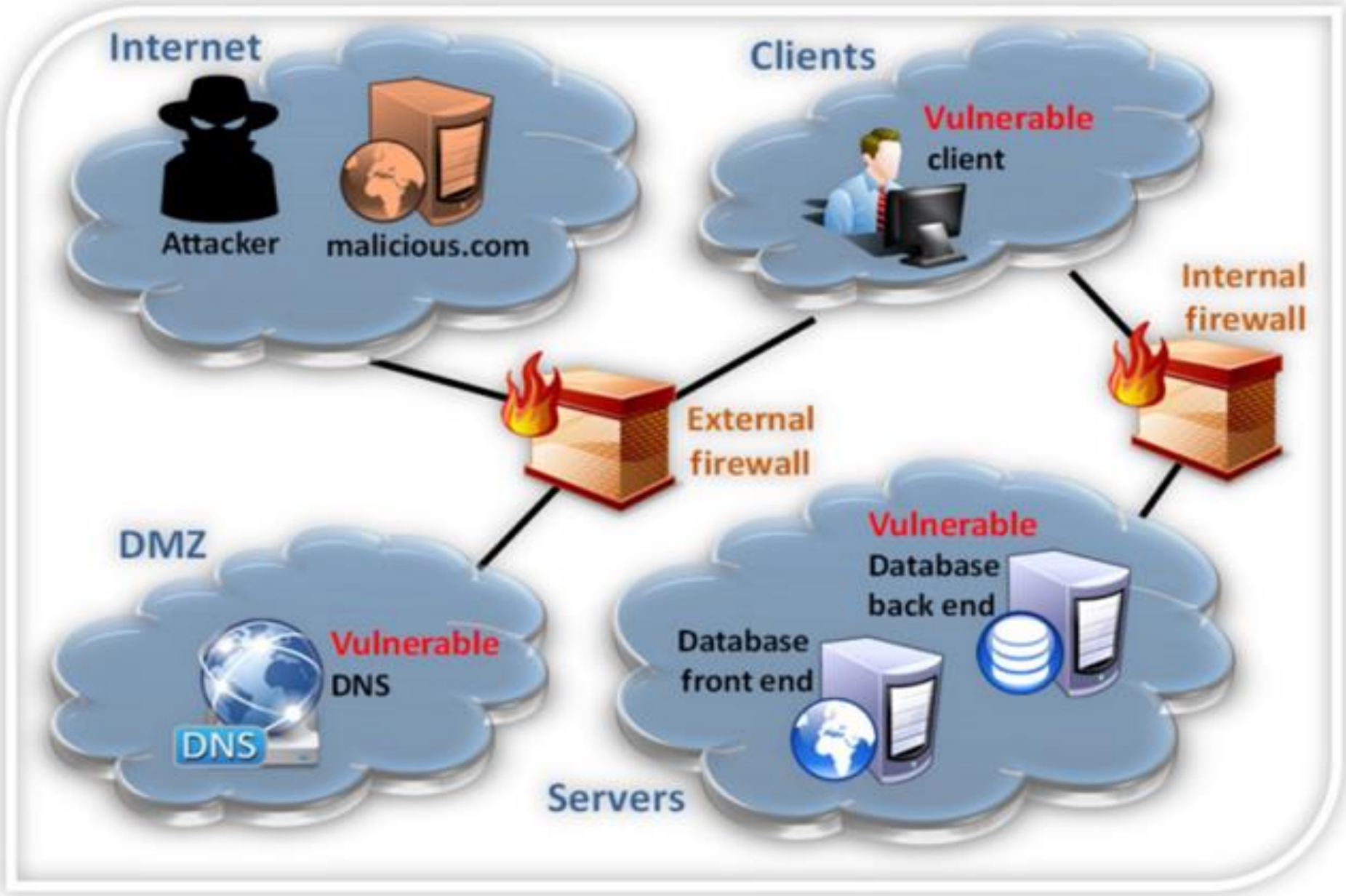
- براساس این تعریف، آگاهی از وضعیت دارای سه سطح ادراک، فهم و پیش بینی (تخمین) است.

- تعاریف متفاوتی از آگاهی از وضعیت ارائه شده است که فرض کلی همه تعاریف این است که هرچه آگاهی از وضعیت بهتری وجود داشته باشد، تصمیم گیری نیز بهتر انجام می شود؛ زیرا اطلاعات، درک و فهم قبل از تصمیم گیری بهبود می یابد.

آگاهی از وضعیت امنیت سایبری [۱۰]

Network Awareness	Threat Awareness	Mission Awareness
• Disciplined asset and configuration management • Routine vulnerability auditing • Patch management & compliance reporting • Recognize and share incident awareness across the organization	• Identify and track internal incidents and suspicious behavior • Incorporate knowledge of external threats • Participate in cross-industry or cross-government threat-sharing communities on possible indicators and warnings	• Develop a comprehensive picture of the critical dependencies (and specific components) to operate in cyberspace • Understanding these critical dependencies to support mission-impact in forensic analysis (after a situation); triage and real-time crisis-action response (during a situation); risk/readiness assessments prior to task execution (anticipating and avoiding situations); and informed defense planning (preparing to mitigate the impact of a future situation).
Today	Evolving	Needed

سناریوی آگاهی از وضعیت امنیت سایبری



NATO CDSA RFI

- در تاریخ ۱۸ می ۲۰۱۵، آژانس اطلاعات و ارتباطات ناتو یک درخواست اطلاعات ارائه داده است که در آن قابلیت های مورد نیاز برای آگاهی از وضعیت دفاع سایبری چند ملیتی ارائـه شـده اسـت کـه شامل ۳۵ مورد کاربرد است.

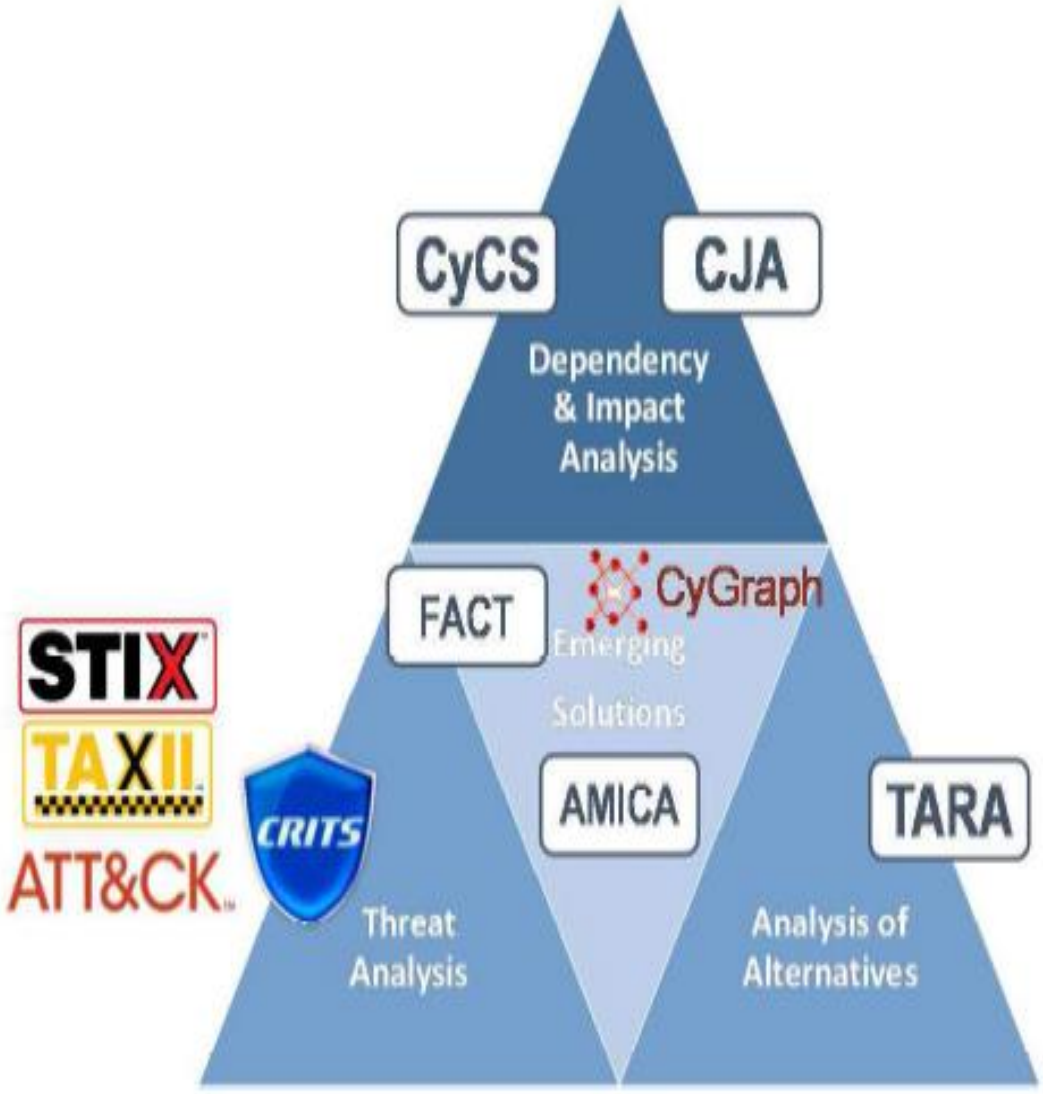
- یک مجموعه کامل و جامع از قابلیت های CDSA شامل چهار حوزه اصلی می شود:

  - **تحلیل تهدیدات**
  - **تحلیل اثرات و وابستگی ها**
  - **تحلیل راه حل های جایگزین**
  - **راه حل های در حال ظهور و نو**

NATO CDSA RFI- MITRE Solutions [10]

Table 1: MITRE Efforts by CDSA Capability

Threat Analysis	CRITs ATT&CK™ STIX™, TAXII™
Dependency & Impact Analysis	CyCS CJA
Analysis of Alternatives (AoA)	TARA
Emerging Solutions	FACT CyGraph AMICA



Appendix: RFI Use Case Capability Mapping

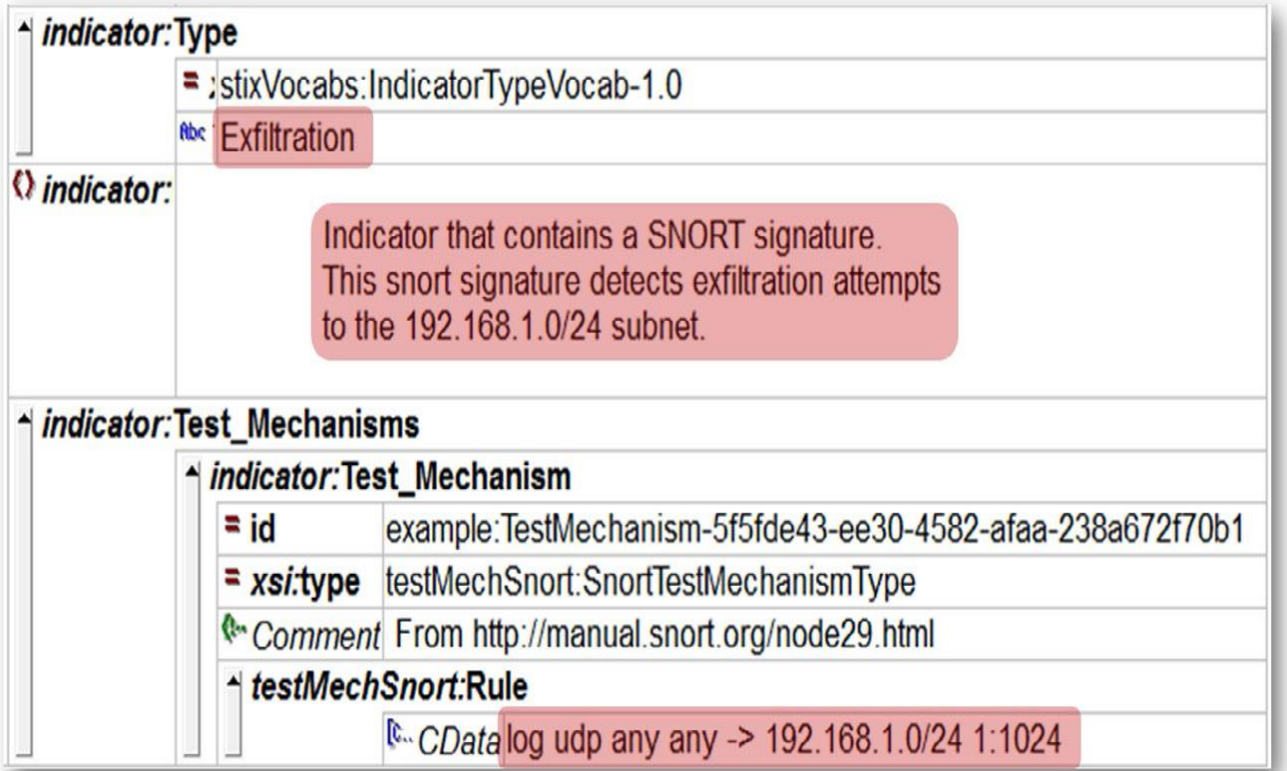
RFI Use Case	MITRE Solution
UC01 View current risks list, ordered by impact, showing geographic location	• Crown Jewels Analysis (CJA) • Cyber Command System (CyCS)
UC03 Drill down / Roll up	• Crown Jewels Analysis (CJA) • Cyber Command System (CyCS)
UC04 Hierarchical view (tailored)	• Cyber Command System (CyCS) • CyGraph: Big-Data Analytics for Network Attack Mapping
UC05 Unit and location based data security	• Cyber Command System (CyCS)
UC06 View asset dependencies	• Crown Jewels Analysis (CJA) • Cyber Command System (CyCS)
UC07 View incidents aggregated by geographic region, with linked views	• Cyber Command System (CyCS)
UC08 Generate and select from Course of Action options	• Threat Assessment and Remediation Analysis (TARA) • Federated Analysis of Cyber Threats (FACT)
UC09 Use complementary tool	• Structured Threat Information eXpression(STIX™) & Trusted Automated eXchange of Indicator Information (TAXII™) • Cyber Command System (CyCS)
UC10 Single authoritative data source	• Cyber Command System (CyCS)

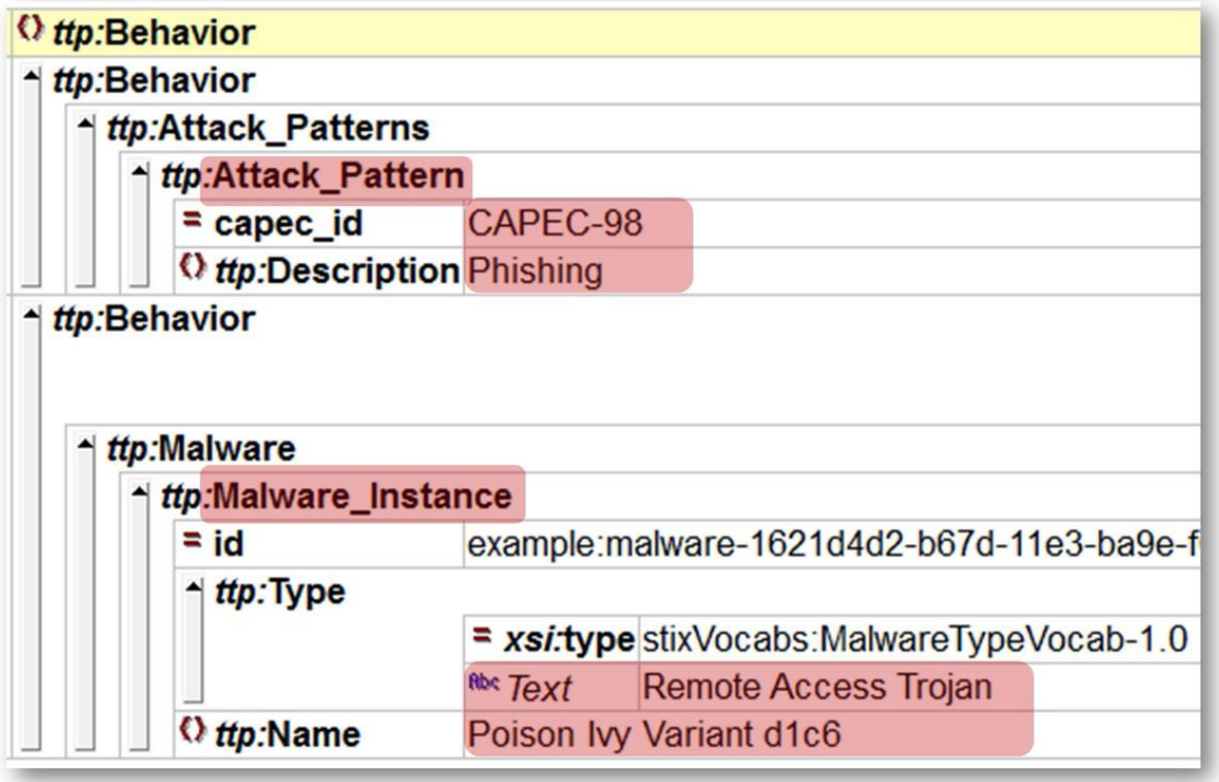
	• Cyber Command System (CyCS)
UC10 Single authoritative data source	• Cyber Command System (CyCS)
UC11 View interconnectivity	• Cyber Command System (CyCS) • CyGraph: Big-Data Analytics for Network Attack Mapping
UC12 View connections of asset	• Cyber Command System (CyCS) • CyGraph: Big-Data Analytics for Network Attack Mapping
UC13 Monitor network (network oversight)	• CyGraph: Big-Data Analytics for Network Attack Mapping
UC15 Fuse data	• Federated Analysis of Cyber Threats (FACT) • CyGraph: Big-Data Analytics for Network Attack Mapping
UC19 Collect asset dependencies [*manual*]	• Crown Jewels Analysis (CJA) • Cyber Command System (CyCS)
UC21 Training and simulation	• Analyzing Mission Impacts of Cyber Actions (AMICA)
UC23 View asset information	• Cyber Command System (CyCS)
UC24 Filter views (linked views)	• Cyber Command System (CyCS)
UC25 Monitor Specific Threat	• Collaborative Research Into Threats (CRITs) • Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)

RFI Use Case	MITRE Solution
UC26 **Visualizations**	• Cyber Command System (CyCS) • CyGraph: Big-Data Analytics for Network Attack Mapping
UC27 **Prioritize Incident**	• Threat Assessment and Remediation Analysis (TARA) • Cyber Command System (CyCS) • Federated Analysis of Cyber Threats (FACT)
UC29 **View historical incidents by asset**	• Collaborative Research Into Threats (CRITs)
UC34 **Capture options and decisions**	• Threat Assessment and Remediation Analysis (TARA) • Cyber Command System (CyCS) • Federated Analysis of Cyber Threats (FACT)
UC35 **View public data sources**	• Structured Threat Information eXpression(STIX™) & Trusted Automated eXchange of Indicator Information (TAXII™) • Cyber Command System (CyCS) • Federated Analysis of Cyber Threats (FACT)

STIX- Structured Threat Information eXpression

- یکی از امکانات مهم برای کمک به تحلیل امنیت سایبری STIX است که یک زبان ساخت یافتـه و قابـل توسـعه برای بیان تهدیدات سایبری است. معماری STIX شامل بازیگران تهدید سایبری، روش ها، فنـون و رویـه آن هـا (TTPs)، رخدادهای سایبری، شاخص های حمله، هدف های حمله و اقدامات متقابل است.





TAXII- Trusted Automated eXchange of Indicator Information

- علیرغم اینکه زبان استاندارد تهدیدات بسیار مفید است، اما ارزش واقعی زمانی بدست می آید که این اطلاعات به اشتراک گذاشته شود.
- TAXII سرویسی برای تبادل خودکار اطلاعات جهت اشتراک گذاری تهدیدات، تعریف می کند.

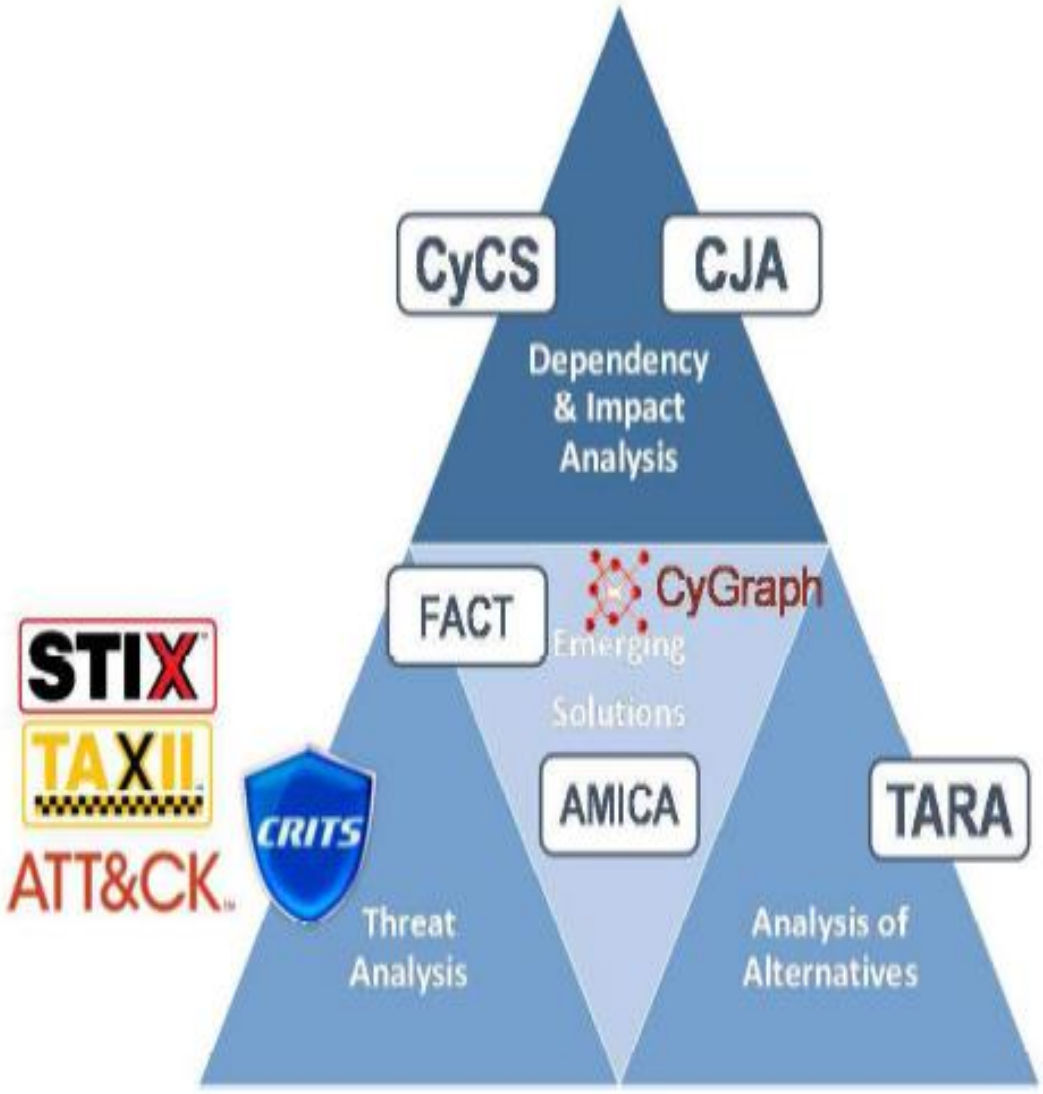
UC09: Use Complementary Tool

UC35: View Public Data Sources

NATO CDSA RFI- MITRE Solutions

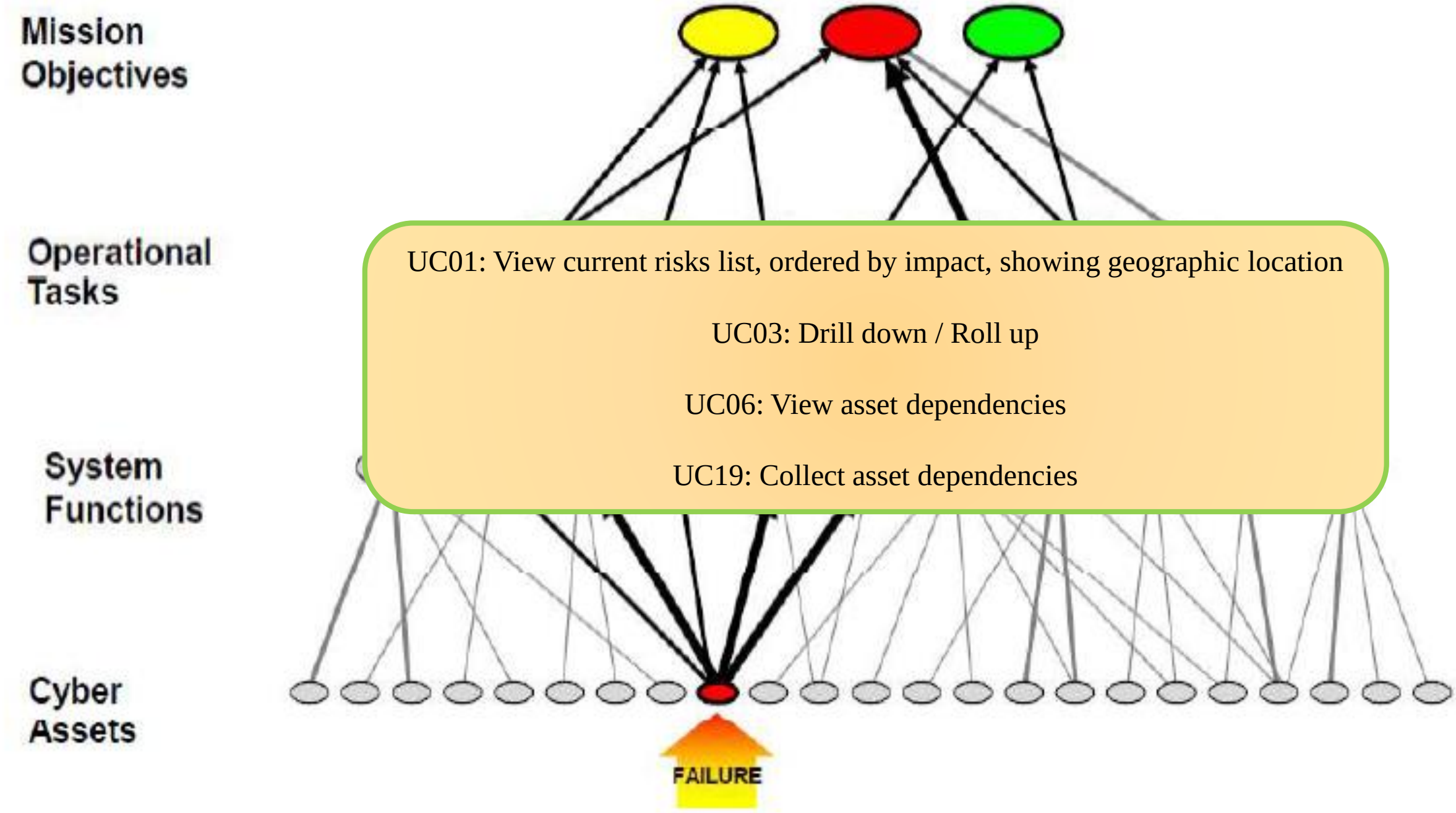
Table 1: MITRE Efforts by CDSA Capability

Threat Analysis	CRITs ATT&CK™ STIX™, TAXII™
Dependency & Impact Analysis	CyCS CJA
Analysis of Alternatives (AoA)	TARA
Emerging Solutions	FACT CyGraph AMICA



CJA- Crown Jewels Analysis

- CJA یک فرایند و مجموعه ابزار برای شناسایی دارایی های بحرانی مأموریت های سازمان است.
- CJA یک نقشه وابستگی برای فهم بهتر بحرانی ترین دارایی ها – طی مراحل توسعه سیستم تا نصب آن- ایجاد می کند.
- نقشه وابستگی با شناسایی مأموریت ها و اولویت بندی آن ها آغاز می شود. در این نقشه، ابتدا مأموریت ها و سپس در لایه بعدی وظایف عملیاتی و سپس توابع سیستمی و نهایتا دارایی های سایبری نمایش داده می شوند.



UC01: View current risks list, ordered by impact, showing geographic location

UC03: Drill down / Roll up

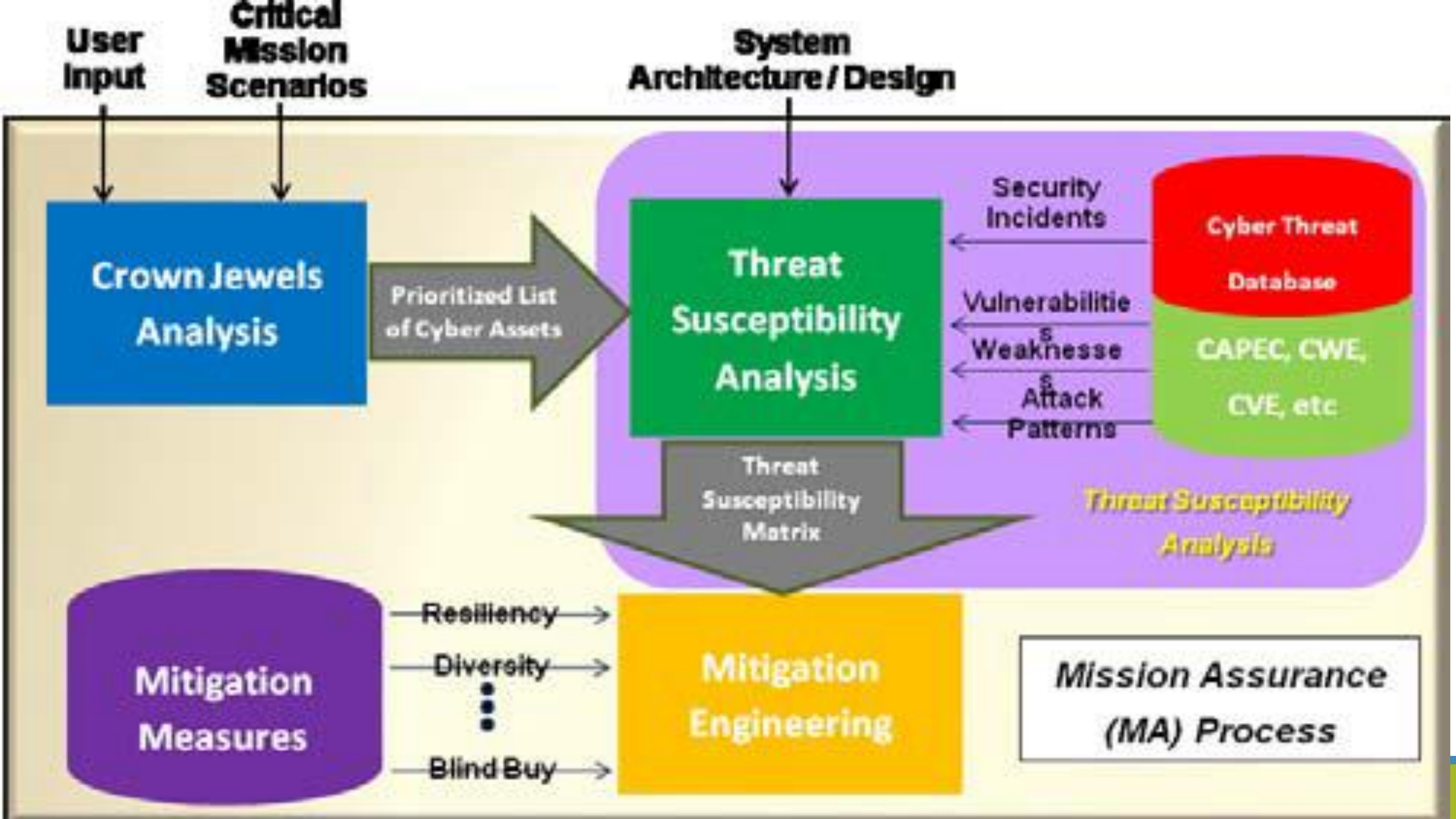
UC06: View asset dependencies

UC19: Collect asset dependencies

CyCS- Cyber Command System

- CyCS، با نگاشت عملیات مأموریت به عملیات شبکه پشتیبان کننده مأموریت، اطمینان از مأموریت در فضای سایبری را به عنوان هدف خود در نظر می گیرد.

- اطمینان از مأموریت، به معنای درجه بالایی از اطمینان داشتن از موفقیت یک مأموریت است. باید طی فرایندهایی این درجه اطمینان از موفقیت، دائما کنترل شود.


User Input
Critical Mission Scenarios
System Architecture / Design
Crown Jewels Analysis
Prioritized List of Cyber Assets
Threat Susceptibility Analysis
Security Incidents
Vulnerabilities
Weaknesses
Attack Patterns
Cyber Threat Database
CAPEC, CWE, CVE, etc
Threat Susceptibility Matrix
Threat Susceptibility Analysis
Mitigation Measures
Resiliency
Diversity
Blind Buy
Mitigation Engineering
Mission Assurance (MA) Process

CyCS

- در طراحی ابزار CyCS، از چرخه مشاهده (Observe)– جهت دهی(Orient) – تصمیم گیری (Decide)– عمل کردن (Act) استفاده می شود.

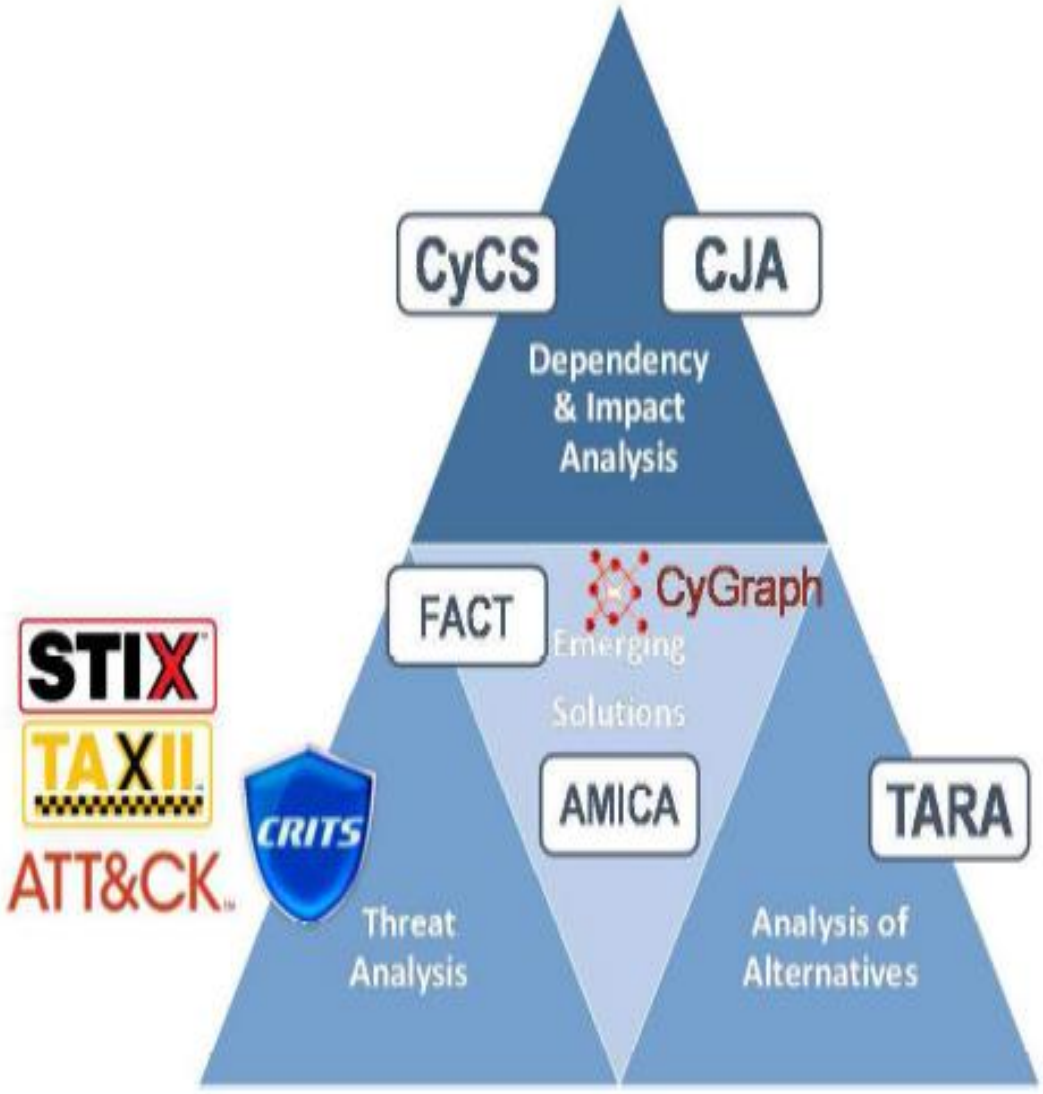
  - زیر سیستم مانیتورینگ برای مشاهده
  - زیر سیستم تحلیل برای جهت دهی
  - زیر سیستم پشتیبانی تصمیم برای تصمیم گیری
  - زیر سیستم تعیین وظایف برای عمل کردن

UC01, UC03-UC07, UC09-UC12, UC23, UC24, UC26, UC27

NATO CDSA RFI- MITRE Solutions

Table 1: MITRE Efforts by CDSA Capability

Threat Analysis	CRITs ATT&CK™ STIX™, TAXII™
Dependency & Impact Analysis	CyCS CJA
Analysis of Alternatives (AoA)	TARA
Emerging Solutions	FACT CyGraph AMICA



ابزار CyGraph

- ابزارهای مختلفی برای تحلیل امنیت وجود دارد که نتیجه استفاده از این ابزارها در کنار هم، حجم بالای اطلاعات و عدم دستیابی به تحلیل درست از وضعیت امنیت سایبری است.

- آقای Steven Noel در دانشگاه George Mason و پس از آن در شرکت MITRE، سعی برآن داشته تا راهی برای تحلیل و ادغام اطلاعات بدست آمده از وضعیت امنیت سایبری را ایجاد نموده و گراف حاصل از اطلاعات بدست آمده را ایجاد کند، تا نتایج بهتری از تحلیل اطلاعات برای تشخیص فعالیت های موذی حاصل شود.

ابزار CyGraph– ادامه

- ابزار CyGraph دارای امکانات بصری سازی گرافیکی و پرس وجوی پیشرفته است.

- این ابزار داده های منابع متعدد (توپولوژی، آسیب پذیری ها، تنظیمات سرویس گیرنـده / سـرویس دهنده، قوانین دیواره آتش، رویدادها، و غیره) را با هم مرتبط می کند و گراف حمله و قابلیت هایی برای تحلیل وضعیت امنیت سیستم ارائه می دهد.

ابزار CyGraph – قابلیت ها

- داده ها و رویدادهای جداگانه را در کنار یکدیگر آورده و بصورت یک تصویر کلی در حال انجام – برای پشتیبانی از تصمیم گیری و آگاهی از وضعیت – نمایش می دهد.
- آسیب پذیری ها را با نگاشت به تهدیدات بالقوه و دارایی های حیاتی مأموریت، اولویت بندی می کند.
- در مواجهه با حملات واقعی، هشدارهای نفوذ را به مسیرهای آسیب پذیری شناخته شده مرتبط کرده و بهترین شیوه های عمل برای پاسخ به حملات را نشان می دهد.
- برای پی جویی پس از حمله، مسیرهای آسیب پذیر را نشان می دهد که ممکن است لازم باشد بررسی های بیشتری بر روی آن ها انجام شود.

پشته دانش ابزار CyGraph [11]

وابستگی مأموریتی
- اهداف
- فعالیت ها
- وظایف

تهدیدات سایبری
- عامل
- حوادث
- شاخص ها
- اشخاص ثالث

مواضع سایبری
- پیکره بندی
- آسیب پذیری ها
- قوانین خط مشی

زیرساخت شبکه
- تقسیم بندی
- سنسور
- توپولوژی

مرتبط با جنگ سایبری و آمادگی مأموریتی

معماری ابزار CyGraph [11]

زیر ساخت شبکه

مواضع سایبری

تهدیدات سایبری

وابستگی مأموریتی

دریافت کردن

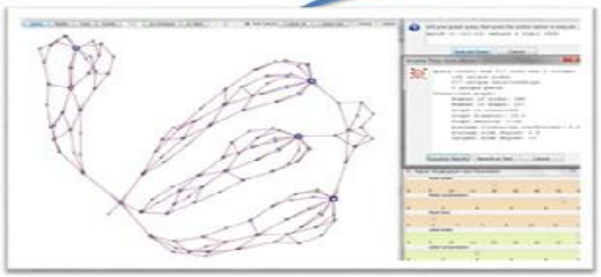
مدل نرمالیزه شده

تبدیل کردن

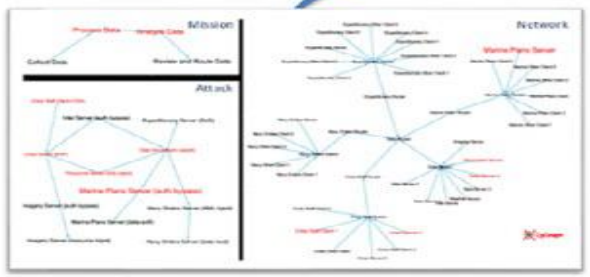
مدل گراف

تحلیل کردن

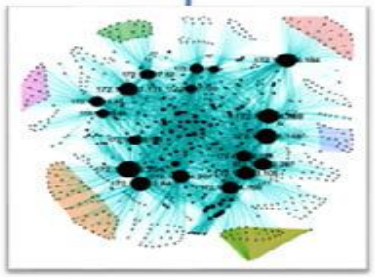
بصری سازی



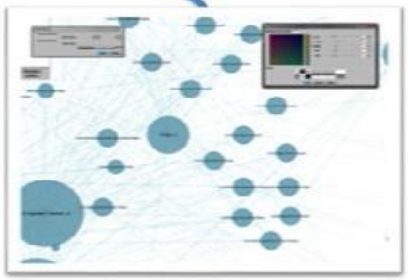
پویایی



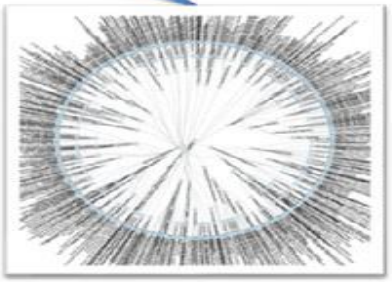
لایه بندی کردن



گروه بندی کردن

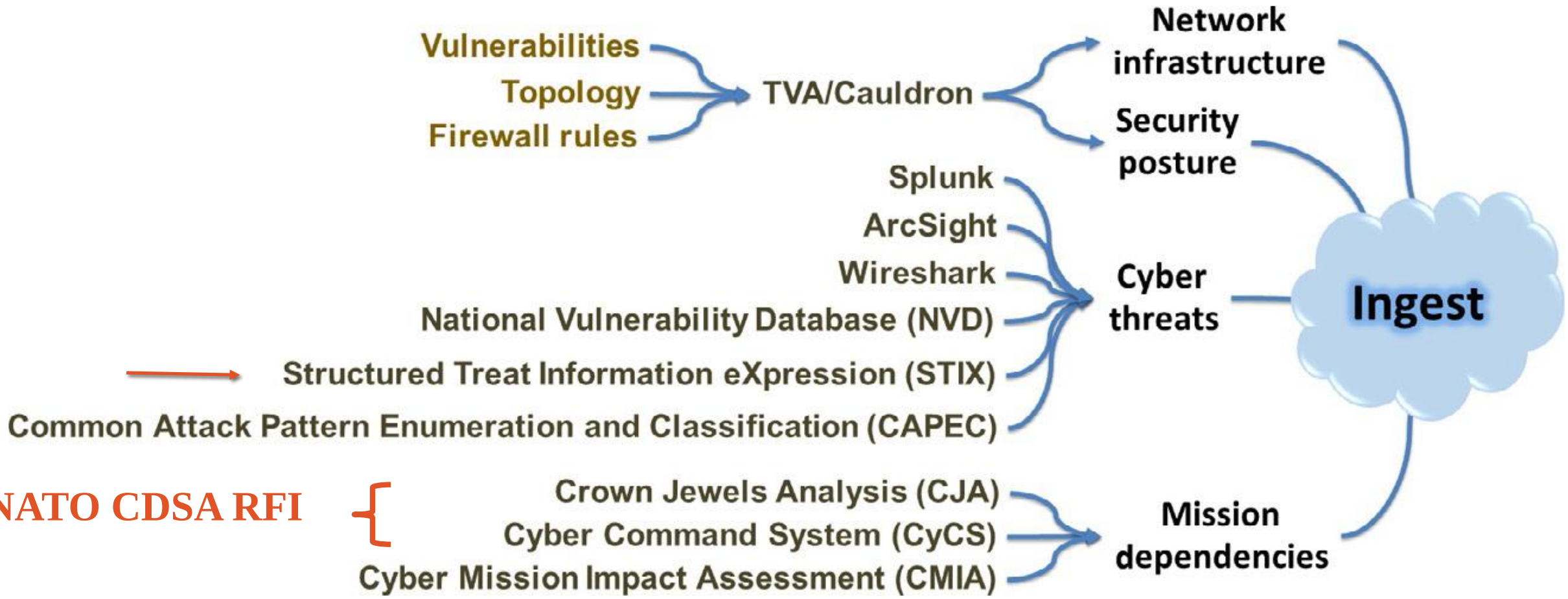


فیلترکردن



دیدهای سلسله مراتبی

نمونه ای از منابع داده مورد استفاده در CyGraph [11]



TVA/Cauldron

- یک قابلیت پایه برای ارزیابی مواضع سایبری و نگاشت آسیب پذیری ها به زیرساخت های شبکه است.
- این نگاشت، به اولویت بندی آسیب پذیری ها، شناسایی قوانین و خط مشی های غیر امن دسترسی ها، نمایش چگونگی استفاده از آسیب پذیری ها برای نفوذ به شبکه توسط حمله کننده ها کمک می کند.
- از ابزار TVA/ Cauldron برای تحلیل توپولوژی، آسیب پذیری ها و قوانین مورد نیاز برای نگاشت مسیرهای آسیب پذیری که بعنوان گراف حمله شناخته می شوند، استفاده می شود.

Firewall Policy

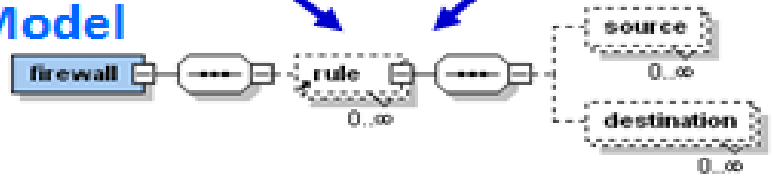
```
acl_outside deny tcp any 62.59.15.0 255.255.255.0 eq smtp
acl_outside permit tcp any host 62.59.15.110 eq smtp
acl_outside permit tcp any object-group dmz_srvce object-group web_srvce
acl_outside permit tcp any host 62.59.14.165 object-group mail_srvce
acl_outside permit tcp host 208.121.58.99 host 62.59.14.165 eq smtp
acl_outside permit tcp host 66.93.145.29 host 62.59.14.165 eq smtp
acl_outside permit tcp host 67.28.57.31 host 62.59.14.165 eq smtp
acl_dmz permit tcp any object-group db_srvce eq 3306
acl_dmz permit tcp any host 172.16.3.40 eq http
acl_inside permit tcp any any object-group tcat_srvce
acl_inside permit tcp any object-group web_srvce eq smtp
acl_inside permit tcp any object-group web_srvce eq ftp
acl_inside deny ip any any
nonat permit ip 172.16.0.0 255.255.0.0 192.168.1.0 255.255.255.0
```

Cisco

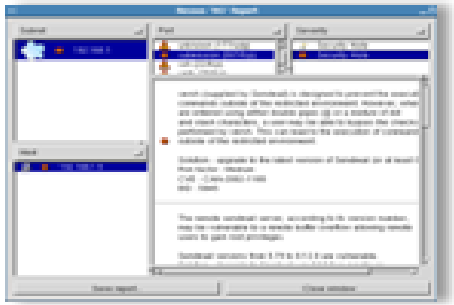
table=subnet name=Remote bits=24 ipaddr=132.38.200.0
table=subnet name=PRINT bits=24 ipaddr=132.38.218.0
table=subnet name=TEST bits=24 ipaddr=132.38.219.0
table=subnet name=IA-hosts bits=24 ipaddr=132.38.105.0
table=subnet name=WID bits=16 ipaddr=172.16.0.0
table=subnet name=WLAN bits=24 ipaddr=132.38.8.0

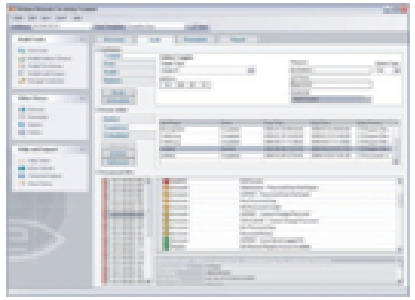
Sidewinder

Access Rules Model



Host Vulnerabilities





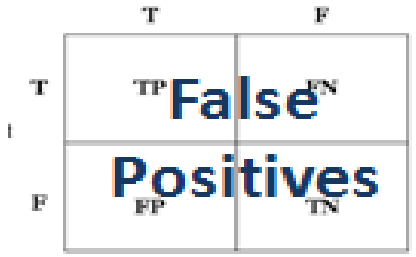
Nessus

Retina

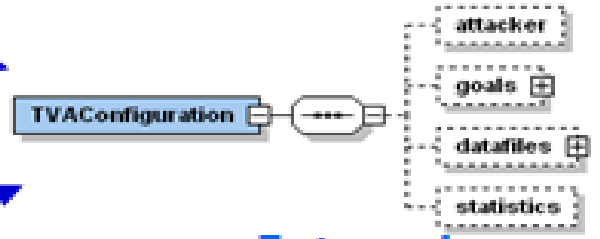
Host Vulnerability Model

Enterprise Environment

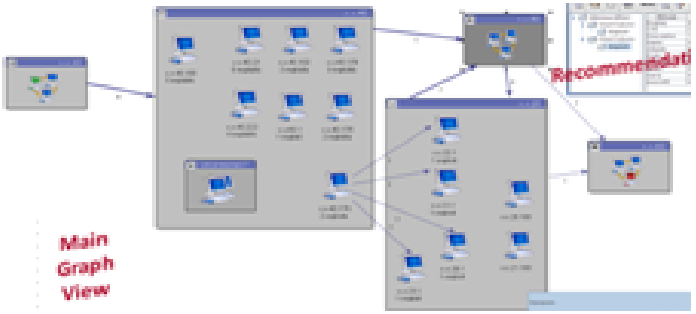
Threats



Critical Assets

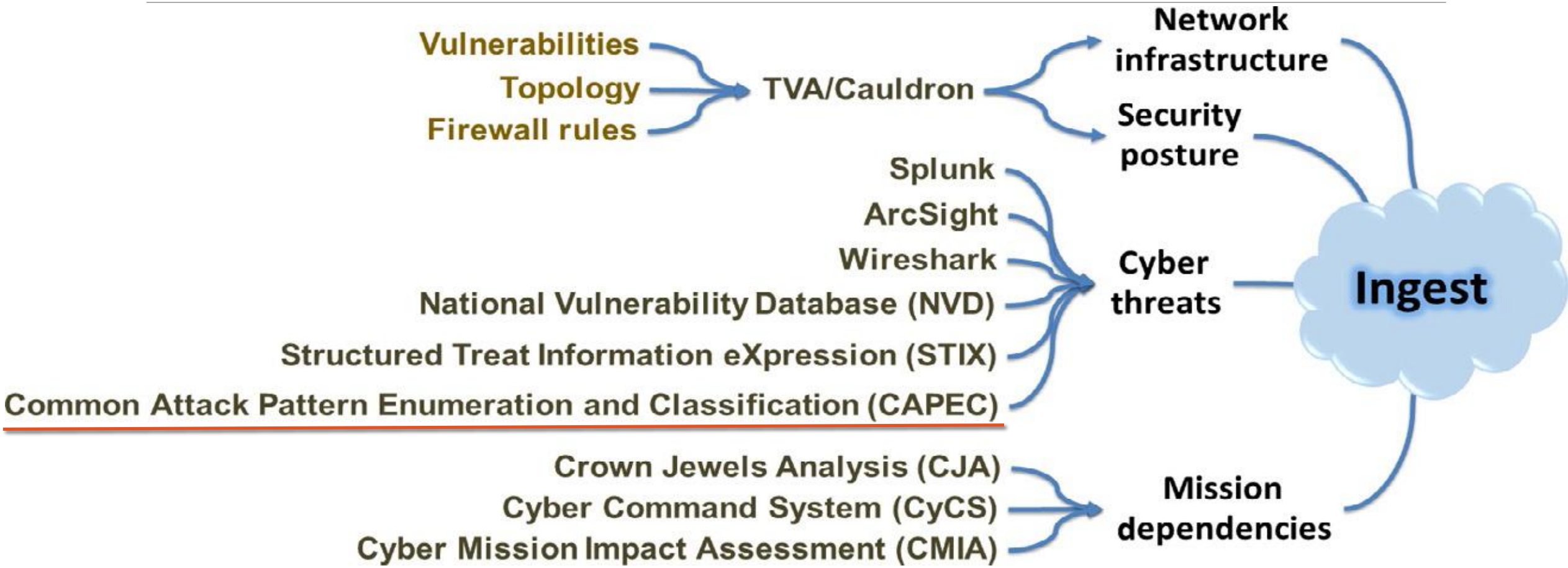


Enterprise Environment Model



Attack Graph

منابع داده مورد استفاده در CyGraph

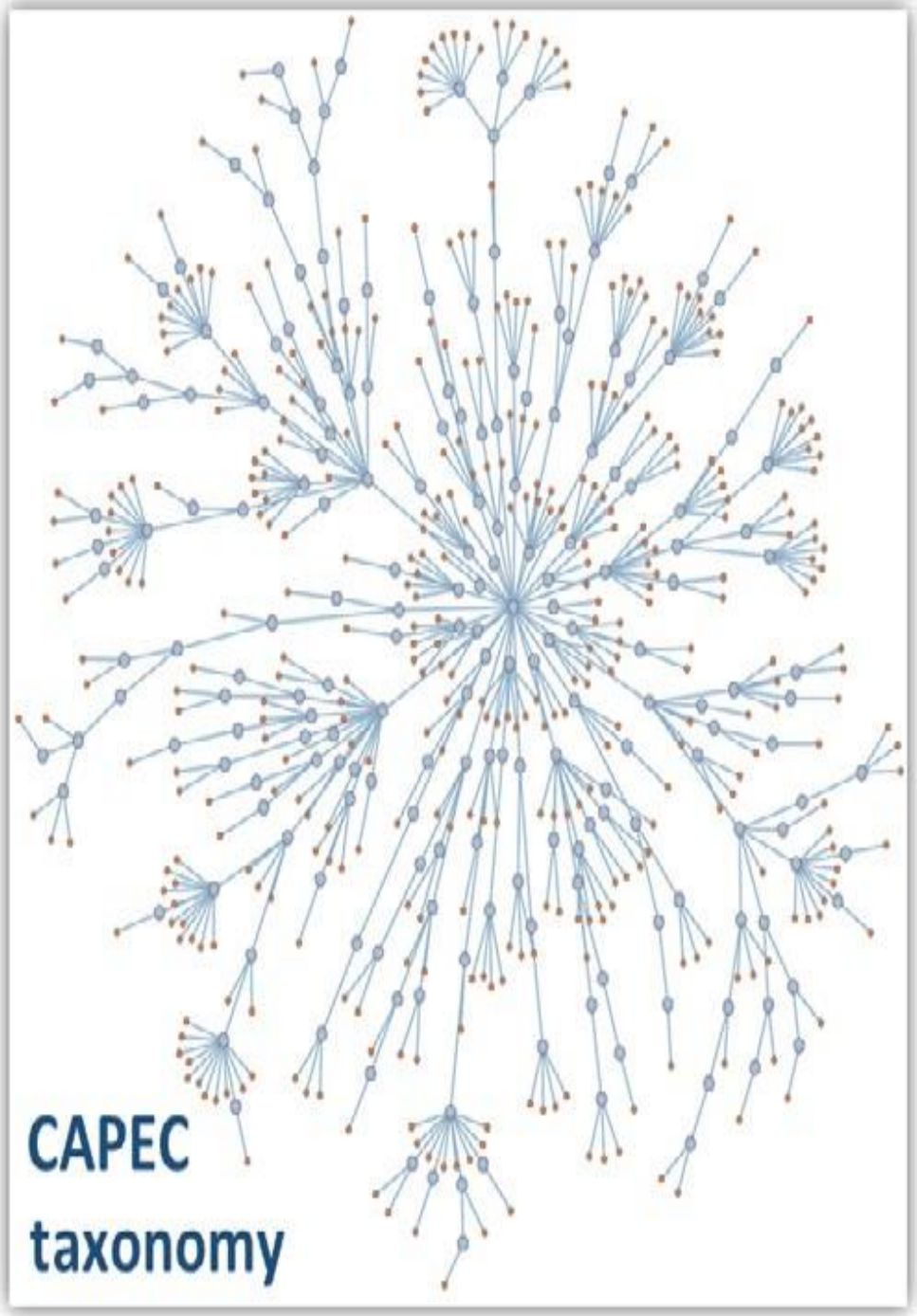


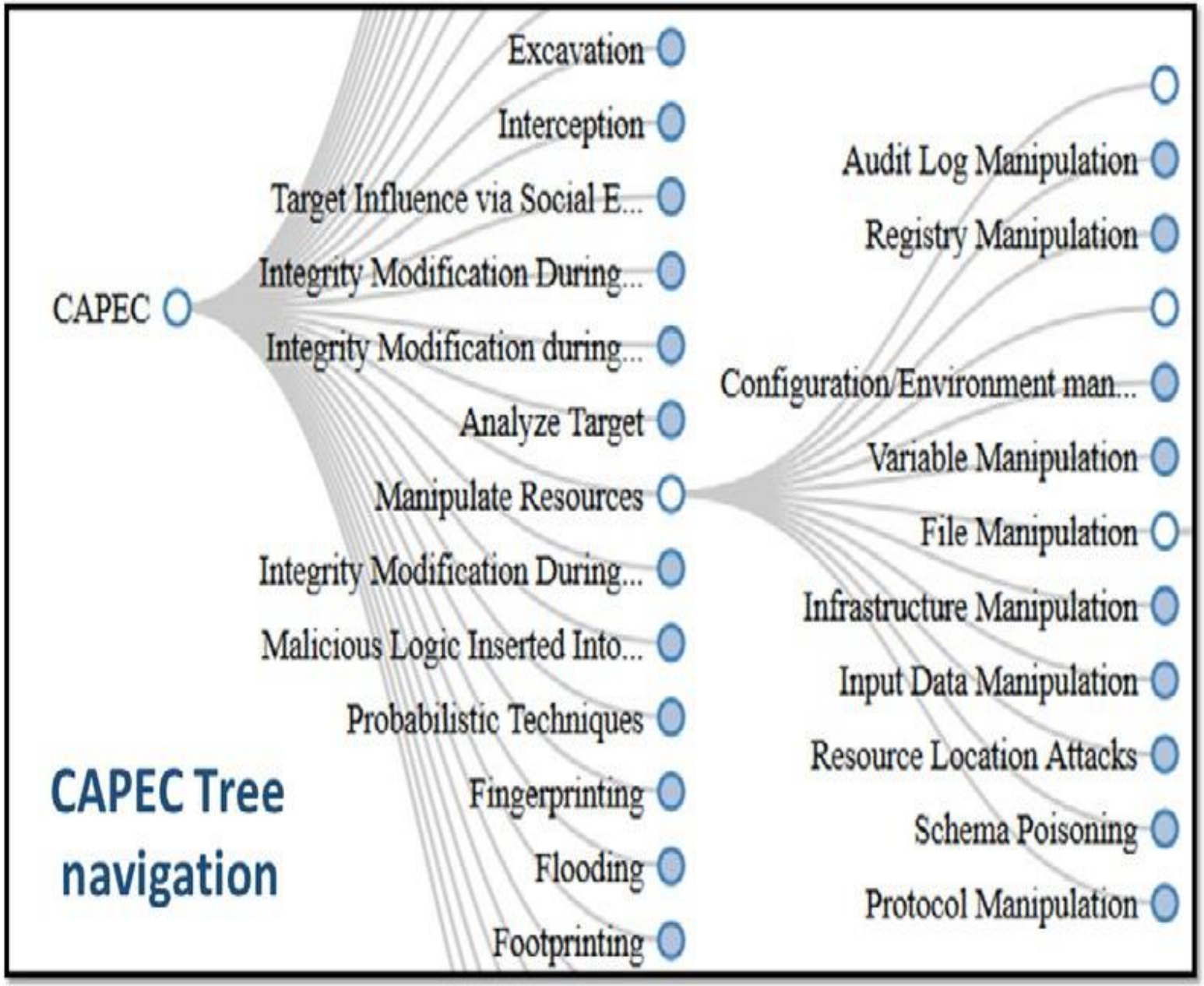
CAPEC- Common Attack Pattern Enumeration and Classification

- یکی از منابع مهم برای اشتراک گذاری تهدیدات، CAPEC است که یک دسته بندی استاندارد از الگوهای حمله است.

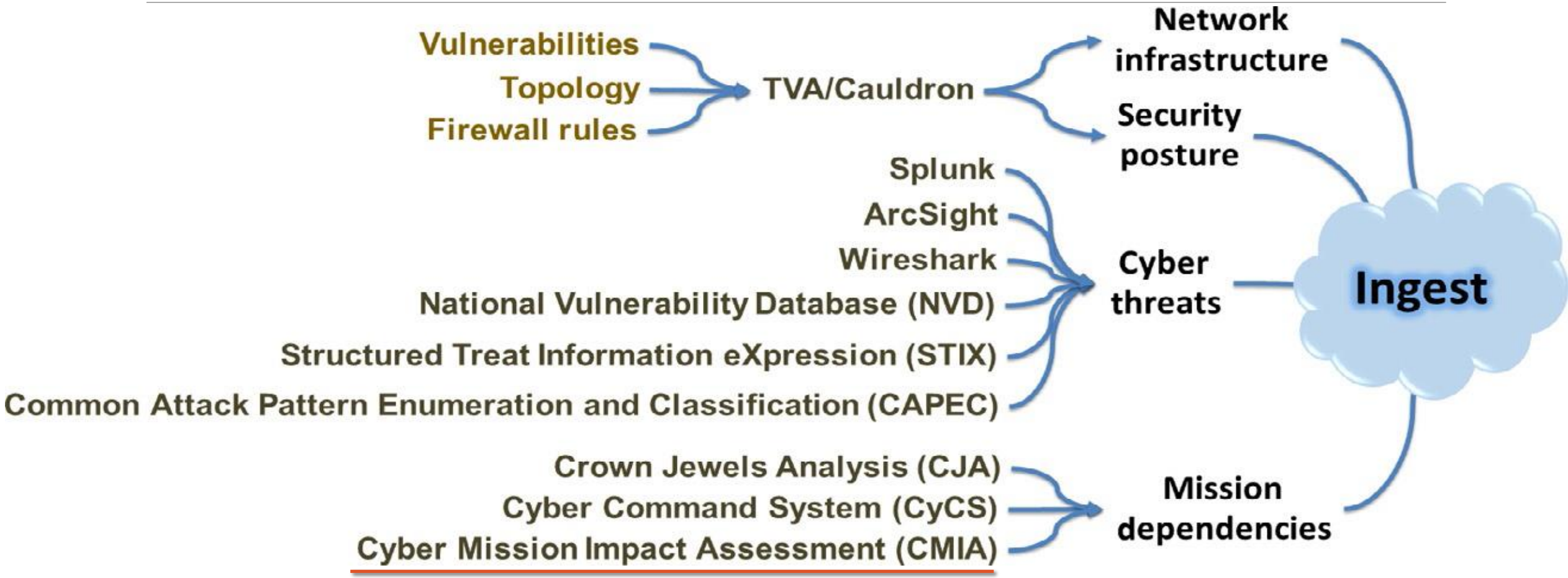
- CAPEC مشخصه هایی همراه با جزئیات از الگوهای حمله فراهم می کند. همچنین، دسته بندی سلسله مراتبی شامل کلاس های کلی حمله، زیر-کلاس های آن ها و حملات خاص را نیز ایجاد می کند.

- دسته بندی CAPEC بصورت متنی است و پیمایش این دسته بندی ها و یافتن الگوهای حملات کار راحتی نیست که ابزار CyGraph این دسته بندی را بصورت بصری ارائه می دهد.


CAPEC
taxonomy


CAPEC
Excavation
Interception
Target Influence via Social E...
Integrity Modification During...
Integrity Modification during...
Analyze Target
Manipulate Resources
Integrity Modification During...
Malicious Logic Inserted Into...
Probabilistic Techniques
Fingerprinting
Flooding
Footprinting
Audit Log Manipulation
Registry Manipulation
Configuration/Environment man...
Variable Manipulation
File Manipulation
Infrastructure Manipulation
Input Data Manipulation
Resource Location Attacks
Schema Poisoning
Protocol Manipulation
CAPEC Tree
navigation

منابع داده مورد استفاده در CyGraph

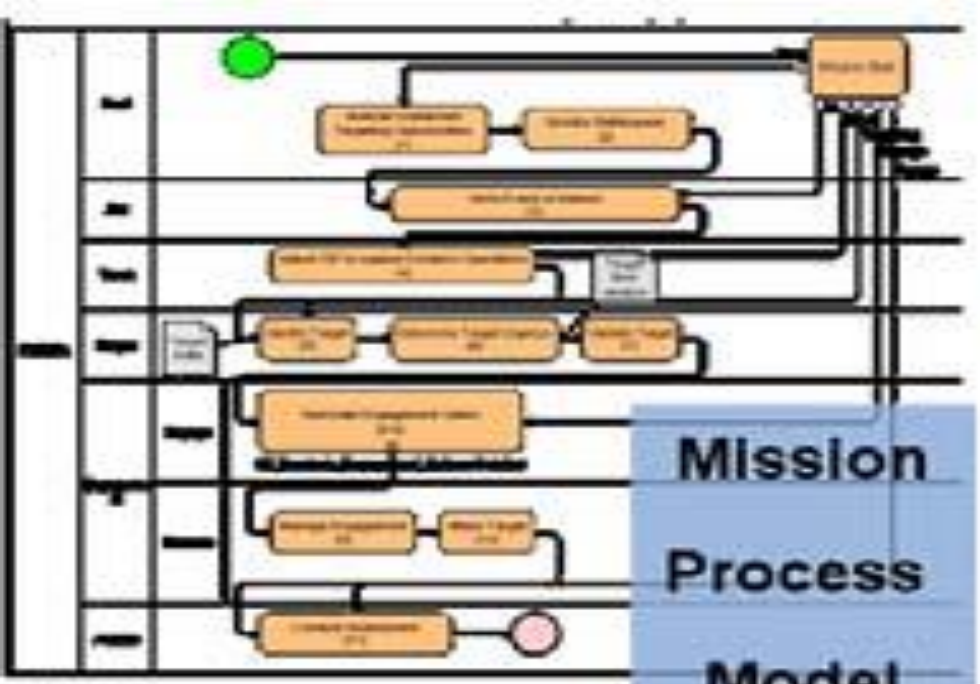


Mission Impact Assessment- MIA

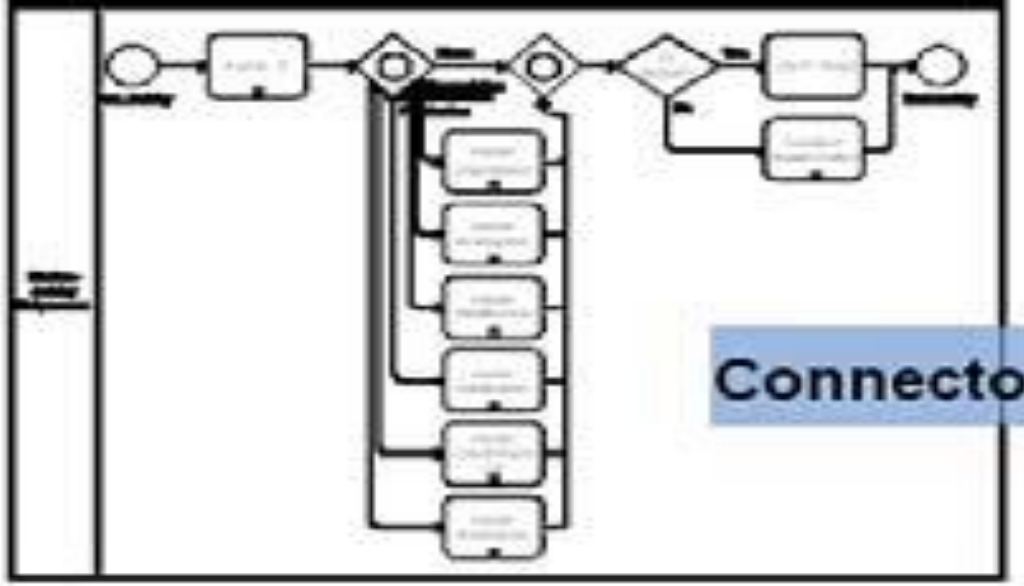
- در لایه وابستگی مأموریتی ابزار CyGraph اثر حملات سایبری بـر روی مأموریـت هـا ارزیابی می شود.

- در این لایه، وابستگی های سلسله مراتبی بین مؤلفه های مأموریتی و دارایـی هـای IT که آن ها را پشتیبانی می کنند بدست می آیـد. سـپس، اثـر حمـلات سـایبری بـر روی مأموریت ها براساس وابستگی مأموریت ها به دارایی های IT، ارزیابی می شود.

- ابزار CMIA محیطی برای شبیه سازی حملات بر روی مأموریت ها و ارزیـابی اثـرات آن ها ارائه می دهد.



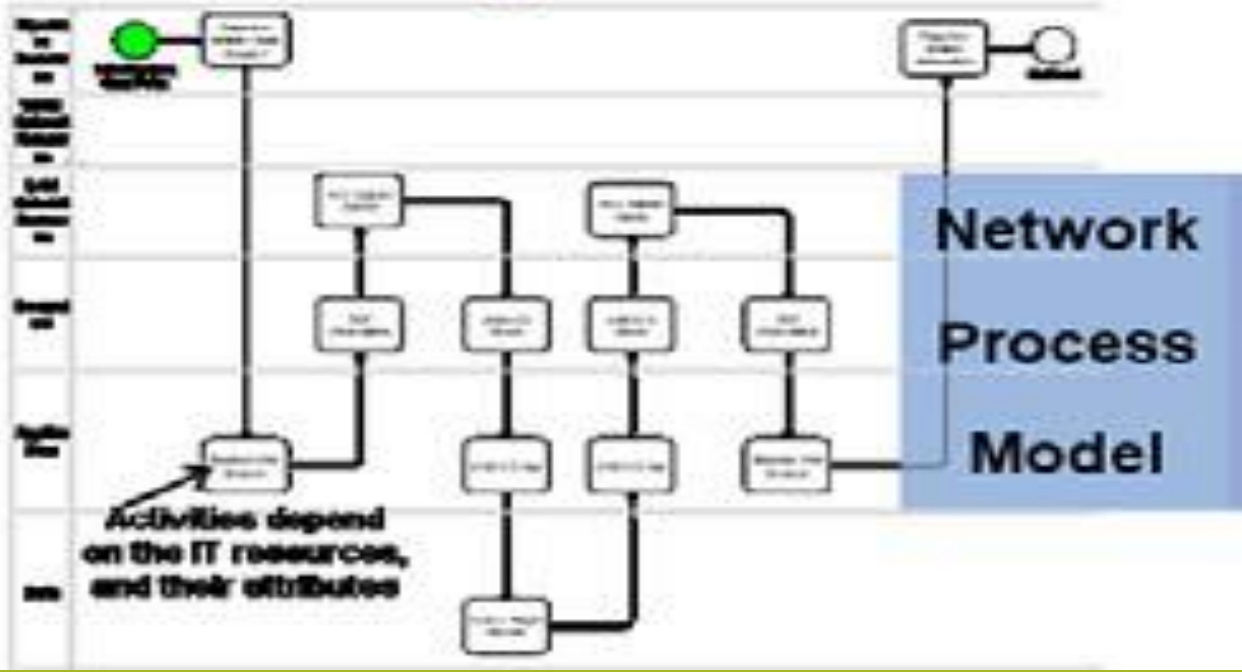
Mission Process Model



Connector

Network Diagram

IT Assets (including data) are modeled as resources



Activities depend on the IT resources, and their attributes

Network Process Model

CMIA- Cyber Mission Impact Assessment

از آن جا که تمرکز اصلی رویکرد CMIA بر ارزیابی اثر بر روی مأموریت ها است، مدل ایجاد شده توسط این ابزار، شامل جزئیات بیشتری است که در سایر مدل های ارزیابی ریسک وجود ندارد. این جزئیات شامل موارد زیر است:

گردش کار: دنباله ای از وظایف تشکیل دهنده مأموریت

خط زمانی: مدت زمان انجام وظایف که می توان با مدت زمان انجام حمله مقایسه نمود.

اثرات حمله: دسته بندی حملات سایبری به شش کلاس از اثرات سایبری.

CMIA

نحوه شبیه سازی حملات و ارزیابی اثرات آن ها

- هر منبع IT، دارای ویژگی هایی است که منعکس کننده این است که آیا منبع مورد نظر تحت تاثیر رخداد سایبری قرار گرفته است یا خیر.
- اجرای مدل فرایند حمله به موازات مدل فرایند مأموریت
- نمایش هر فعالیت مأموریت وابسته به IT با وابستگی های خودش
- اندازه گیری پارامتر MOE با/ بدون اثرات حمله سایبری

Probabilistic Mission Impact Assessment

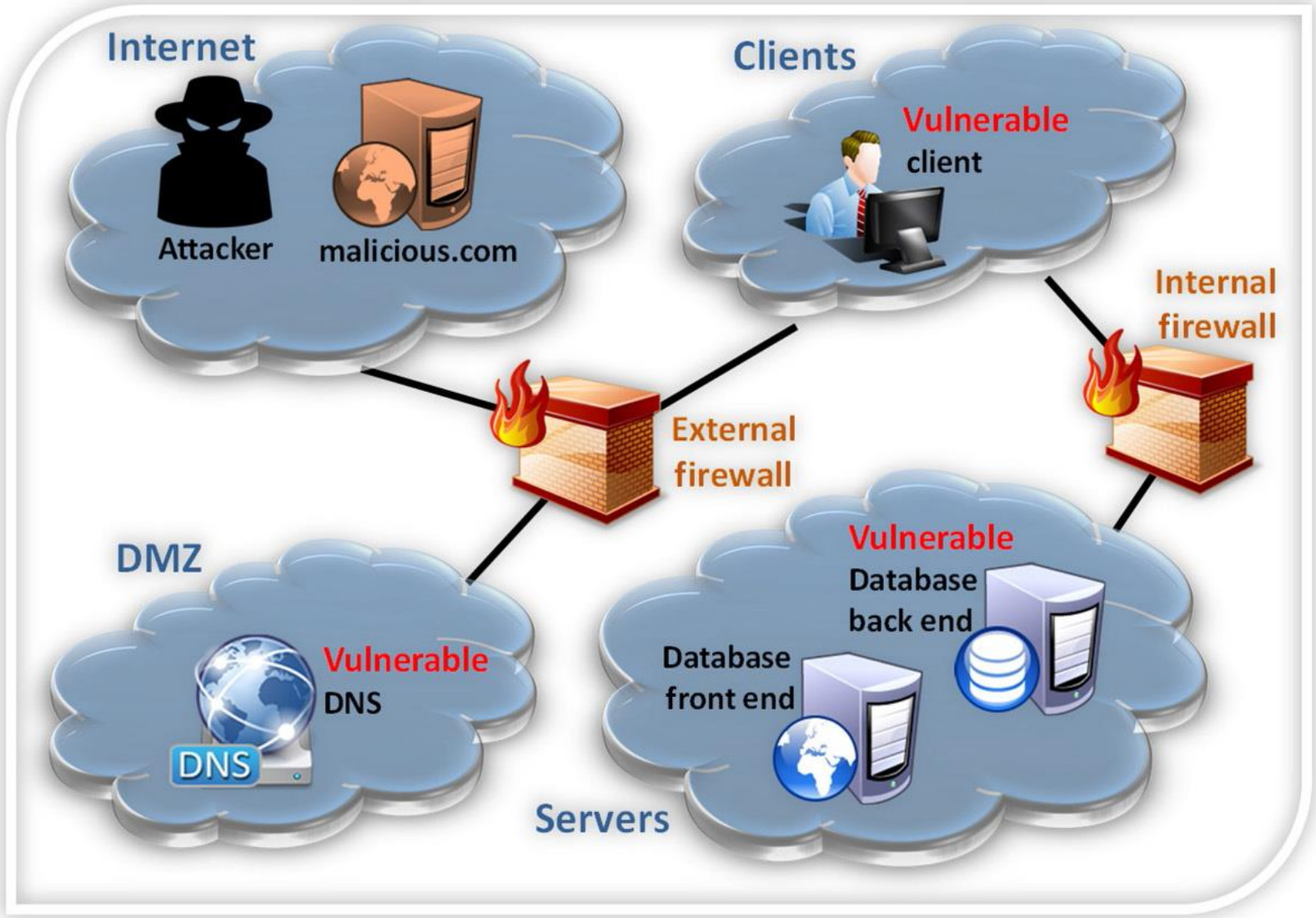
- زمانی که عدم قطعیت ورودی وجود دارد، از ارزیابی اثرات احتمالی بر روی مأموریت استفاده می شود.

- اگر ورودی‌های توصیف‌کننده یک سیستم، غیرقطعی باشند، آنگاه پیش‌بینی عملکرد پیش رو به طور قطع غیرقطعی است. این بدان معنی است که نتیجه هر گونه تحلیل مبتنی بر ورودی‌های نمایش داده شده با توزیع‌های احتمال، خود یک توزیع احتمال است.

- برای ارزیابی از روش (شبیه سازی) مونته کارلو استفاده می شود.

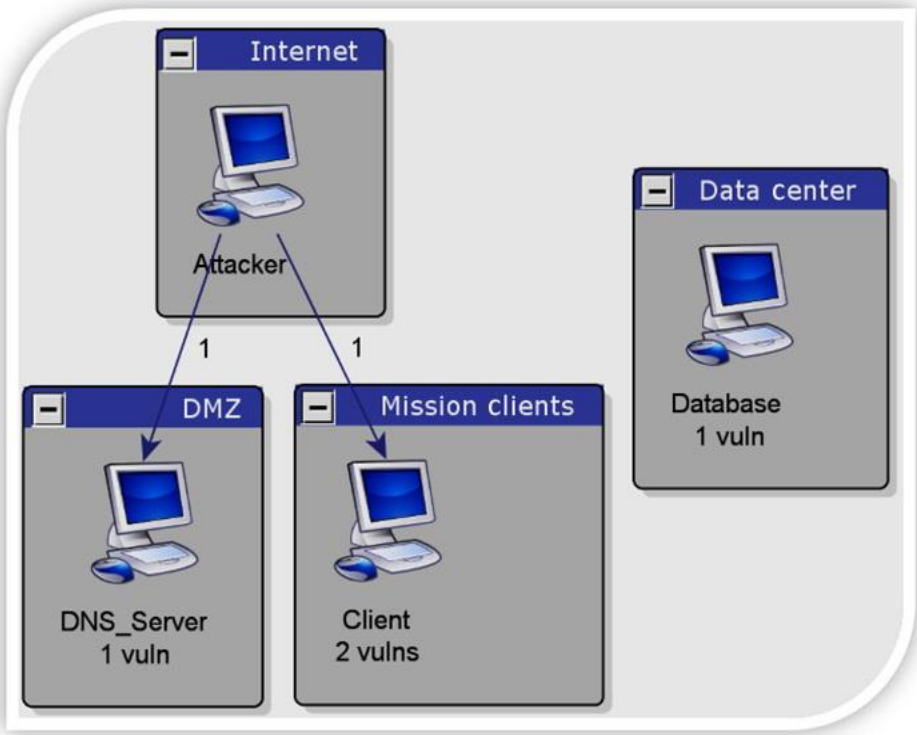
- شبیه‌سازی مونته کارلو برای توصیف روشی جهت انتشار عدم قطعیت‌های موجود در ورودی مدل به عدم قطعیت‌ها در خروجی مدل، به کار می‌رود.

مثال کاربردی

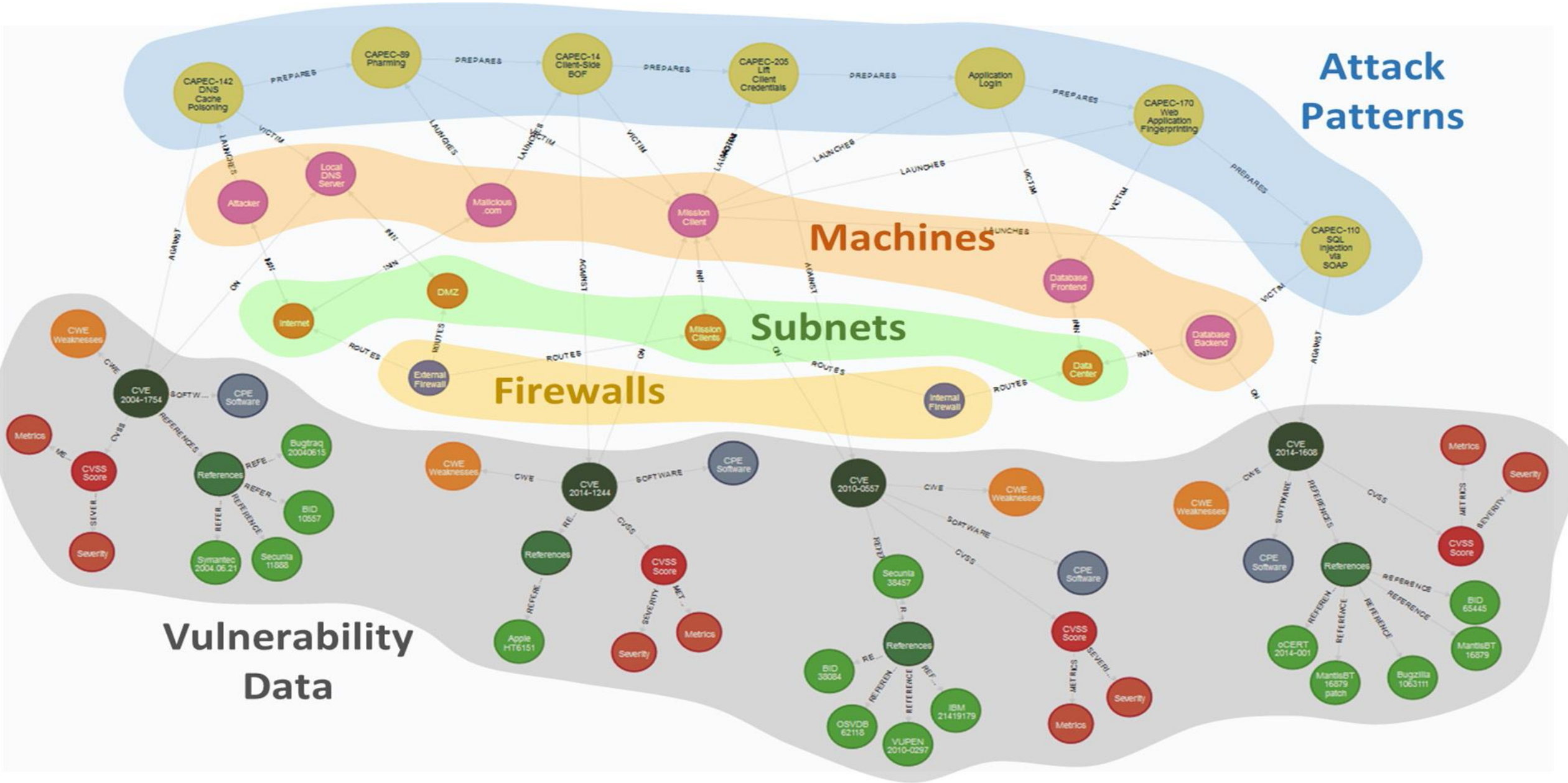


Network

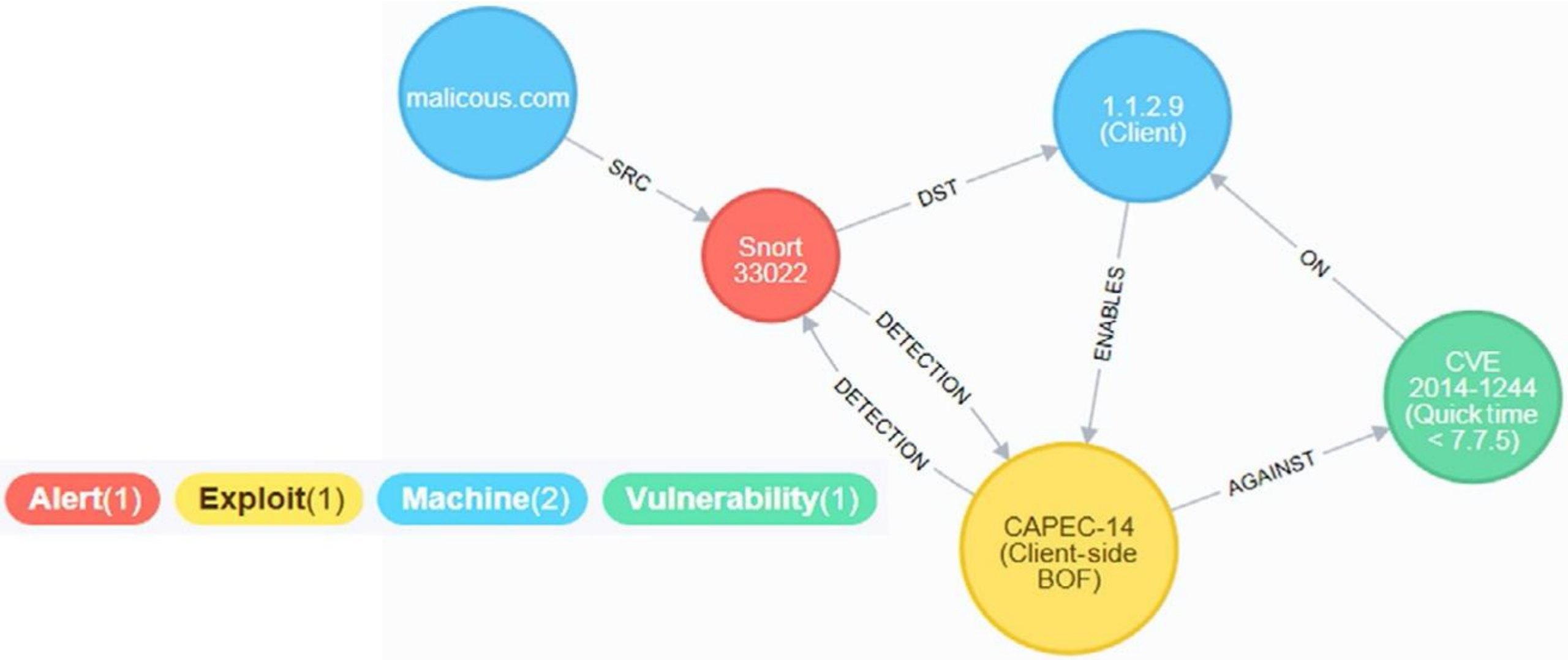
Attack graph



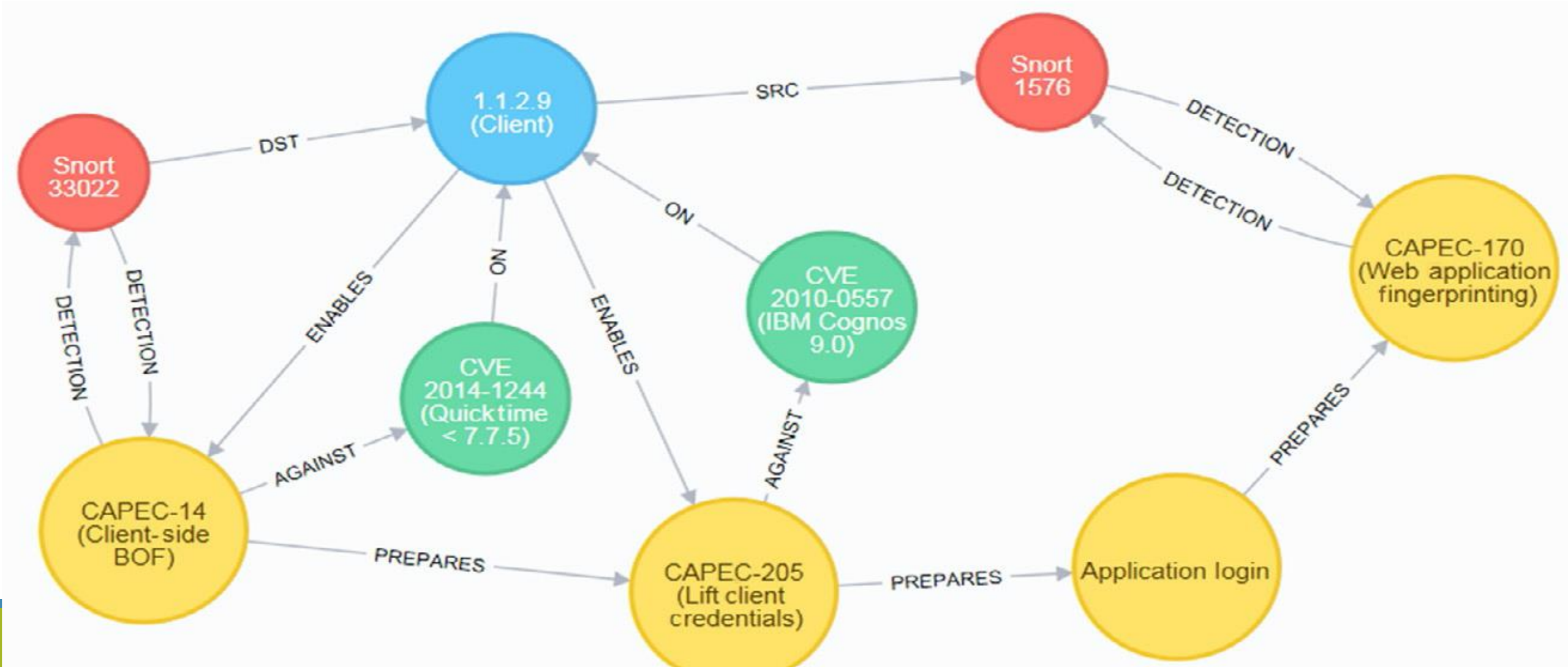
مثال کاربردی- خروجی ابزار CyGraph برای سناریوی داده شده



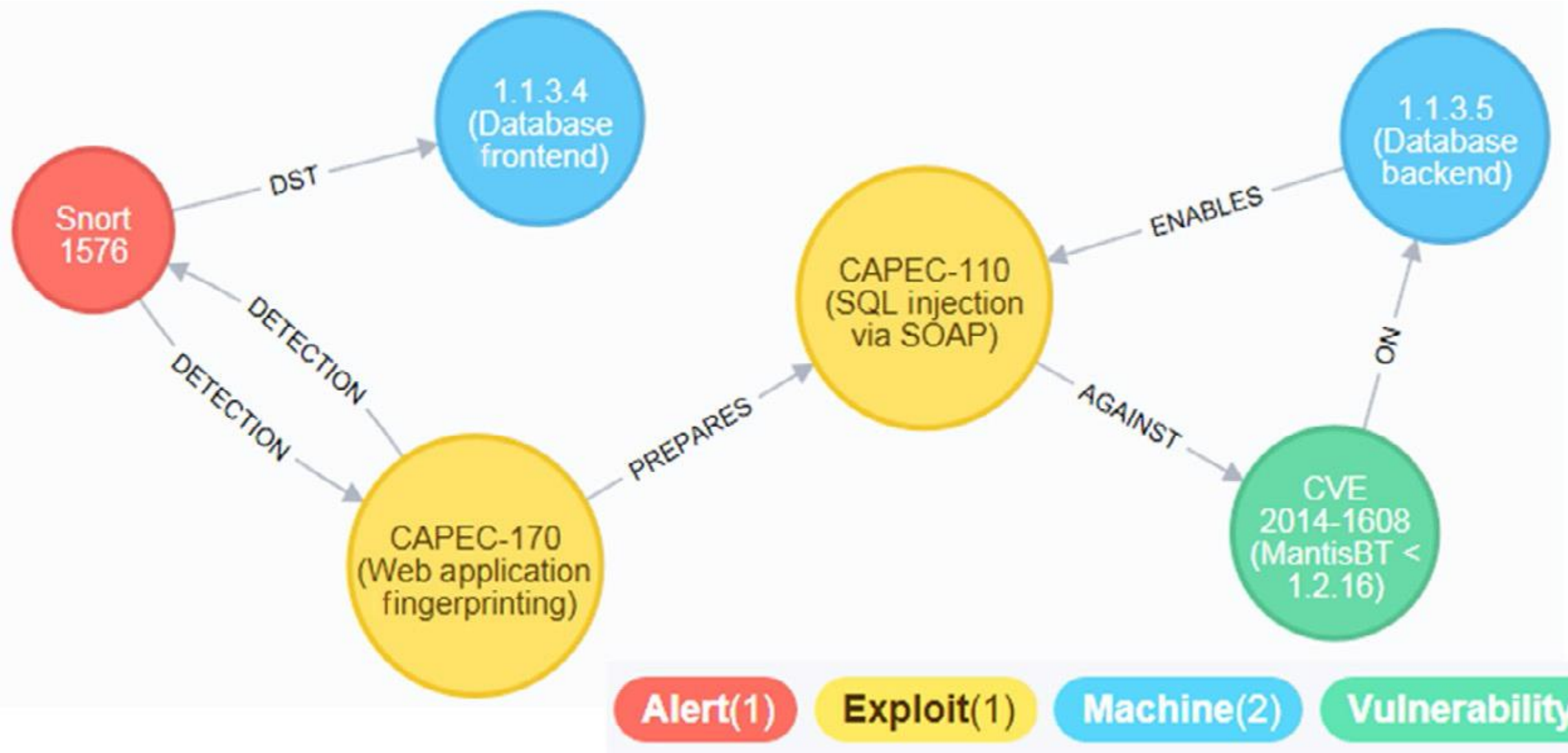
```
MATCH paths = (:Machine)-[:SRC]->
    (:Alert {name:"Snort 33022"})-[:DETECTION]->
    (:Exploit)-[:AGAINST]->
    (:Vulnerability)-[:ON]->
    (:Machine)
RETURN paths
```



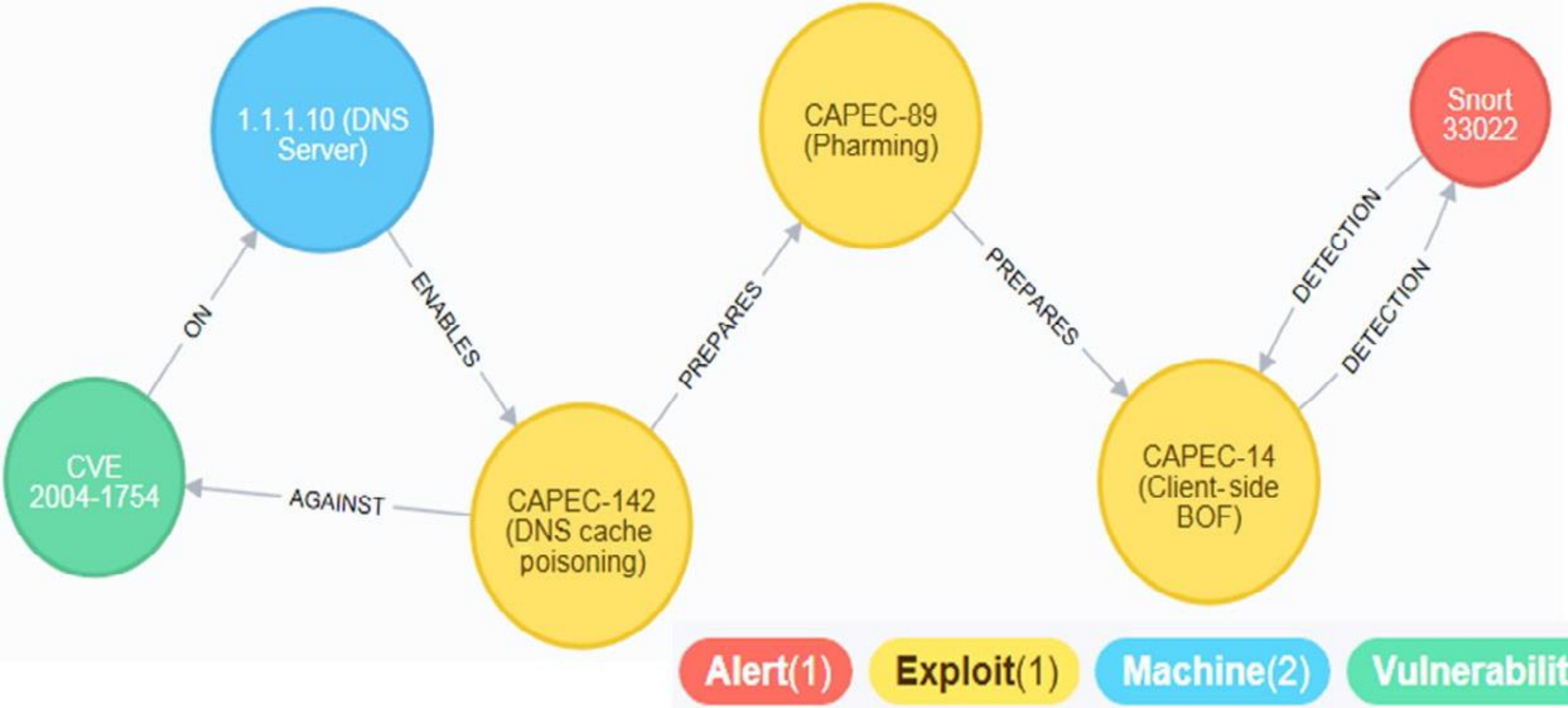
```
MATCH paths = (:Alert {name:"Snort 33022"})-
   [:SRC|DST|DETECTION|ON|ENABLES|AGAINST|PREPARES*]->
   (:Alert {name:"Snort 1576"})
RETURN paths
```



```
MATCH paths = (:Alert {name:"Snort 1576"})-
   [:DST|DETECTION|ON|ENABLES|AGAINST|PREPARES*]->()
RETURN paths
```



```
MATCH paths = ()-[:PREPARES|ON|ENABLES|AGAINST*]->
    ()-[:PREPARES]->
    (:Exploit)-[:DETECTION]->
    (:Alert {name:"Snort 1576"})
RETURN paths
```



مراجع

[1]. Mandiant Threat Report, “M-Trends 2015: A View from the Front Lines,” February 2015, Pg. 3

[2]. Kott A, Wang C, Erbacher RF, editors. “Cyber defense and situational awareness”. *Springer*; 2015 Jan 5.

[3]. Barford, P., M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, J. … Yen, 2010. “Cyber SA: Situational awareness for cyber defense. In *Cyber Situational Awareness*,” (pp. 3–14).

[4]. Jones, D., and M. Endsley. 1996. “Sources of situation awareness errors in aviation.” *Aviation, Space, and Environmental Medicine*, (67)507–512.

[5]. Skladman R, Bublitsky R, Korach H, Keshales B, inventors; Israel Aerospace Ind Ltd, assignee. “Deployable emergency situation awareness support system”. United States patent application US 16/313,684. 2019 Oct 17.

[6]. Endsley, M. R., and E. O. Kiris, 1995. “The out-of-the-loop performance problem and level of control in automation.” *Human Factors*, 37(2)381–394.

[7]. Endsley, M. R. 1995b. “Toward a theory of situation awareness in dynamic systems.” *Human Factors*, *37*(1)32–64.

مراجع

[8]. Endsley MR, Garland DJ, editors. “Situation awareness analysis and measurement.” *CRC Press;* 2000 Jul 1.

[9]. Barford P, Dacier M, Dietterich TG, Fredrikson M, Giffin J, Jajodia S, Jha S, Li J, Liu P, Ning P, Ou X. “Cyber SA: Situational awareness for cyber defense.” In *Cyber situational awareness* 2010 (pp. 3-13). Springer, Boston, MA.

[10]. Solutions, MITRE CDSA. "An Overview of MITRE Cyber Situational Awareness Solutions."

[11]. Noel S, Harley E, Tam KH, Limiero M, Share M. “CyGraph: graph-based analytics and visualization for cybersecurity.” In *Handbook of Statistics* 2016 Jan 1 (Vol. 35, pp. 117-167). Elsevier.

[12]. Musman, S. and Temin, A., 2015, April. A cyber mission impact assessment tool. In *2015 IEEE International Symposium on Technologies for Homeland Security (HST)* (pp. 1-7). IEEE.

[13]. Musman, S., Tanner, M., Temin, A., Elsaesser, E. and Loren, L., 2011, April. A systems engineering approach for crown jewels estimation and mission assurance decision making. In *2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)* (pp. 210-216). IEEE.

مراجع

[14]. Musman, S., Temin, A., Tanner, M., Fox, D. and Pridemore, B., 2010, July. Evaluating the impact of cyber attacks on missions. In *Proceedings of the 5th International Conference on Information Warfare and Security* (pp. 446-456).

[15]. Musman, S., Tanner, M., Temin, A., Elsaesser, E. and Loren, L., 2011, April. Computing the impact of cyber attacks on complex missions. In *2011 IEEE International Systems Conference* (pp. 46-51). IEEE.

[16]. Motzek, A., Möller, R., Lange, M. and Dubus, S., 2015, June. Probabilistic mission impact assessment based on widespread local events. In *NATO IST-128 Workshop on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact*.