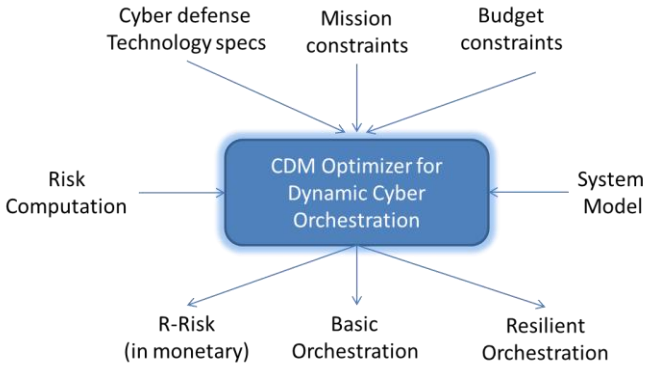
Automated Decision Making for Optimizing Orchestration of Cyber Defense Matrix

PI: Ehab Al-Shaer, UNC Charlotte, ealshaer@uncc.edu

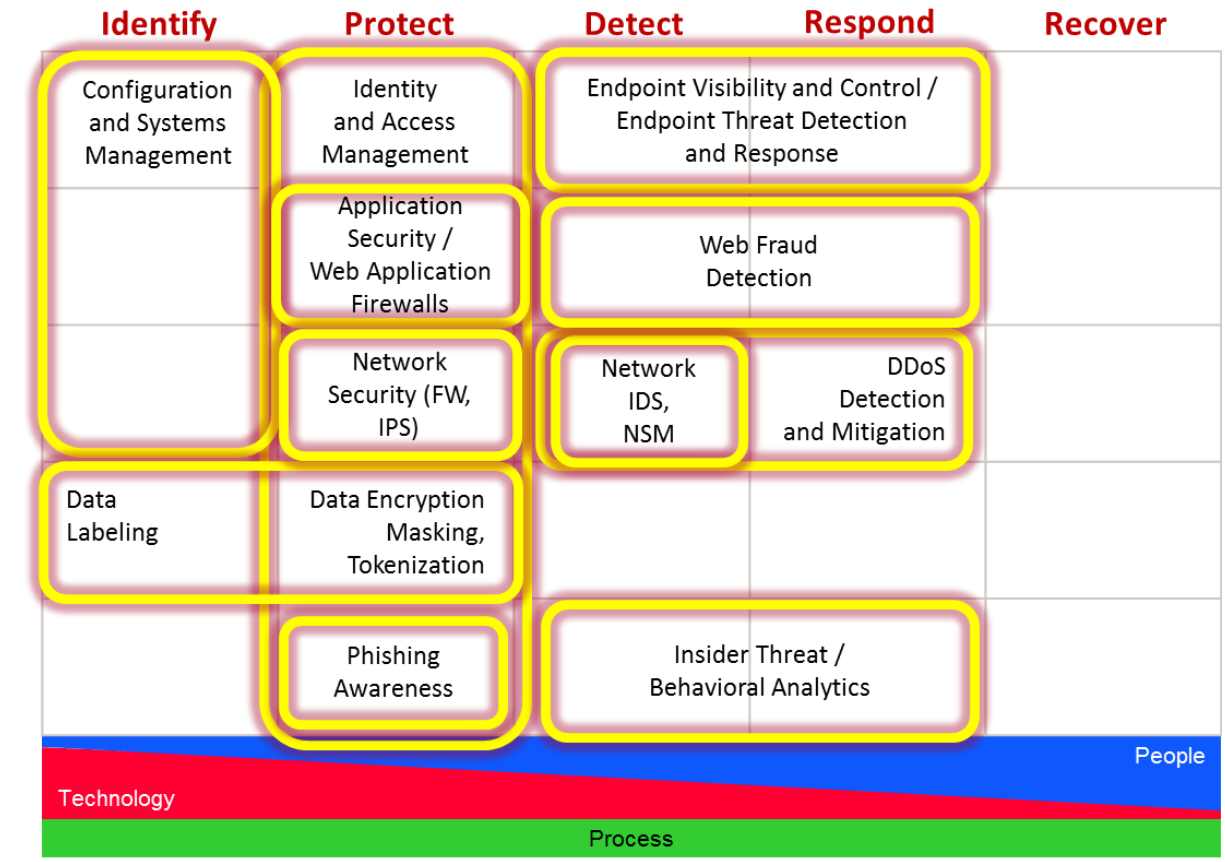
Executive Summary. The decision making for cost-effective cyber defense planning and mitigation is a complex task. There are many different security controls for identifying, avoiding, preventing, detecting, responding and recovering attacks that are deployed at various levels/layers of cyber systems including device, application, network, data and people behavior. With enterprise budget and usability constraints, selecting the optimal combination and orchestration of security controls to minimize security risk based on enterprise mission is the holy grail of cyber security for all large-scale enterprises. We call the assignment of *security controls* (solutions/tools) into specific cyber layer to optimize risk mitigation the "*Cyber Defense Matrix* (CDM)" problem. We also call the optimal composition of the selected security controls (solutions/tools) in CDM the Cyber Defense Orchestration (CDO) problem. CDO can allow for constructing *multi-layer resilient CDM orchestration* to defend against stealthy attack and attack evasion (defense-in-depth). CDO is constructed statically (offline) or dynamically tuned (on-line) according to risk measurement feedback.

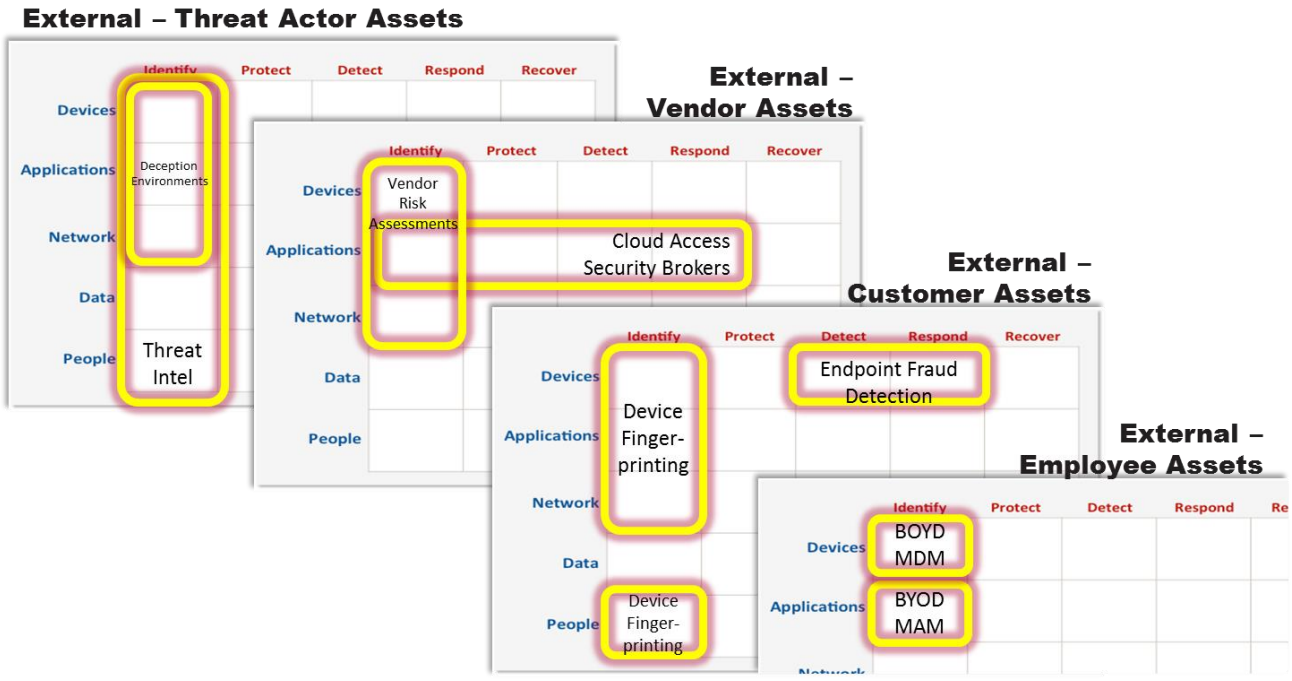
The goal of this project is to investigate metrics, formal techniques and tools to address CDM and cyber orchestration to offer the maximum cyber security benefit with the affordable budget and usability cost considering the enterprise mission requirements. The optimization of CDM/CDO must satisfy number of conditions: (1) minimizing the attack surface and potential damage, (2) creating metrics for measuring "benefit" and "cost" to provide a cost-effective security investment according mission and budget, and (3) multi-layer defense diversity for enabling built-in cyber resiliency against single-point of failure/attacks.

System Overview. The developed tools or system will take as an input and produce the output in the following figure:



Given that each technology solutions exhibits a measurable security benefit (based on the false negative) and cost (based on operational overhead, performance, $$ and false positive), it is important for large-scale enterprises to identify the optimal (minimum number) of existing technology solutions that will provide the best cyber defense matrix (minimum damage). In this project, we will address this problem by defining the formal foundation to optimize Cyber Defense Matrix, and develop analytic tools that can effectively enhance cybersecurity decision making process. We will evaluate our approach using various technology solutions and applications domains. Examples of CDM/CDO is next page (courtesy slides from Sounil Yu from BAC).


Identify
Protect
Detect
Respond
Recover
Configuration and Systems Management
Identity and Access Management
Endpoint Visibility and Control / Endpoint Threat Detection and Response
Application Security / Web Application Firewalls
Web Fraud Detection
Network Security (FW, IPS)
Network IDS, NSM
DDoS Detection and Mitigation
Data Labeling
Data Encryption Masking, Tokenization
Phishing Awareness
Insider Threat / Behavioral Analytics
People
Technology
Process


External – Threat Actor Assets
Identify
Protect
Detect
Respond
Recover
Devices
Applications
Network
Data
People
Deception Environments
Threat Intel
External – Vendor Assets
Vendor Risk Assessments
Cloud Access Security Brokers
External – Customer Assets
Endpoint Fraud Detection
Device Finger-printing
Device Finger-printing
External – Employee Assets
BOYD MDM
BYOD MAM