

Open Threat Hunting Framework

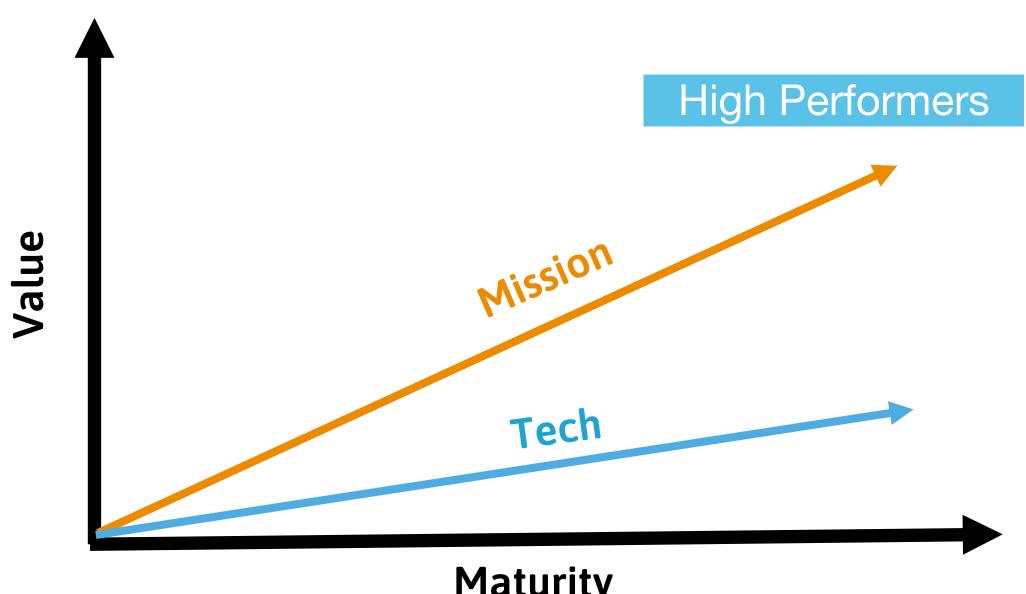
John Dwyer, X-Force Head of Research (@TactiKoolSec, LinkedIn: john-dwyer-xforce)

Neil Wyler, X-Force Global ATA Lead (@Grifter801)

Sameer Koranne, X-Force Global OT Lead



Chasing Excellence

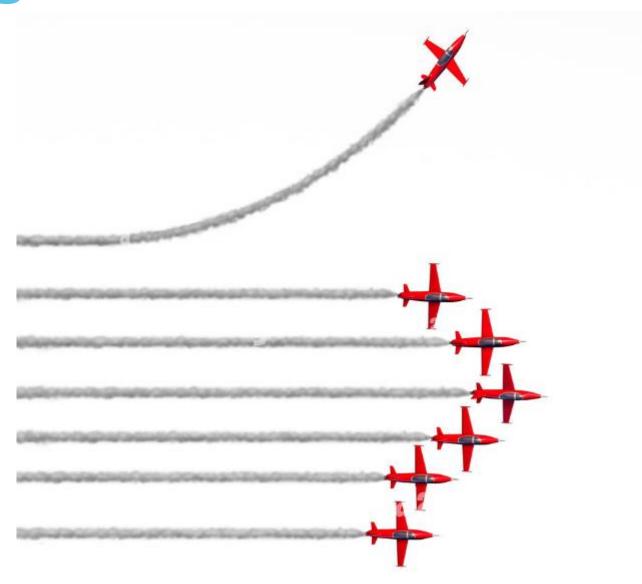


Analysis of high performing programs revealed that alignment with a mission was a stronger indicator of value and maturity than technical investment.

Maturity



"You cannot look in a new direction by looking harder in the same direction."



#BHUSA @BlackHatEvents
Information Classification: General



Open Threat Hunting Framework

Foundational

Structure

Preparation

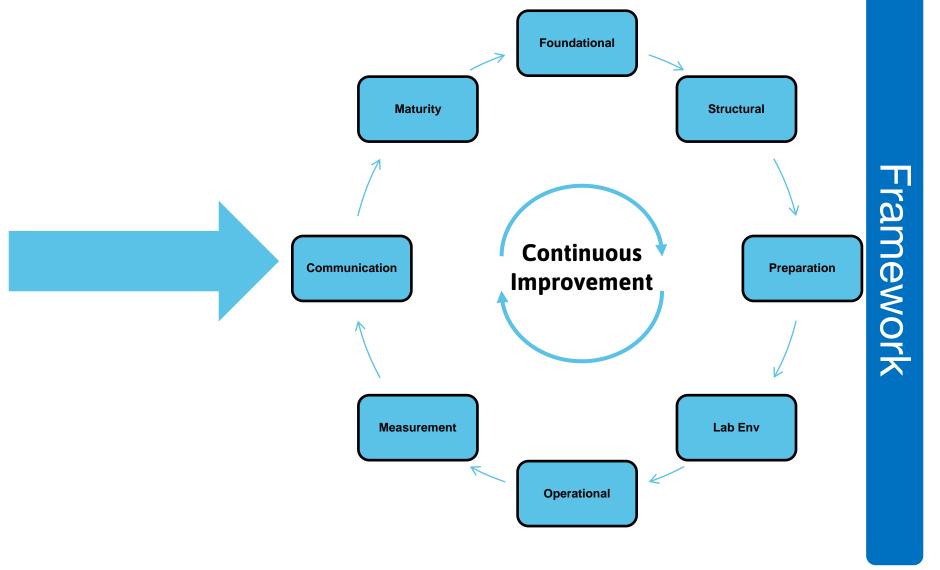
Lab Env

Operational

Measurement

Communication

Maturity

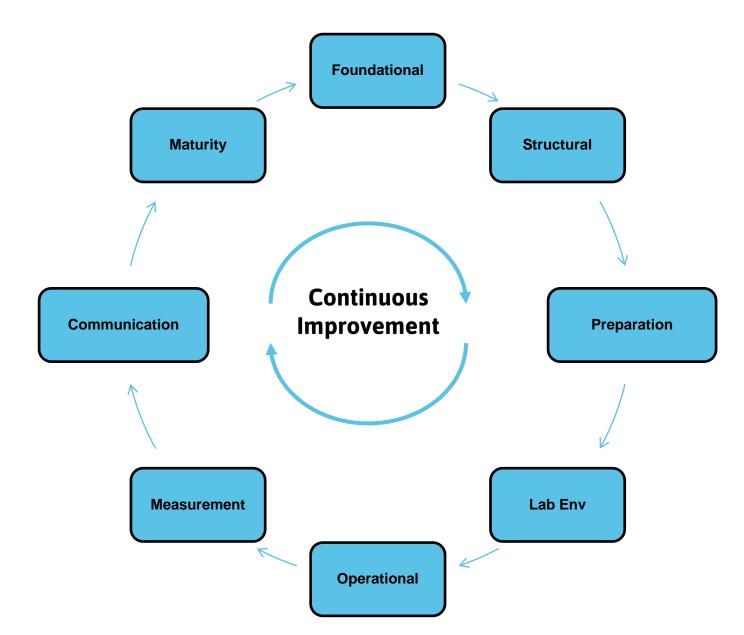


Information Classification: General

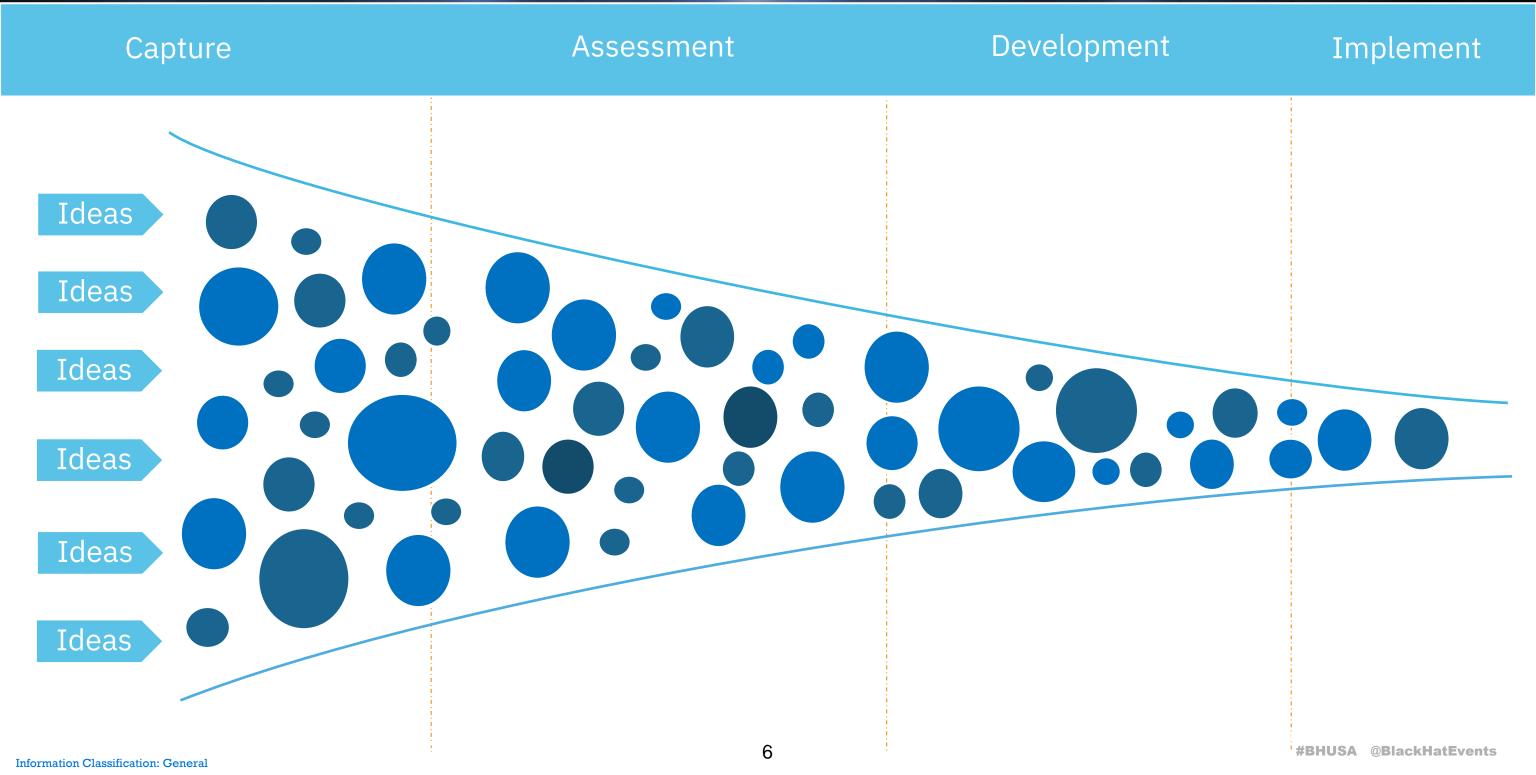
Modules



Open Threat Hunting Framework









Backup/Dev

#BHUSA @BlackHatEvents
Information Classification: General