MAPPS

Shipboard Computing (Cybersecurity/Dependable Software)

presented to

UBC Marine Systems Initiative

March 2019

Pascal Pelletier
Cyber Security Expert

Introduction

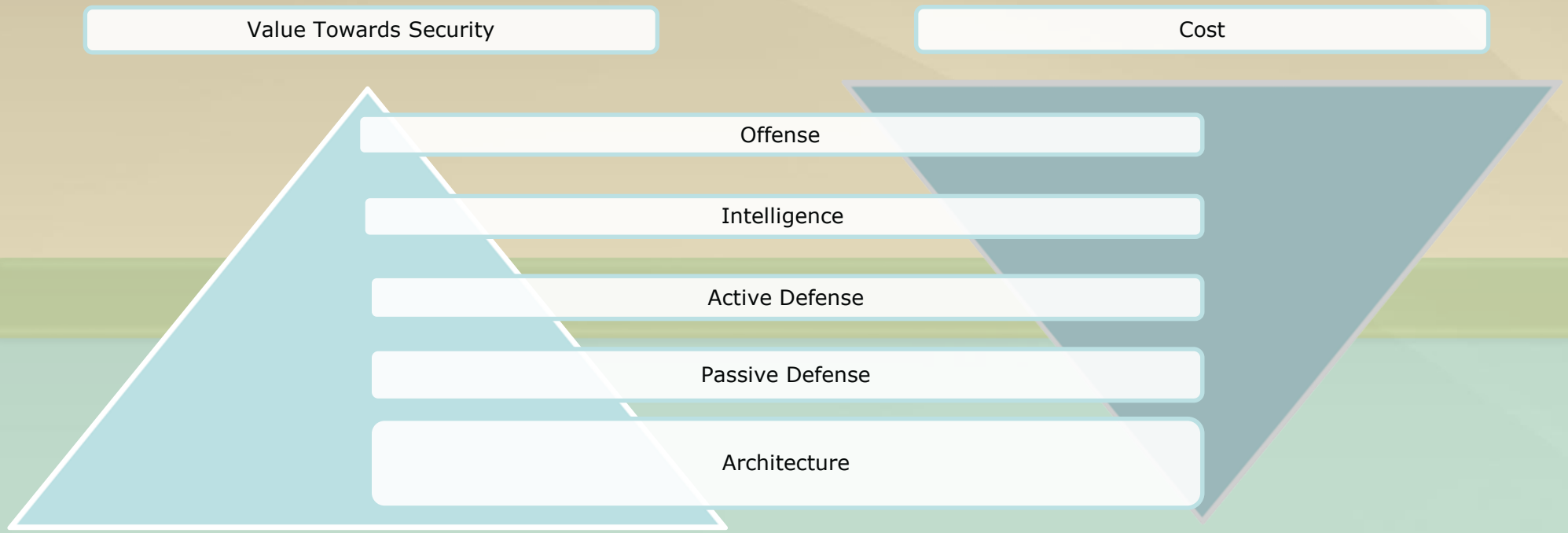
- **Who**
  - Ret'd Lt(N) P. Pelletier, M.A.Sc, rmc, CD, OSM(H)
- **What**
  - Cyber activities for dependable software, major areas for research, a cycle approach
- **Why**
  - Cyber activities are taking a large place into todays modern technology production and operation. Delivering strong and secure systems, with the toolsets allowing resiliency and robustness, is at the heart of the Canadian defense production mechanic. Todays research will lead the technology of tomorrow.
- **How**
  - Lead by Example; innovate and be engaged with partners.

What we do

- **REMOVED VIDEO ---**

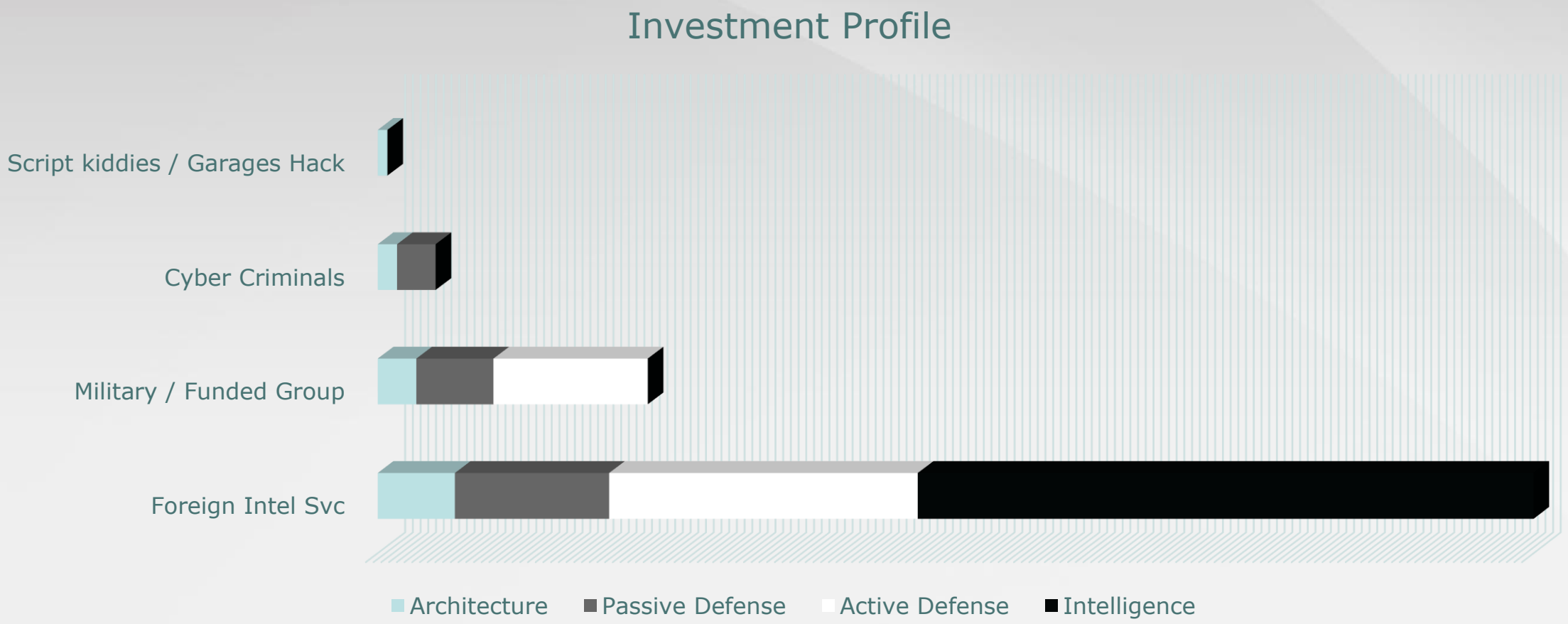
Security versus Cost

Human Oriented tools and technologies (Operations)



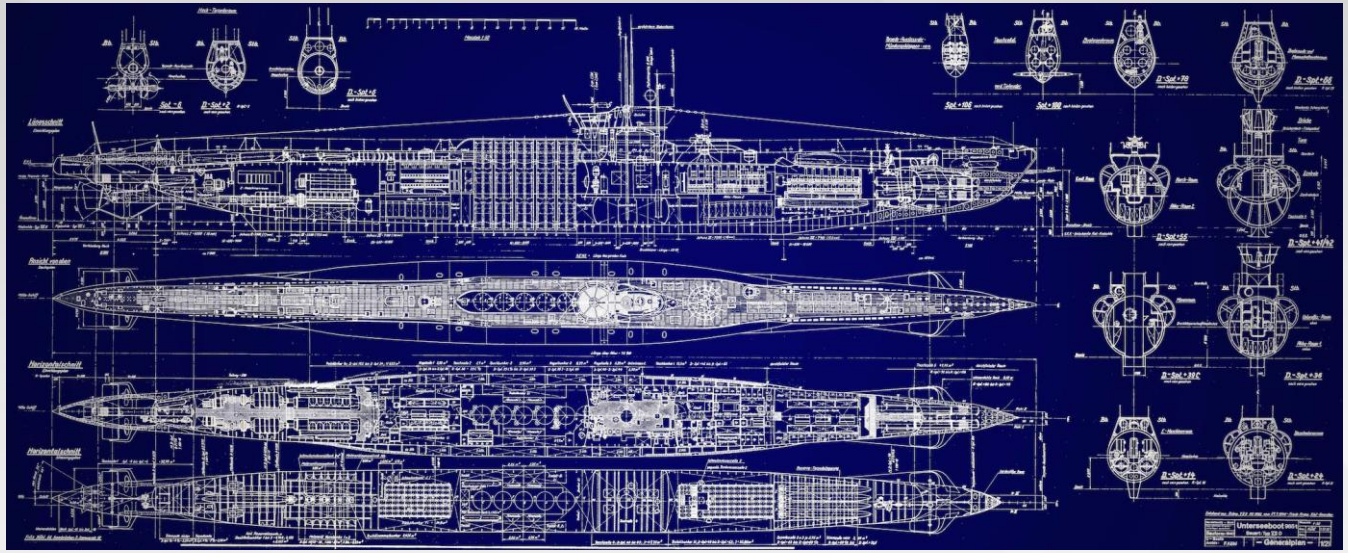
Architecture driven Cyber Defensive Tools and Technologies (Production)

Cyber Cycle investment profile as a function of adversary



Architecture

- **Architecture**
  - Design control
    - Open Source intelligence (OSINT) control
    - Design documentation
  - System Hygiene
    - Verification and Validation
    - Field support
    - Installation baselining
    - Operational Configuration control

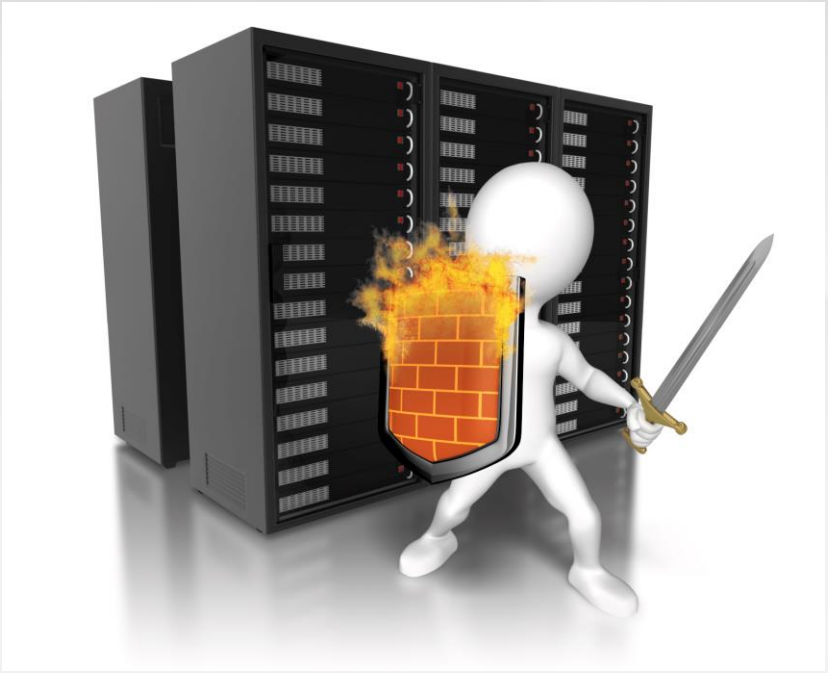


Passive Defense

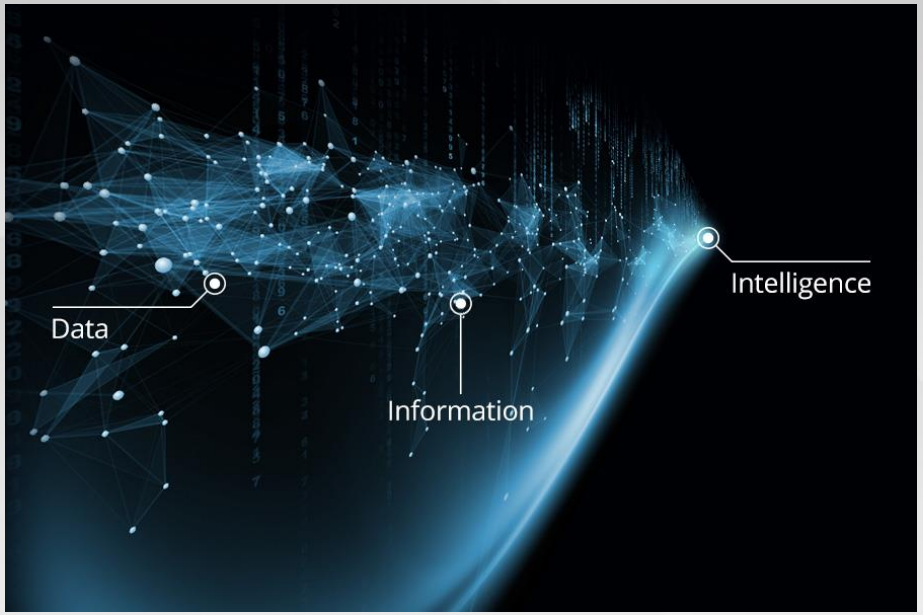
- **Passive defense**
  - Tools Installation and configuration
    - Firewall
    - Rules and traffic flows documentation
  - Tools Innovation
    - Technology R&D
  - Research & collaboration
    - Number of ties with Universities
    - Industry Canada & DRDC

Active Defense

- **Active defense**
  - Baseline documentation
    - Software binary blobs & configuration files
    - Operating systems configuration and binary documentation
    - Centralized Domain Control & configuration documentation
  - Forensics tools & techniques
    - Memory baselining
    - File system baselining
  - System Expertise
    - Known Normal operating baseline (Human expertise)
    - Documented Normal operating baseline



Threat Intelligence



- **Threat Intelligence**
  - Tactics, Technique and procedures (TTP) consumption
    - Requirements generation using Tactics and techniques for architecture
    - Agile Integration within design
    - Requirement generation using NIST Profile
    - Best practice research and hygiene tools developed to generate TTP

Product Lifecycle in the Cyber perspective
Activities mapping into existing process

Software Generation

- Cyber Architecture
- Requirement delineation
- Design activities and reviews cycles

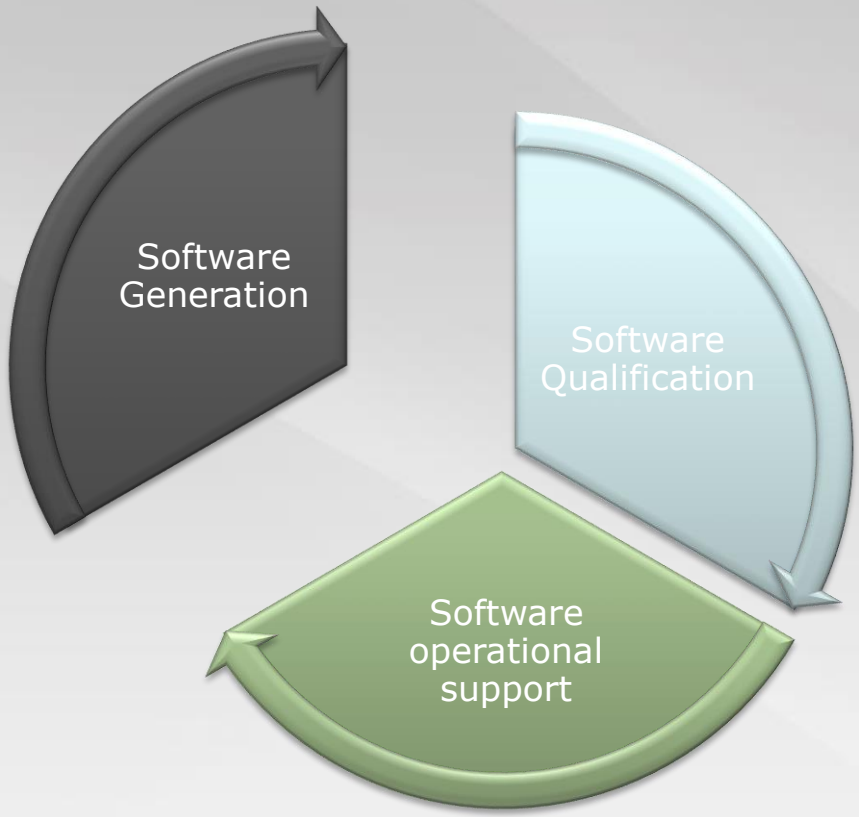
Software Qualification

- FAT / HAT / SAT
- Software verification and validation
- Pen-testing

Software Operational Support

- Support
- Forensics
- Mission Assurance

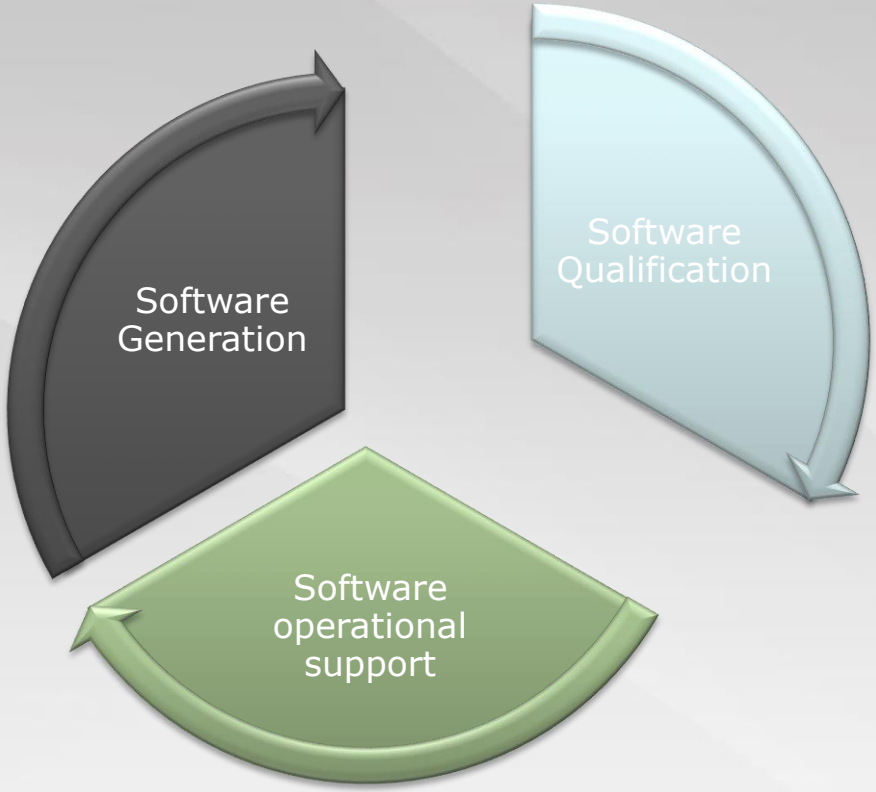
Software Generation



- **Cyber Architecture**
  - Requirement driven
  - Best practices and hygiene implementation
  - Incremental process
- **Requirement delineation**
  - Financial consideration
  - Risk managed, priority driven
- **Design activities and reviews cycles**
  - [INPUT] Main ingestion point for all phases
  - Design activities generates new cyber requirements [OUTPUT]

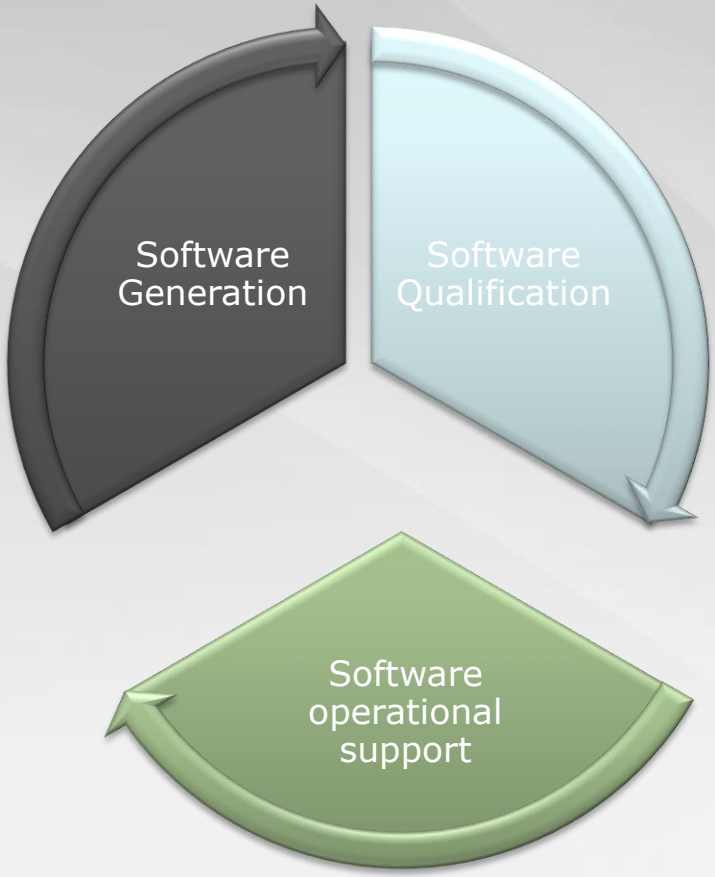
Software Qualification

- **FAT / HAT / SAT**
  - Software qualification with various stages
    - Risk tolerances decrease as stages advances
    - Assurance increase as stages advances
- **Pen-testing**
  - TTPs - Tactics and techniques and procedures
  - Indicator of Compromise (IOCs) vs signature generation
- **Software verification and validation**
  - Automated validation against Open-source threat [INPUT]
  - Automated requirements generation [OUTPUT]



Software Operational Support

- **Support**
  - Threat and environment Manipulation
  - Recovery, restoration & hardening
  - Evidence gathering
- **Forensics**
  - Incident response support
  - Forensics collection and Analysis
- **Mission Assurance**
  - Threat Intelligence TTP analysis [INPUT]
  - Requirement generation from IOCs and TTP [OUTPUT]



Cyber Security Generic Research topics

- **Securing measures in Windows & Unix systems**
  - Best practices
  - Data hygiene
  - Anomaly detection (Operating)
- **COTS products testing & evaluation**
  - Products strength and weaknesses
  - Products vulnerabilities and Exploits
  - Mitigations
- **Data forensics**
  - Automated data ingestion
  - Automated analysis
  - Anomaly detection (Response)
- **Boundary attack surface quantization**
  - Automated measurements
- **ICS specific Threat Intelligence**
  - Honeypots, TTP & IOC
  - OSINT crawler and search tools
  - Intelligence aggregation
- **Verification & Validation**
  - Automated frameworks
  - Common tools, techniques and practices

Questions ?

MAPPS

Thank you

L3 MAPPS Inc.
8565 Côte-de-Liesse
Montréal, Québec, Canada
H4T 1G5

Tel: +1 (514) 787-5000
Fax: +1 (514) 788-1442
Web: www.L3T.com/MAPPS
LinkedIn: L3 MAPPS