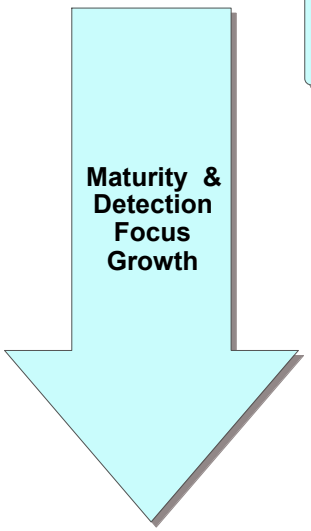
Detection in Depth Focus Model



General Detection Controls - High Noise, Low Signal, Low Relevance to Specific Asset

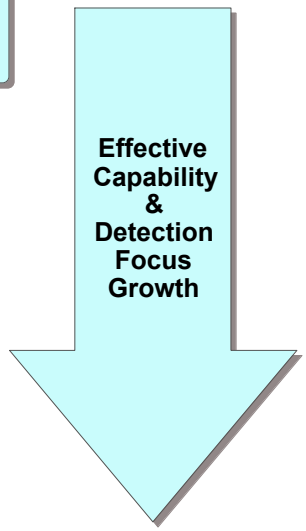
Perimeter Network IDS/IPS
Perimeter Network Firewall Log Parsing & Review

Mid-Layer Detection Controls - Medium Noise, Medium Signal, Medium Relevance to Specific Asset

Web Application Firewall Logs (if hosting multiple applications)
System Log Parsing & Review
Cloned/Adjoining/Clustered HoneyPoint Deployments
Anti-Virus & HoneyPoint Wasp on Hosting System
Hosting System HoneyPoint Agent
HoneyPoint Trojans on the Hosting System

Nuance Detection Controls - Low Noise, High Signal, High Relevance to Specific Asset

Application Log Parsing & Review
HoneyPoint Elements in the Web Application
HoneyPoint Pseudo-Data in the Database
Database Threshold Alerts on Large Record Sets
Script Checking for New Base64decode() Files



Asset:
Example - PII in a Database Accessed Via PHP Web Application

MICROSOLVED,INC.
www.microsolved.com