CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Sachin Shetty

Old Dominion University

sshetty@odu.edu

April 10, 2019

Cyber Risk Scoring and Mitigation(CRISM)

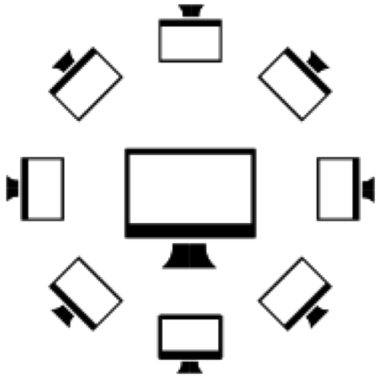
Customer Need - Life in the Security Operation Center

Intrusion Detection System alerts

Users and data assets

Prioritized Mitigation Plan

Network configuration



Vulnerability reports

Apache HTTP Server 2.4 vulnerabilities

Security advisories

Market Needs

- Security metrics will play a key role in supporting *risk management* and *mitigation* decisions for critical infrastructure

- Availability of quantitative insights ensure *operational resilience* and assist in development of cost-effective mitigation plan.

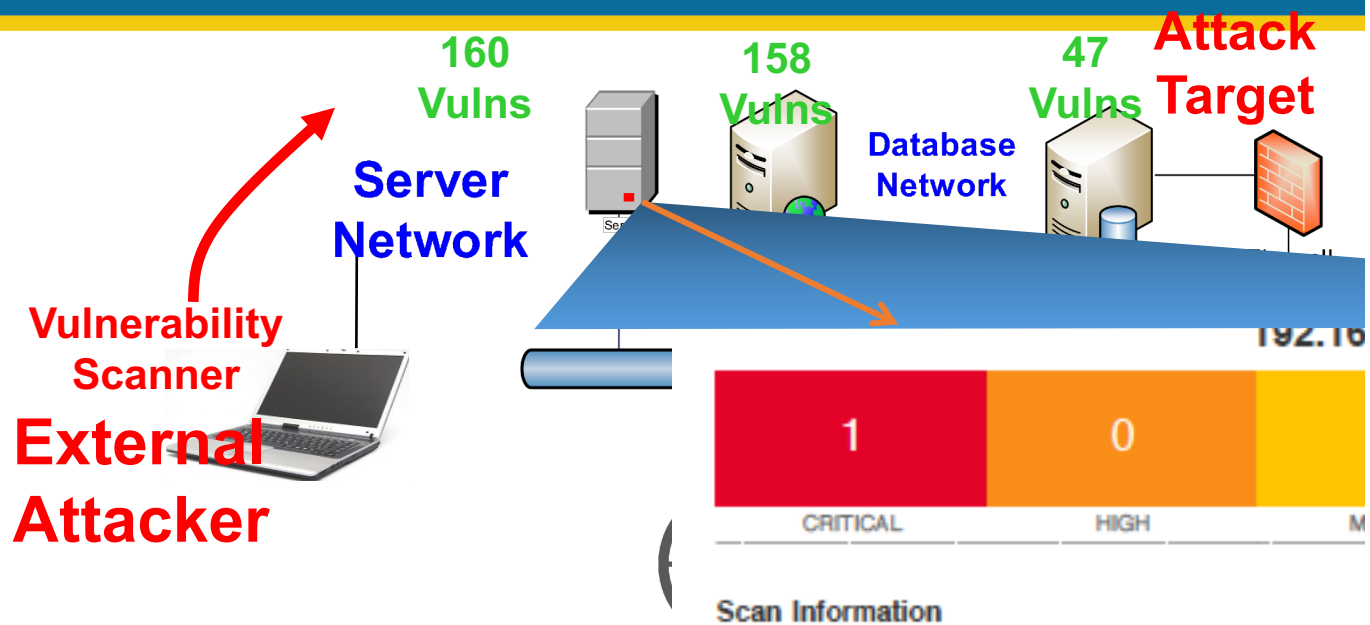
- IT and OT organizations need tools to aid in *continuous assessment* their cyber resilience capabilities

Approach

Vulnerability List

IP Address	Vulnerability	Risk	Fix Information
10.0.0.16	Discard port open CVE-1999-0636	10	GO
10.0.0.16	IIS .IDA ISAPI filter applied CVE-2001-0500	10	GO
10.0.0.16	Windows NT NNTP Component Buffer Overflow CVE-2004-0574	10	GO
10.0.0.16	Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote CVE-2008-411	10	GO
10.0.0.16	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468) CVE-2010-002	10	GO
10.0.0.16	Message Queuing Remote Code Execution Vulnerability (951071) - Remote CVE-2008-3479	10	GO
10.0.0.16	Microsoft IIS FTPd NLST stack overflow CVE-2009-3023	9.3	GO

- Quantitatively analyze *cyber risk* of company's hardware and software systems
- Provide *security scores* provided at several levels of granularity
- Provide prioritized mitigation plan to reduce cyber risk and improve cyber resilience
- Adapt to diverse network configurations and dynamically scaling cloud environments



192.168.148.137

5	0	2	0
CRITICAL	HIGH	MEDIUM	LOW

Scan Information

Start time:	Tue Sep 4 20:06:18 2018
End time:	Tue Sep 4 20:08:03 2018

Host Information

Netbios Name:	ORG-JLF9I0GWXFM
IP:	192.168.148.137
MAC Address:	00:0C:29:73:D8:AA
OS:	Microsoft Windows XP Service Pack 2, Microsoft Windows XP S XP for Embedded Systems

1	0	
CRITICAL	HIGH	M

Scan Information

Start time:	Tue Sep 4 20:06:18 2018
End time:	Tue Sep 4 20:12:53 2018

Host Information

Netbios Name:	USER-PC
IP:	192.168.148.136
MAC Address:	00:0C:29:8E:C8:41
OS:	Microsoft Windows 7 Professional

Scanner

41 Vulns

15 Vulns

192.168.148.139

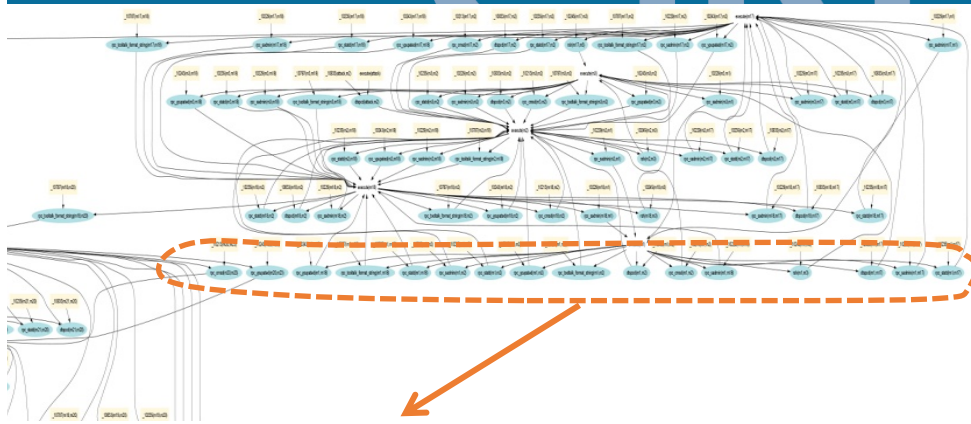
8	5	19	7	120
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Tue Sep 4 20:06:18 2018
End time: Tue Sep 4 20:15:23 2018

Host Information

Netbios Name: METASPLOITABLE
IP: 192.168.148.139
MAC Address: 00:0C:29:45:E9:DD
OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)



192.168.217.139

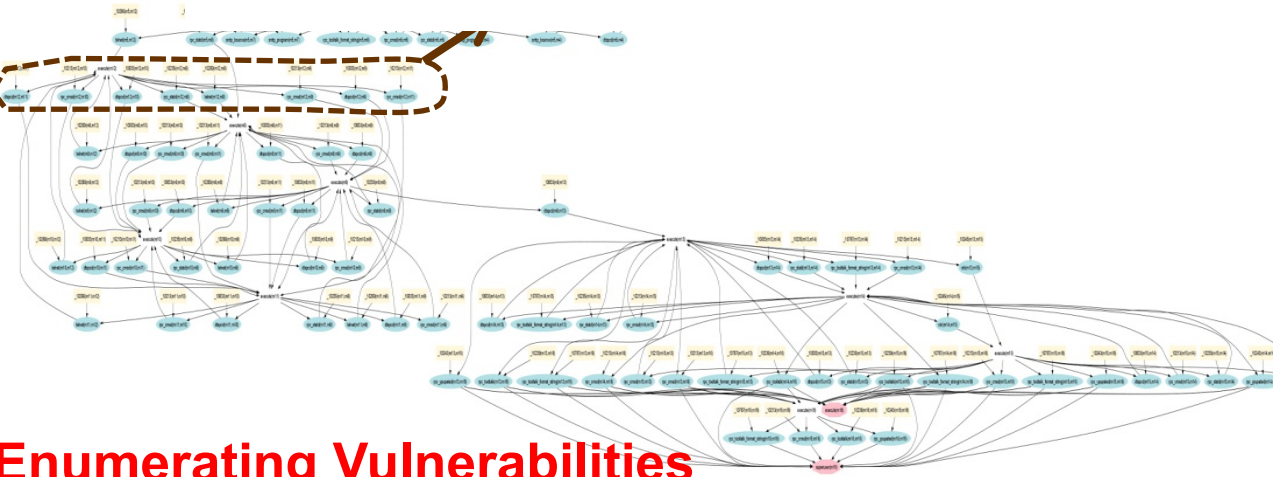
1	2	10	3	65
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Tue Sep 4 20:06:18 2018
End time: Tue Sep 4 20:24:45 2018

Host Information

IP: 192.168.217.139
OS: Linux Kernel 3.0 on Ubuntu 12.04 (precise)



Enumerating Vulnerabilities Misses the Big Picture!

Requirements

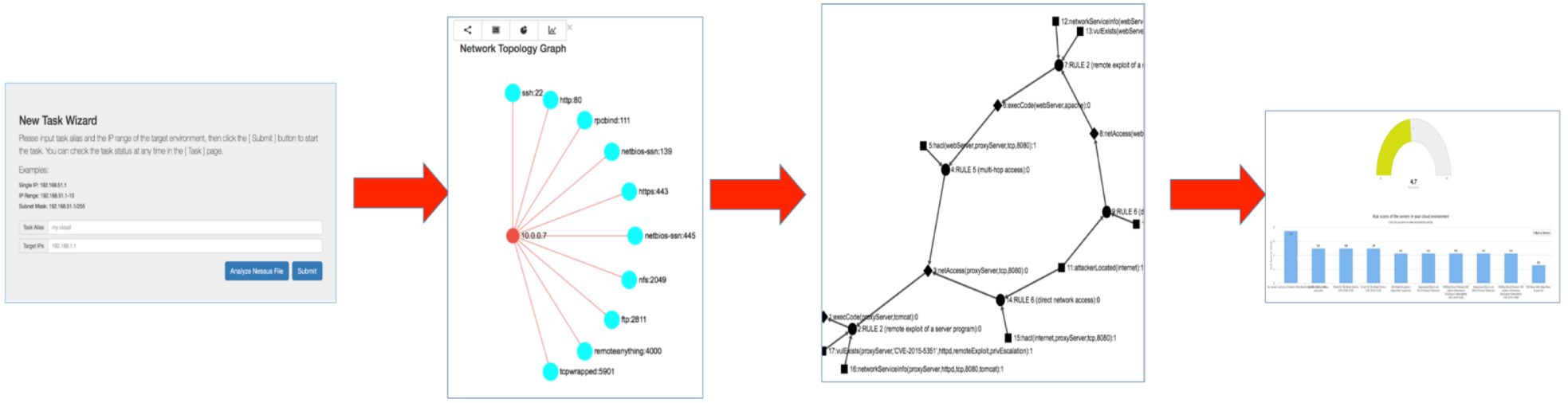
- Lateral propagation analysis
  - Analysis provides information on stepping-stones, pivot points, attack paths, vulnerable nodes that provides insights into adversarial strategies
- Security metrics
  - Quantification of attack surfaces based on exploitability and impact analysis
- Prioritized mitigation plan
  - Ordered list of vulnerabilities to patch or apply security controls to achieve a desired security score.
- Compliance with NIST cyber security framework

Potential Solutions

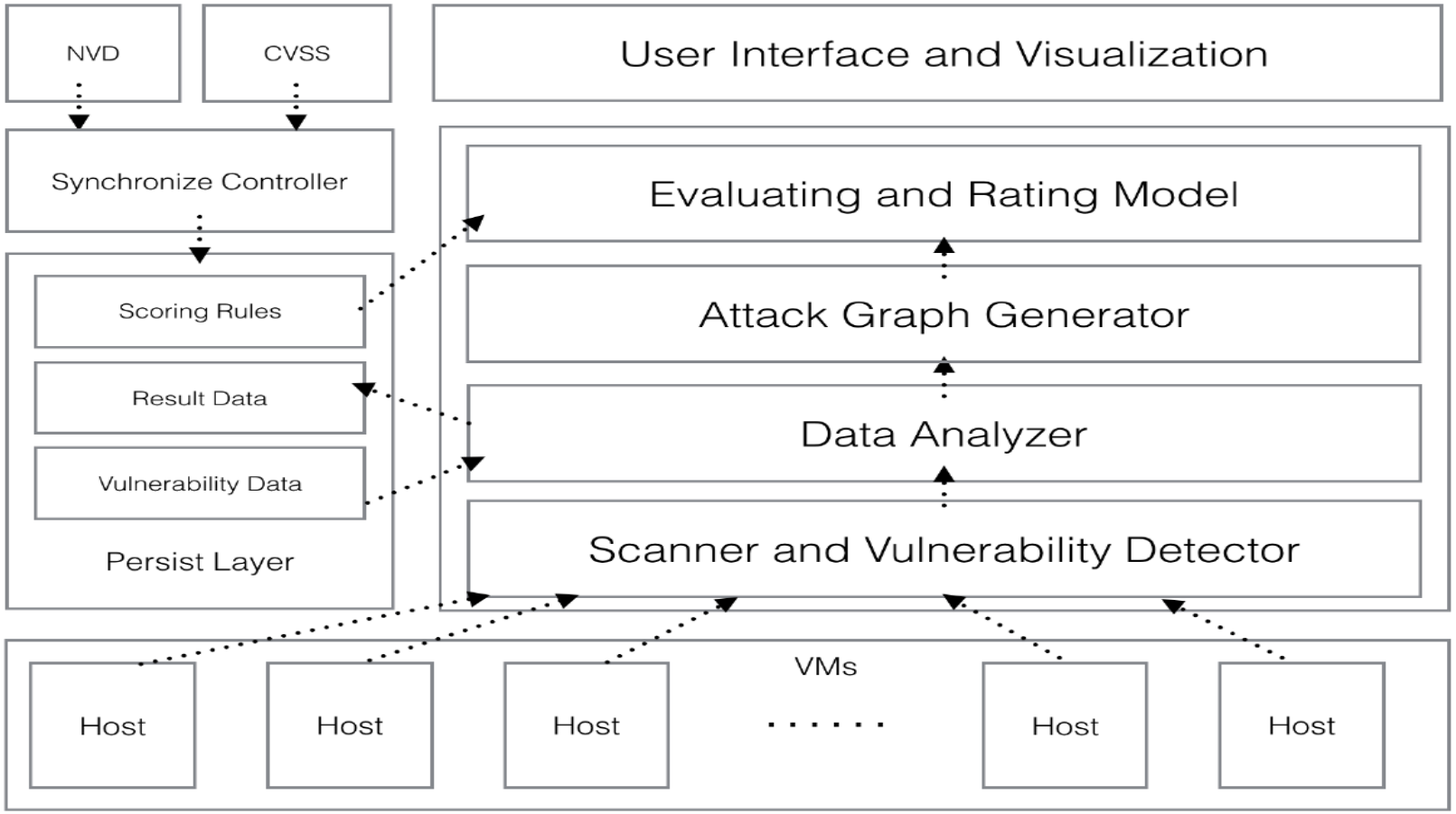
	Cyber Risk analysis based on lateral propagation analysis	Scoring based on vulnerability graphs	Prioritize mitigation plan	Identify most vulnerable paths and nodes	Impact analysis based on asset importance	Quantify and visualize risk scores at several levels of granularities
CRISM	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓
Quadmetrics	✓✓	✓✓	✗	✗	✗	✓✓✓
Bitsight	✓✓	✓✓	✗	✗	✗	✓✓✓
SecurityScorecard	✓✓	✓✓	✗	✗	✗	✓✓✓
Efortresses	✓✓	✓✓	✗	✗	✗	✓✓✓
Beyond Security	✓✓	✓✓	✗	✗	✗	✓✓✓
Nexpose	✓✓	✓✓	✓✓✓	✗	✗	✓✓✓
Core Security	✓✓	✓✓	✓✓✓	✗	✗	✓✓✓

Cyber RIsk Scoring and Mitigation (CRISM©)

- Provides cyber security scores and prioritized mitigation plan
- Works with diverse software, networking and cloud environment.
- Provides quantitative risk assessment and categorizes attack paths based on the impact of vulnerabilities



CRISM© Architecture Components

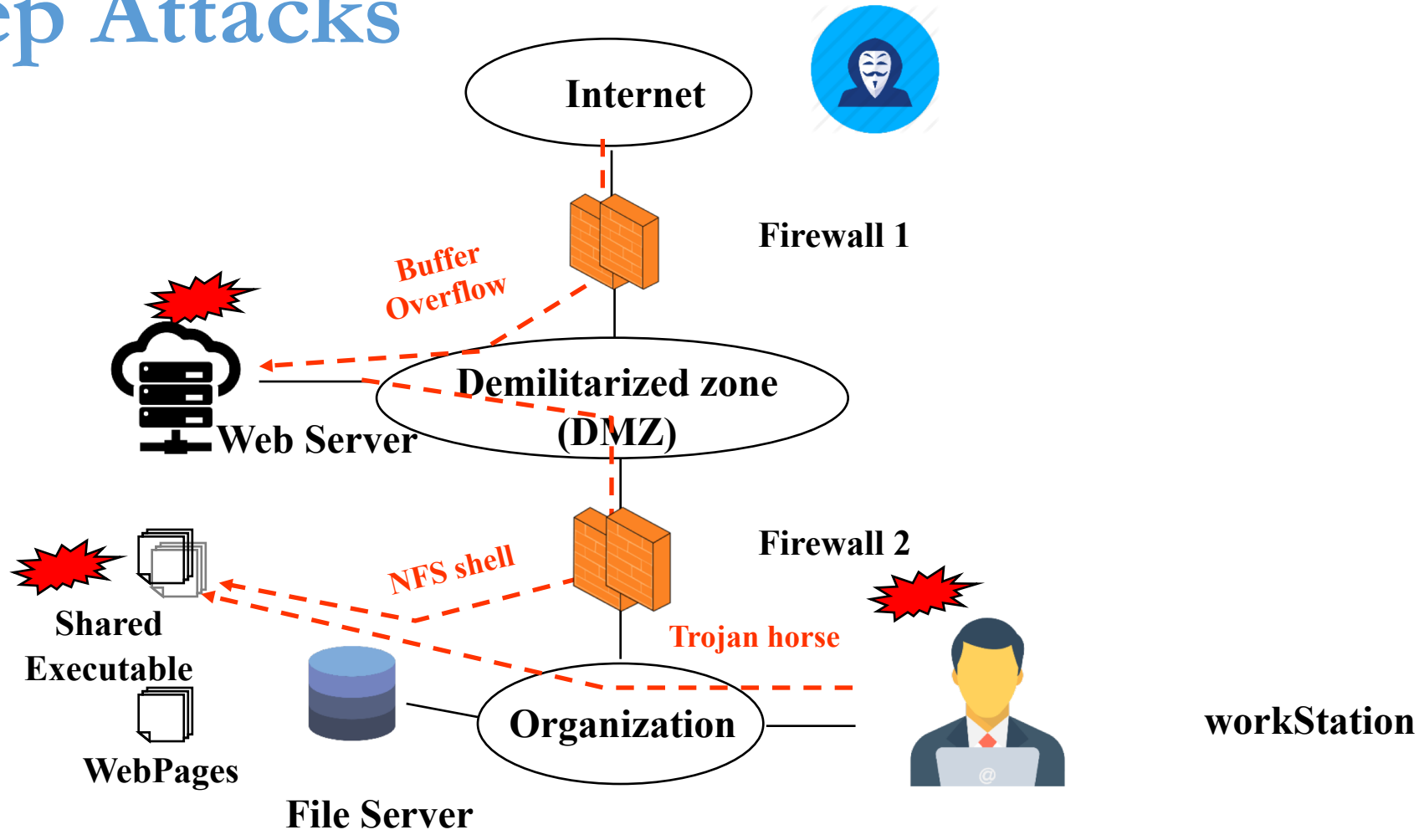


Sachin Shetty, Michael McShane, Linfeng Zhang, Jay Kesan, Charles A. Kamhoua, Kevin Kwiat, Laurent Njilla, " Reducing Informational Disadvantages to Improve Cyber Risk Management", Geneva Papers on Risk and Insurance, April 2018, Volume 43, Issue 2, pp 224–238

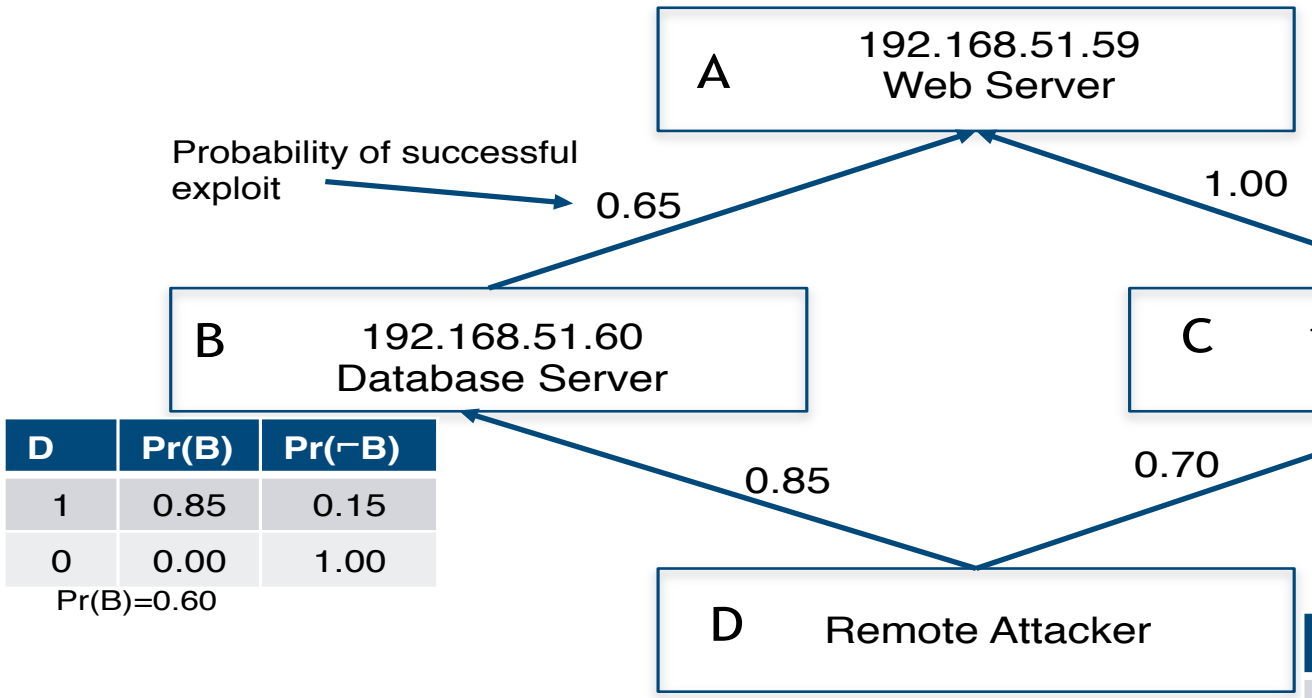
Measure Cyber Risk - Attack Graphs

- Adversaries penetrate network through a chain of exploits
  - Each exploit lays foundation for subsequent exploits
- Chain is called an attack path
- All possible attack paths form an attack graph
- Generate attack graphs to mission critical resources
- Report only those vulnerabilities associated with the attack graphs

Multi-step Attacks



Bayesian Attack Graph



B	C	Pr(A)	Pr(¬A)
1	1	1.00	0.00
1	0	0.65	0.35
0	1	1.00	0.00
0	0	0.00	0.00

Pr(A)=0.61 Unconditional Probability

D	Pr(B)	Pr(¬B)
1	0.85	0.15
0	0.00	1.00

Pr(B)=0.60

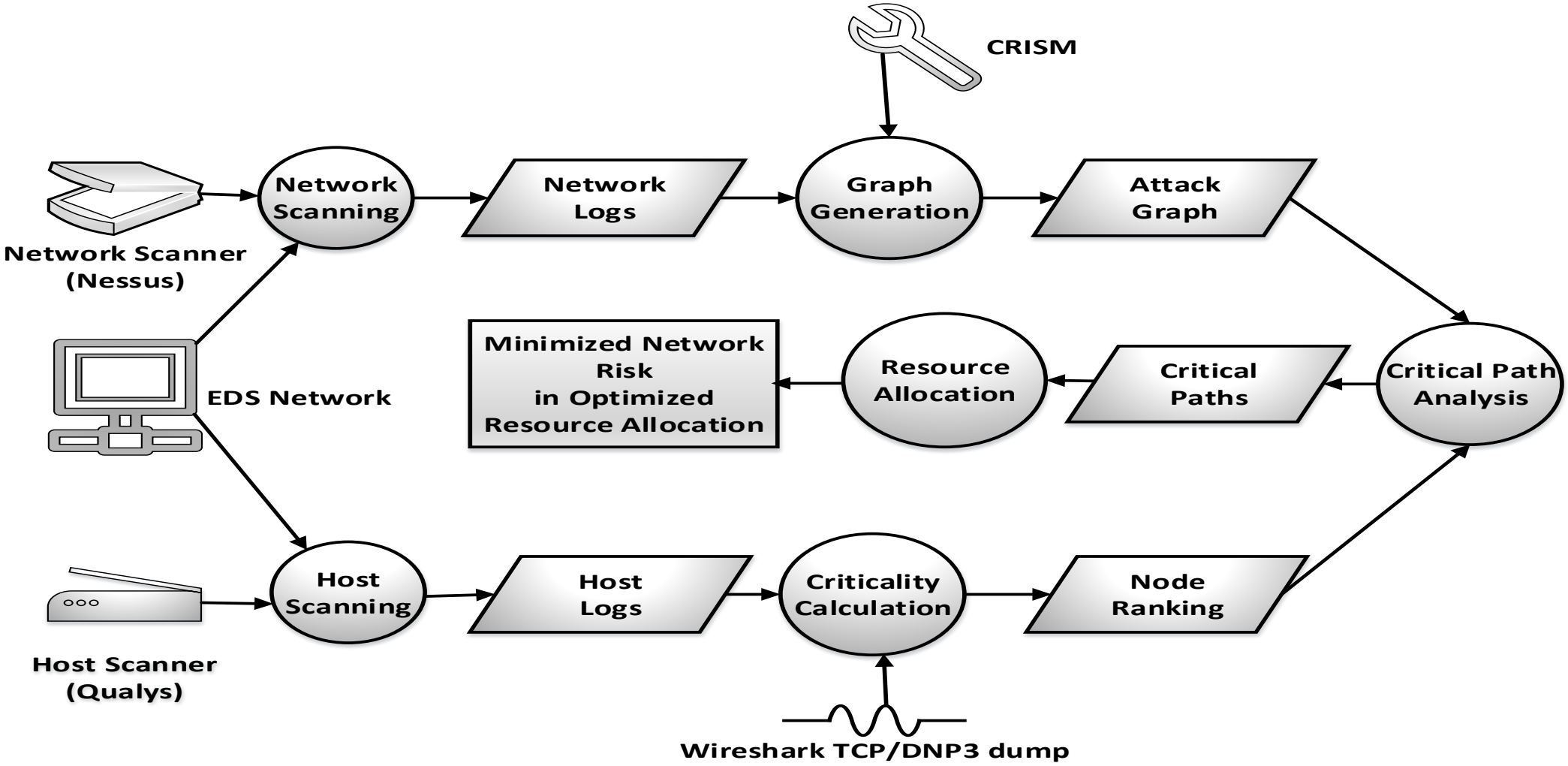
D	Pr(C)	Pr(¬C)
1	0.70	0.30
0	0.00	1.00

Pr(C)=0.49

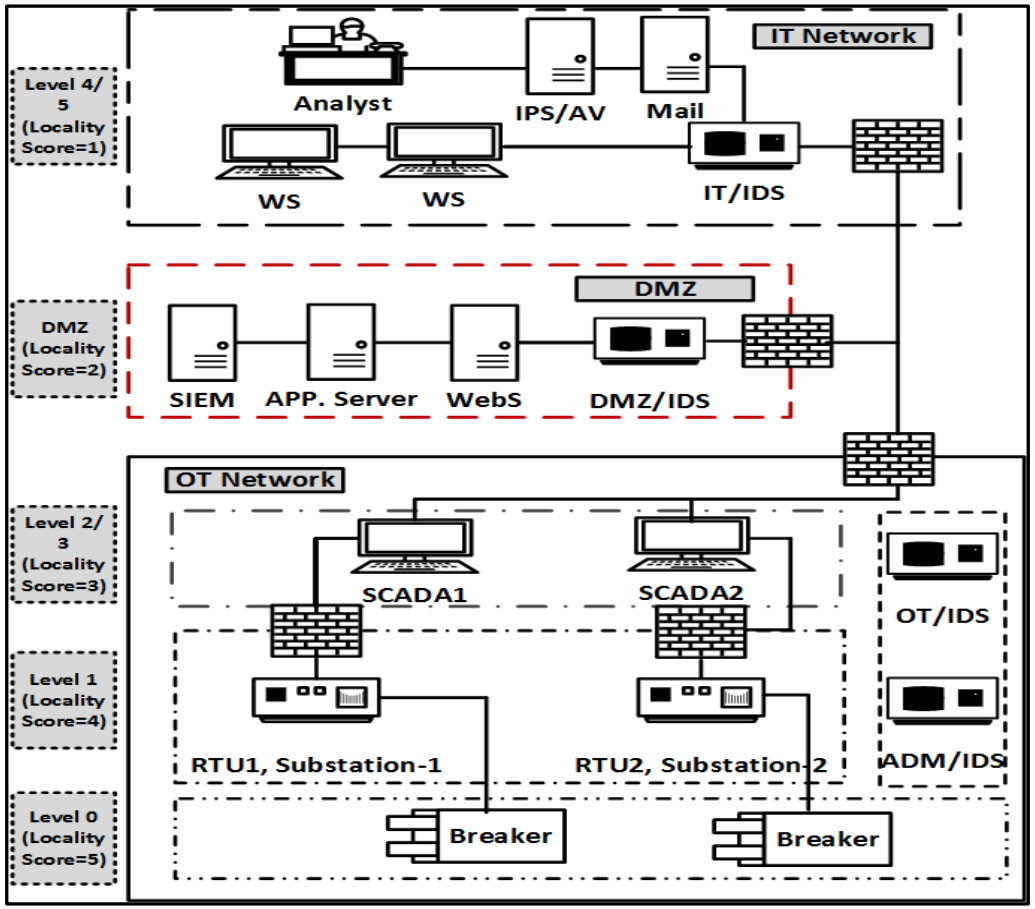
Pr(D)	Pr(¬D)
0.70	0.30

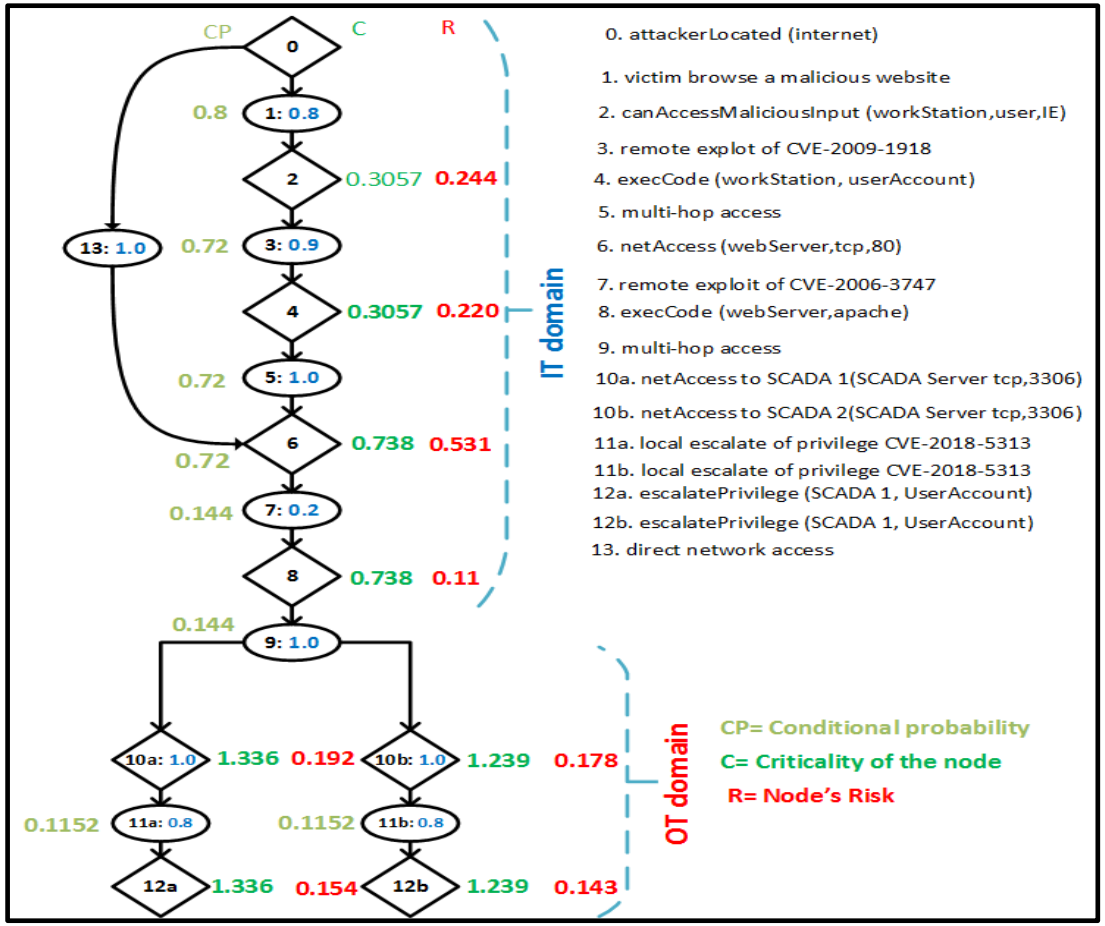
Pr(D)=0.70

Criticality Analysis



Criticality Analysis





Cyber RIsk Scoring and Mitigation (CRISM©)

Challenges	Solutions
Automatic Identification of Attack Surfaces	Acquisition of vulnerability scores from live threat intelligence feeds and vulnerability databases
Lateral Propagation Analysis	Network Vulnerability Tests and attack graph generation
Security Metrics and Prioritized Mitigation Plan	Bayesian attack graph modeling techniques to categorize attack paths by impact, cost and degree of difficulty
Compliance	NIST Cybersecurity Framework
On demand and real-time access to quantifiable cyber risks	Cloud based risk assessment tool

CRISM Benefits

- Distills *complex threat analysis* processes into numerical risk score.
- Provides a detailed, *prioritized mitigation plan*.
- Employs *visualization* techniques to ensure information synthesis.
- Provides insights into risk posed by external vs. insider adversaries
- Adaptable in diverse network configuration, low overhead and scalable

Transition Activities

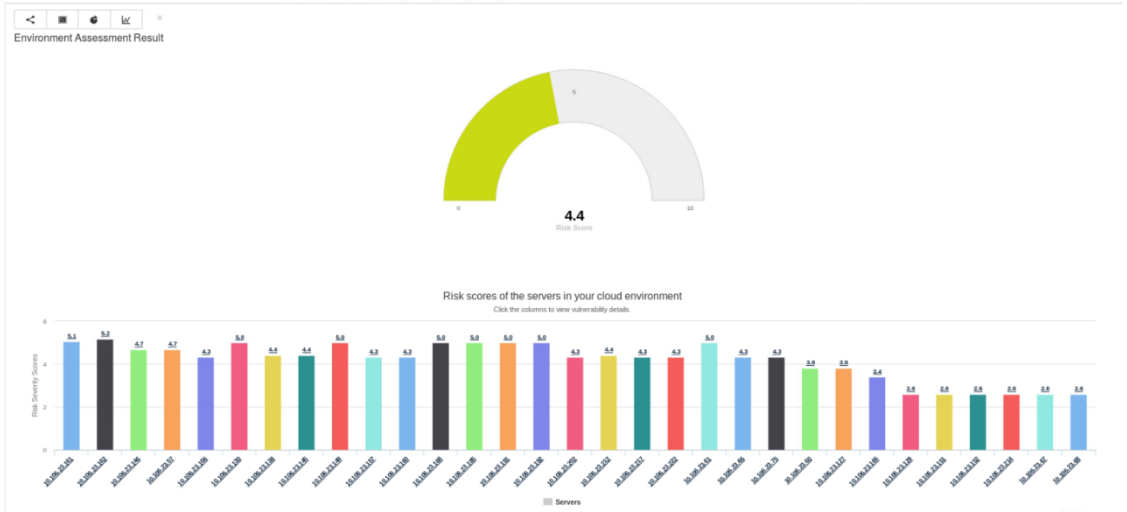
- CRISM© is property of ODU
- Software License available from www.crism.org
- Patent Pending
- Working with CIRI on commercialization plan

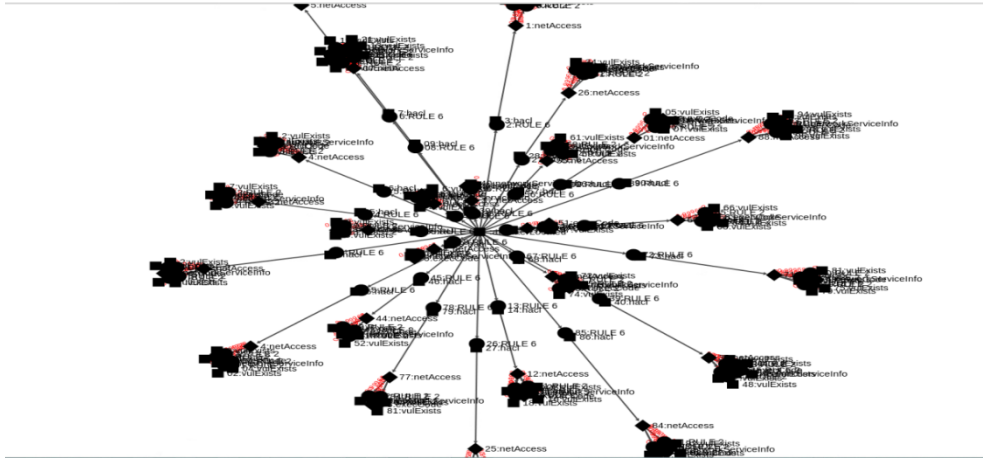
Transition Activities

- **FBI (Norfolk Cyber Crime Unit)**- Scalable testing of CRISM© on a network with 100 nodes
- **Sentara Health** – Evaluation of CRISM© in production environment
- **Naval Surface Warfare Center Crane** – CRISM© demonstration at Glendora Lake Test Facility
- **Accenture** – Evaluation of CRISM© for OT customers

Evaluation of CRISM at Sentara Healthcare

- Sentara Healthcare serves over 2 million residents in 100 sites in Virginia and North Carolina
- Interested in complementary suite of tools that provide security risk assessment and prioritized mitigation plan
- Evaluation on Sentara Healthcare's cyber infrastructure
  - Production IT systems at Norfolk site running diverse Windows and Linux distributions
  - Complement to Nessus





Evaluation of CRISM at Sentara Healthcare

Test Cases	Date	Duration	Objective	Summary
Test 1	Jun 15,2018	3:30 – 5:45	Test effectiveness of CRISM in Sentara's IT cyber infrastructure	37 nodes, 65 vulnerabilities
Test 2	Jun 21, 2018	11:07 – 13:38	Estimate the total time for assessing target machines with mix of different OS (Windows & Linux)	Scanning time – approximately 2 hours and 30 minutes
Test 3	June 22,2018	11:33 – 13:50		
Test 4	July 27, 2018	14:36 – 15:17	Develop test scenarios with varied combinations of mission specific IT configurations	Two groups of OS i.e. Windows and Linux. There are 6 nodes in each group. Windows group took less time than Linux group.
Test 5	Dec 12, 2018	10:37 – 18:17	Conduct live testing on operational environments , Conduct maximum capacity testing with varying application traffic speeds and incoming connections .	167 nodes, 111 vulnerabilities, scanning time – approx. 9.5 hours.

Summary

- Deployment of CRISM in additional Sentara Healthcare sites in Virginia
- Aiding Sentara sites without a full fledged security team with easy to digest analytics that provide increased visibility into risk and strength of existing defenses
- Exploring with Accenture on deployment of the tool in the power utility sector.