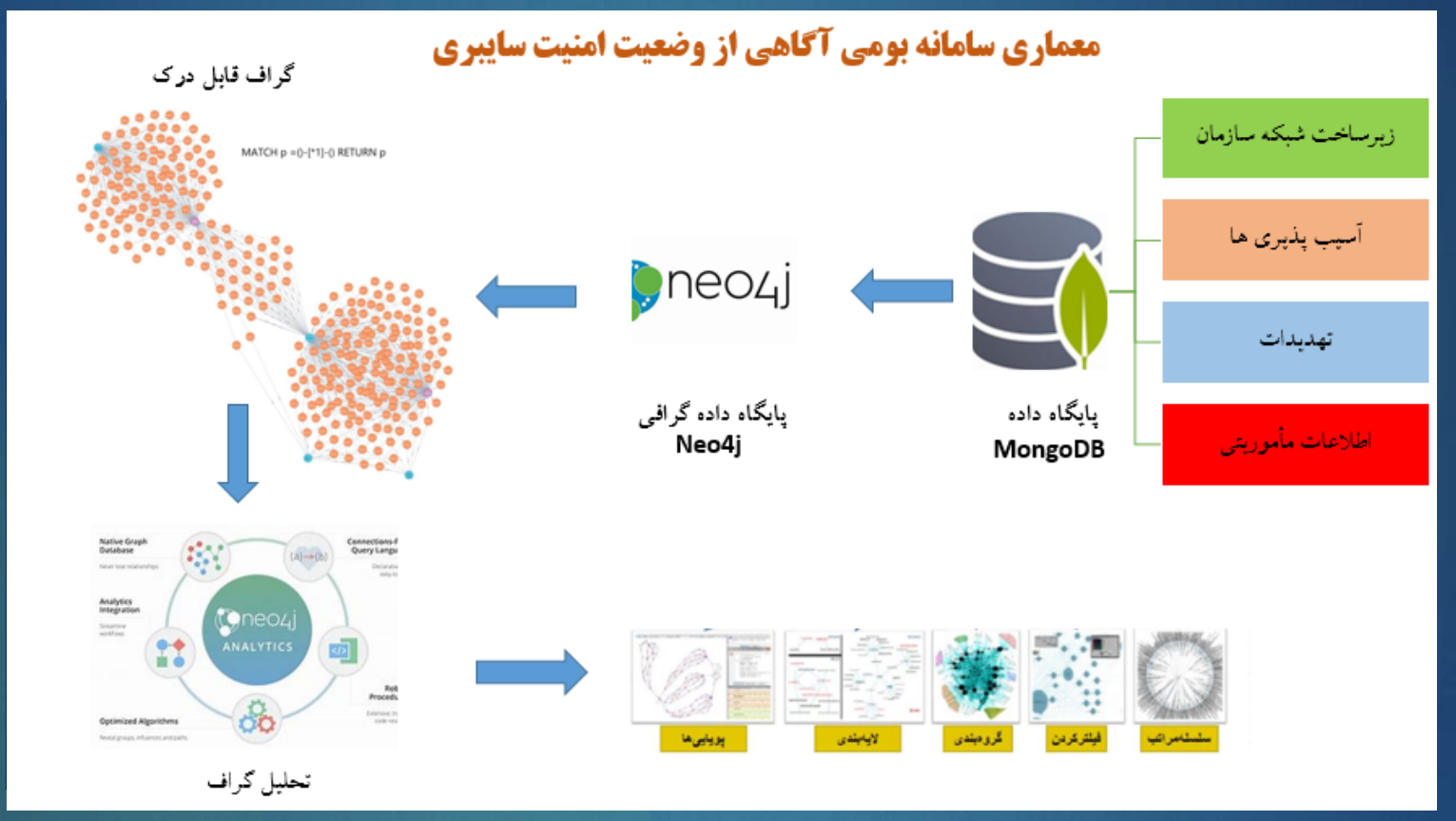
دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

محصولات فناورانه دانشگاه صنعتی امیرکبیر



عنوان طرح: تحقیق و توسعه یک سامانه بومی آگاهی وضعیت امنیت سایبری (مبتنی بر مدل آگاهی وضعیت اِندزلی)

نام مجری و همکاران : مرکز پژوهشی آپا دانشگاه صنعتی امیرکبیر

دکتر بابک صادقیان، دکتر مطهره دهقان

(و با همکاری تیم ۷ نفره از دانشجویان)

محصولات فناورانه

دانشگاه صنعتی امیرکبیر

معرفی طرح:

سامانه ها و شبکه های کامپیوتری بسیار پیچیده هستند و سیّار شدن دستگاه ها پیچیدگی ها را افزایش داده است. ازطرف دیگر، با افزایش تعداد و پیچیدگی و پنهان ماندن فعالیت های موذی سایبری، لزوم تصمیم گیری برای اقدام مناسب و اعمال مناسب مکانیزم های امنیتی در مقابله با تهدیدات سایبری اهمیت چشم گیری یافته است. برای دفاع از شبکه‌ها و سامانه ها، شَناسایی تمام دارایی‌های حیاتی سامانه ها، و انتساب ها و ناهنجاری‌های مرتبط با کاربری ضروری است. آگاهی ناقص یا ناکافی از وضعیت سایبری و تاثیر تهدیدات سایبری بر ماموریت یک سازمان، یکی از دلایل عمده برای عدم تصمیم گیری و اقدام مناسب و به-هنگام در مقابله با تهدیدات سایبری است. از اینرو، آگاهی از وضعیت امنیت سایبری بعنوان یک مولفه مهم برای امنیت سامانه های سایبری در نظر گرفته میشود.

حوزه آگاهی از وضعیت امنیت سایبری یکی از حوزه های مربوط به امنیت سایبر است که در سندهای دولت ایالات متحده آمریکا تحت عنوان: " طرح استراتژیک تحقیق و توسعه امنیت سایبری فدرال" (نشرهای سند از ۲۰۱۶ تا کنون که هر چهار سال مورد بازنگری و اصلاحات بوده) به عنوان یک حوزه استراتژیک برای تحقیق و توسعه در زمینه امنیت سایبر مورد تاکید قرار گرفته است.

با توجه به مطالعات صورت گرفته در مرکز پژوهشی آپا دانشگاه صنعتی امیرکبیر، ابزار CyGraph از محصولات شرکت MITRE به عنوان یک ابزار قابل توجه بدین منظور شناسایی گردید. از آنجا که فروش این ابزار به ایران جزو موارد تحریمی و ممنوع میباشد، تحقیق و توسعه برای بومی سازی و مهندسی این ابزار و انتقال دانش و تکنولوژی مربوط به آن با توجه به مقالات منتشره در رابطه با آن وجهه همّت این مرکز پژوهشی قرار گرفت.

ابزار CyGraph پس از پردازش و ادغام اطلاعات بدست آمده از زیرساخت شبکه، تهدیدات، آسیب پذیری ها، مأموریت ها و دارایی های سازمان، قابلیت های موثری را برای بررسی وضعیت امنیت سایبری فراهم می کند. ابزار CyGraph مبتنی بر مدل اندزلی طراحی شده است که در آن سه سطح ادراک، فهم و تجسم آینده نزدیک برای آگاهی وضعیت در نظر گرفته میشود. در این طرحَ سامانه بومی با هدف بازآفرینی ابزار CyGraph برای آگاهی از وضعیت امنیت سایبری تحقیق و توسعه داده شده است.

کاربرد:

سامانه آگاهی از وضعیت امنیت سایبری برای نهادهای با زیرساخت شبکه کامپیوتری و با دارایی های سایبری و همچنین دارای اهداف مأموریتی مشخص، جهت بهبود وضعیت امنیت سایبری، تصمیم گیری و اقدام عملی مناسب و به‌موقع ضروری است. از آن‌جا که این نهادها به دلیل ماهیت سایبری خود، در معرض آسیب پذیری ها و تهدیدات متنوع، پیچیده و در حال پیشرفت هستند، لزوم بکارگیری سامانه آگاهی از وضعیت امنیت سایبری برای چنین نهادهایی، یک نیاز اساسی است.

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

محصولات فناورانه
دانشگاه صنعتی امیرکبیر

بررسی بازار عرضه و تقاضای محصول (فناوری):

سامانه آگاهی از وضعیت امنیت سایبری برای نهادهای با زیرساخت شبکه کامپیوتری و با دارایی های سایبری و همچنین دارای اهداف مأموریتی مشخص، جهت بهبود وضعیت امنیت سایبری، تصمیم گیری و اقدام عملی مناسب و به-هنگام ضروری است. از آن‌جا که این نهادها به دلیل ماهیت سایبری خود، در معرض آسیب پذیری ها و تهدیدات متنوع، پیچیده و در حال پیشرفت هستند، لزوم بکارگیری سامانه آگاهی از وضعیت امنیت سایبری برای چنین نهادهایی، یک نیاز اساسی است.
در کشور ما تاکنون، چنین سامانه ای با تطابق بر مدل اندزلی توسعه داده نشده است و ما در مرکز پژوهشی آپا برای اولین بار سامانه آگاهی از وضعیت امنیت سایبری با تطابق بر مدل اندزلی را توسعه داده ایم.
این سامانه برای محیط دانشگاه صنعتی امیرکبیر مورد ارزیابی قرار گرفته است و توانایی های آن نشان داده شده است.

سطح بلوغ فناوری در کدام مرحله است (.....:TRL):

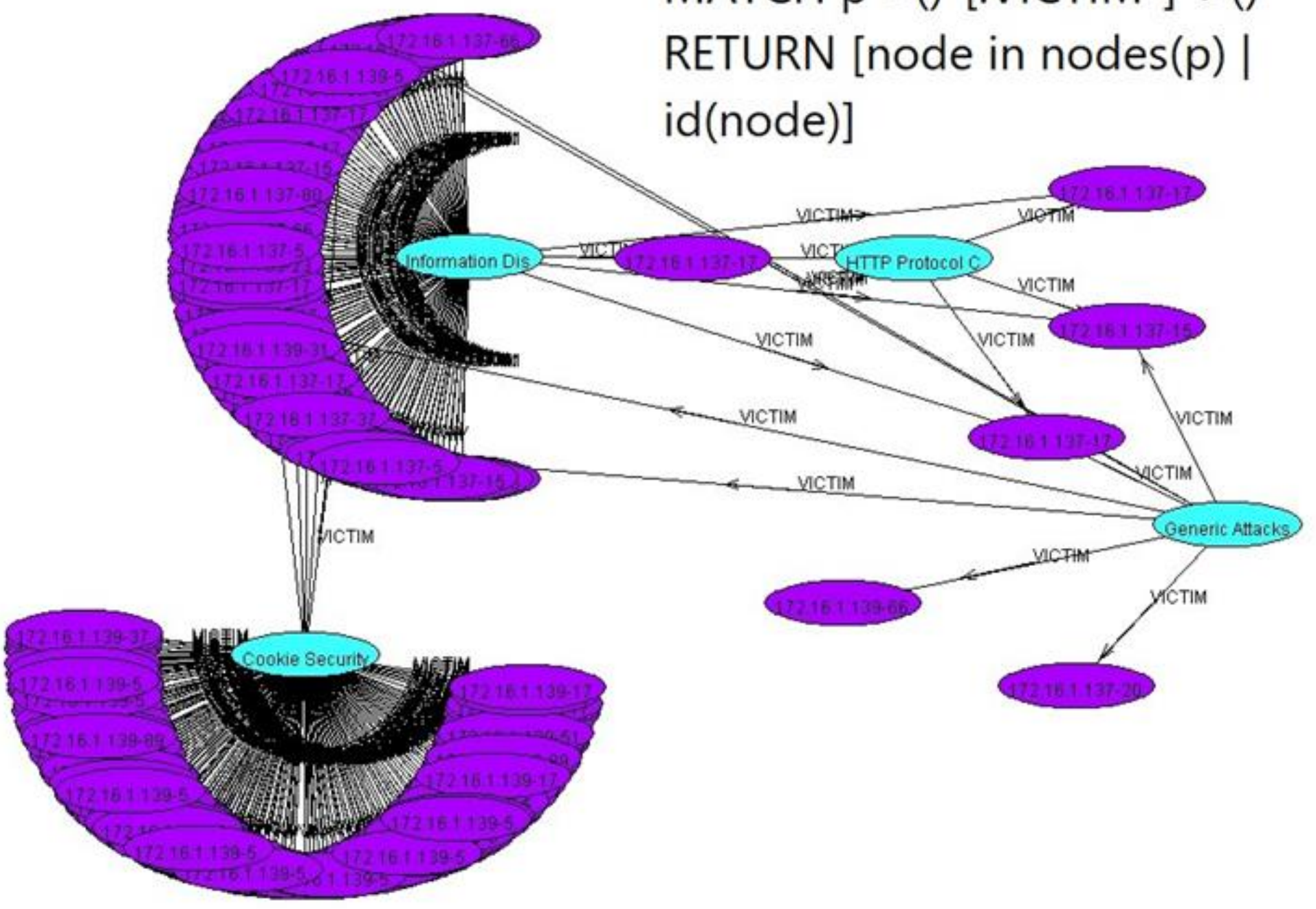
- ❑ در مرحله تحقیق و توسعه (R&D)
- ❑ در مرحله تولید نیمه صنعتی (پایلوت) (ظرفیت تولید فعلی در ماه .....):
- ❑ نمونه آزمایشگاهی
- ❑ در مرحله تولید انبوه (ظرفیت تولید فعلی در ماه:.....)
- ■ وجود یک نمونه با قابلیت استفاده در شرایط واقعی
- ❑ سایر .....

❑ ثبت اختراع داخلی / خارجی با شماره ثبت ..... و سال ثبت .....

**** تصویری از محصول پیوست شود (الزامی) و در صورت وجود فیلم آن نیز به همراه فرم ارسال گردد.**

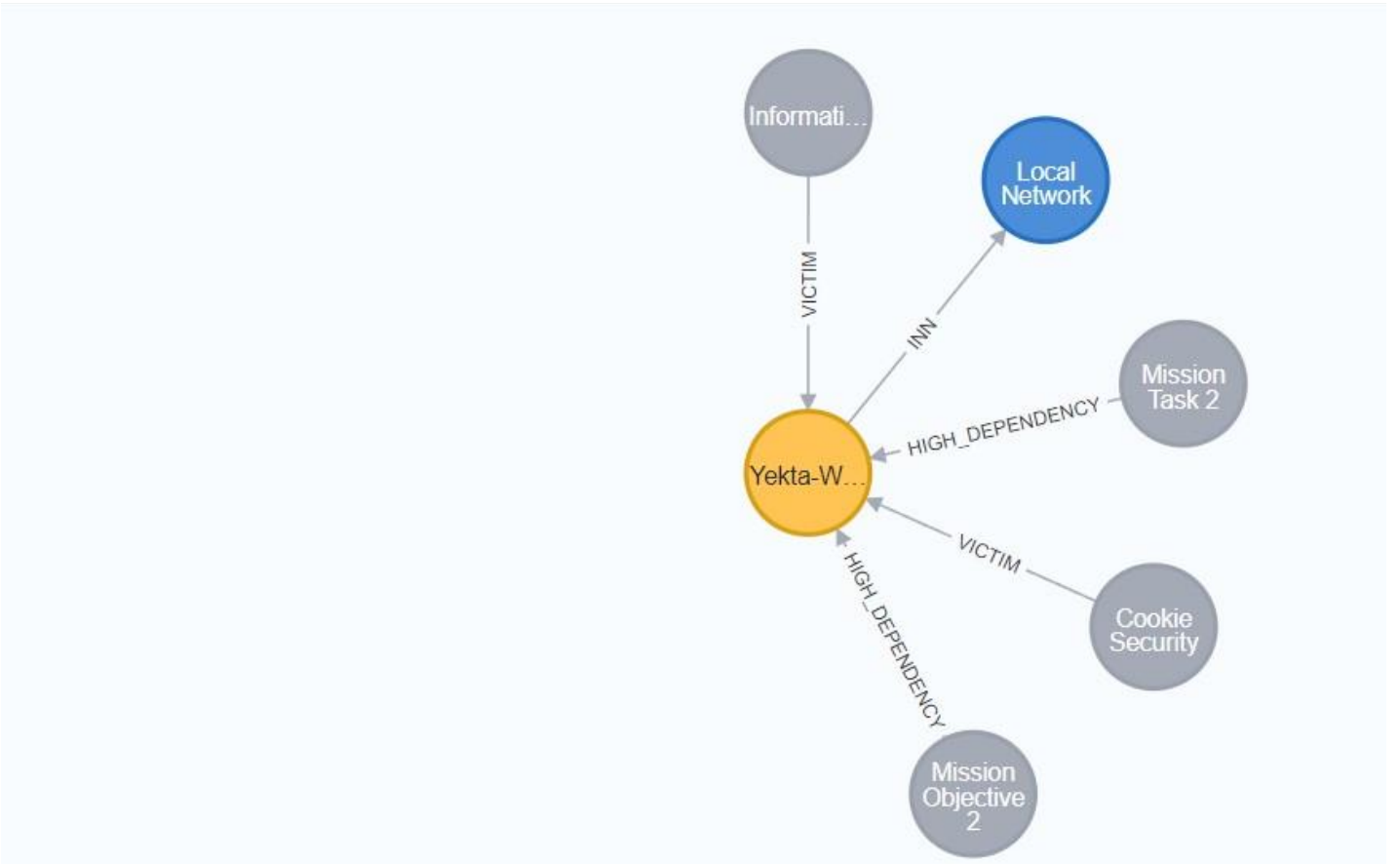
نمونه پرس و جو و خروجی های سامانه

```
MATCH p =()-[:VICTIM*]->()
RETURN [node in nodes(p) |
id(node)]
```



نمونه پرس و جو و خروجی های سامانه

MATCH p = () – [*2] – (ATTACK_PATTERN{name: “Cookie Security”}) RETURN p



نمونه صفحه کاربری سامانه

تسهیل پرسمان کاربری