CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS'

# Standard-based Tools Output Integration Framework (TOIF)

Model Driven Solutions & KDM Analytics

Division of Data Access Technologies

Djenana Campara

*09/16/2013*

Homeland Security

Science and Technology

# Team Profile - Organizations

- KDM Analytics
  - Security Assurance Company
  - Leaders in providing standard based assurance tools and technologies
    - Automated Threat Risk Assessment Solution
    - Integrated standard-based security assurance environment
  - Receiver of Product Awards
    - "Best of Show" award at FOSE 2009
    - Canadian Innovation Commercialization Program 2012 in area of safety and security
- Model Driven Solutions - Division of Data Access Technologies
  - Trusted small business provider
  - Specializing in Model Driven Architecture
    - Enterprise and System Architecture
    - Service Oriented Architecture
    - Cyber Security
    - NIEM
    - Information Federation
    - Software Development Automation

# Customer Need - Cyber Security

- Governments and industry are in need of security solutions that assist in making their network centric systems cyber resilient
  - Increasingly sophisticated cyber attacks use technology readily available on the internet and utilizes unprotected computers to launch attacks on governments and business systems
- Key capabilities of security solutions
  - effective measurement, prioritization and mediation of the assurance risks posed by system vulnerabilities
    - Comprehensive, objective, systematic and automated
    - Cost-effective

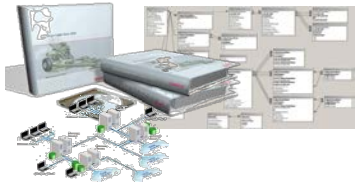
# Approach

- Our solution employs a highly automated and formal approach to security evaluation and risk analysis of IT and embedded software systems, resulting in comprehensive and objective outcomes
  - Threat Risk Assessment (TRA) transparency and traceability models are generated and connected to formal system artifacts for automated and visual inspection/review.
  - The size and complexity of the system does not compromise the fidelity, accuracy and comprehensiveness of information and results.

# Our Tools, Technologies and Methodologies: Landscape

FORSA methodology

**CONOPS**

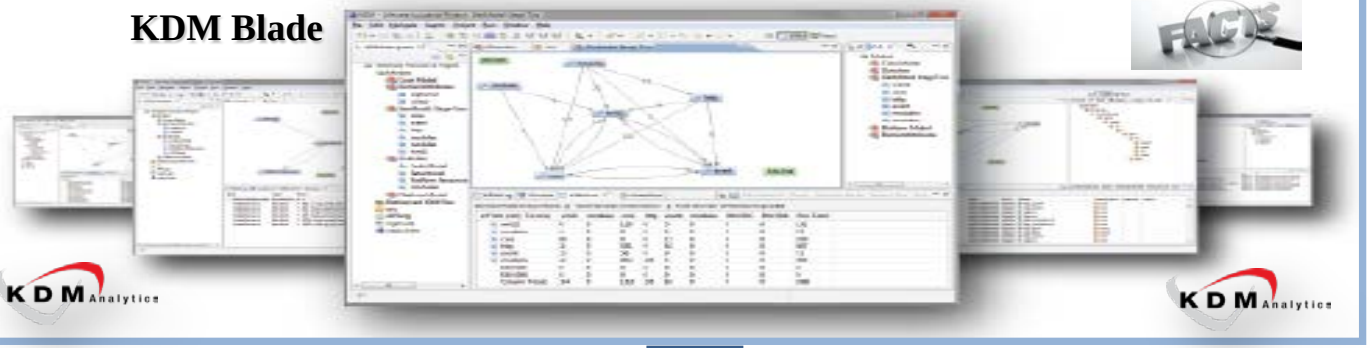


**Reference Information**

- National Vulnerability Database
- Compliance Specifications
- Software Fault Patterns
- Code Security Defects
- Threat-Risk Analysis models

**Software System**

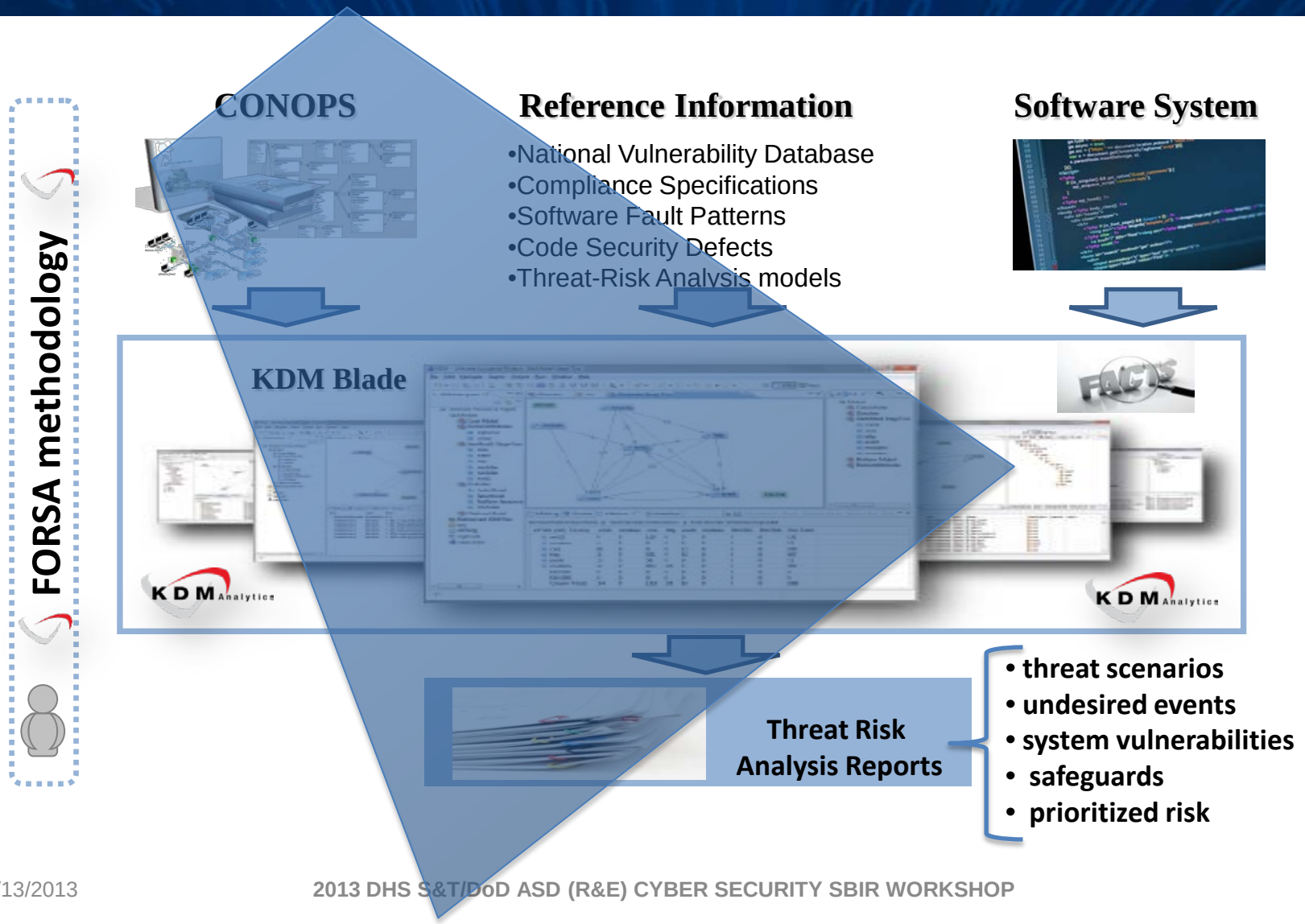
**KDM Blade**




**Threat Risk Analysis Reports**

- threat scenarios
- undesired events
- system vulnerabilities
- safeguards
- prioritized risk

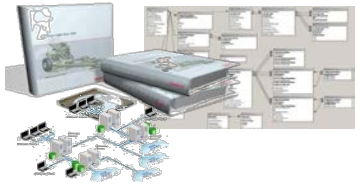
# Our Tools, Technologies and Methodologies: Landscape



# Our Tools, Technologies and Methodologies: Landscape

FORSA methodology

**CONOPS**

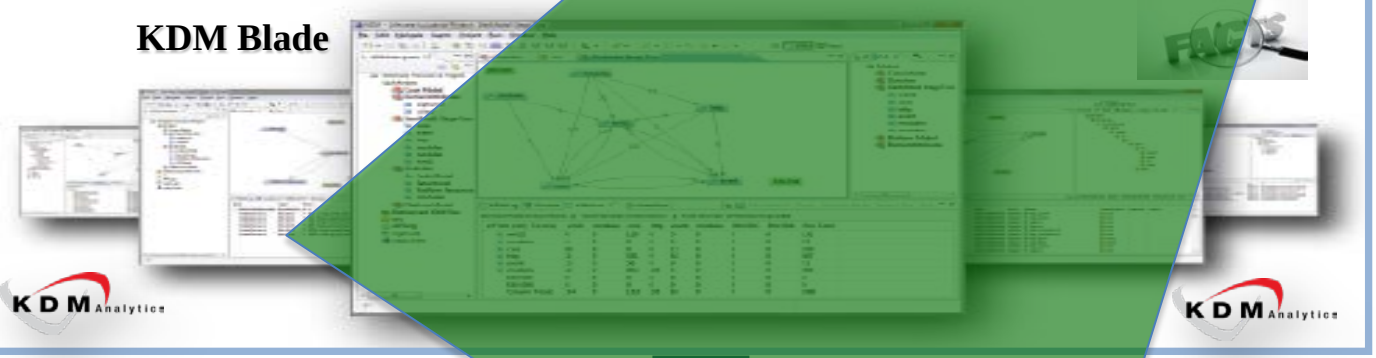


**Reference Information**

- National Vulnerability Database
- Compliance Specifications
- Software Fault Patterns
- Code Security Defects
- Threat-Risk Analysis models

**Software System**

**KDM Blade**




**Threat Risk Analysis Reports**

- threat scenarios
- undesired events
- system vulnerabilities
- safeguards
- prioritized risk

# Key Capabilities

- Threat Modeling Environment
- DoDAF Analytics
  - Automated extraction of system information/facts related to risk
  - Automatically synthesized system's security view
  - Contributing to evidence-driven risk assessment
- Traceability between risk model and system facts contributing to the risk
- Automated generation of Threat Risk Assessment reports
- Automated generation of system models with drill down capabilities used to perform architecture risk analysis
- Composite code vulnerability analysis and cross-correlation of their findings with architectural risk analysis
- Provided risk assessment knowledge base
- System transparency and traceability capability

# Benefits

- Automated and cost effective Risk Management
  - Evidence-based, objective and systematic risk analysis enables costs and benefits to be weighted so that informed decision can be made on protective actions
  - Mediation is only possible where the vulnerability is identified!

- Can be integrated into organizations existing management systems such as quality and safety

# Competition

- The competition's approach to Threat Risk Assessment relies mostly on informal artifacts and rarely analyzes formal facts
  1. involves documentation and personnel interviews,
  2. tools deployed in analysis of formal facts are point solutions
  3. above two points make this approach subjective, non-comprehensive, non-repeatable, and prone to inaccuracies about the true nature of the system risks and vulnerabilities

- Our competitors are point solutions and manual risk assessment process deployed by security professionals

- Our solution integrates and automates multiple tools to federate point solutions

# Current Status

- TOIF framework and repository for static analysis is in-place and ready for use
- Published as open source to help coalesce the SwA community and lower the barriers to entry
- The Threat Risk Assessment solution, Blade productized and commercially available
- Currently has been evaluated by
  - Lockheed Martin (Blade)
  - Air Force Research Lab (Blade with TOIF)
- Already sold licenses
  - Defence Research and Development of Canada (Blade with TOIF)
  - Lockheed Martin (TOIF)
  - EWA Canada and EWA US (Blade)

# Next Steps

- Going forward
  - Expand scope of CWEs & SFPs federated
  - Encompass hybrid static and dynamic analysis
  - Integrate into “SWAMP”

- Technology Transition
  - Published as open source
  - Included in KDM Analytics products (e.g. Blade)
  - Solution provider partnerships (e.g. LM)
  - Software Assurance lab partnerships (e.g. AFRL)
  - Software licensing
  - Analytics Services

**Our Clients are using TOIF to integrate reporting of commercially available static analysis tools**

# Contact Information

Cory Casanave, CEO, Model Driven Solutions,
Division of Data Access Technologies
Phone: (703) 880-6708
cory-c@modeldriven.com
www.modeldriven.com

Djenana Campara, CEO, KDM Analytics
Phone: (613) 627-1012
djenana@kdmanalytics.com
www.kdmanalytics.com