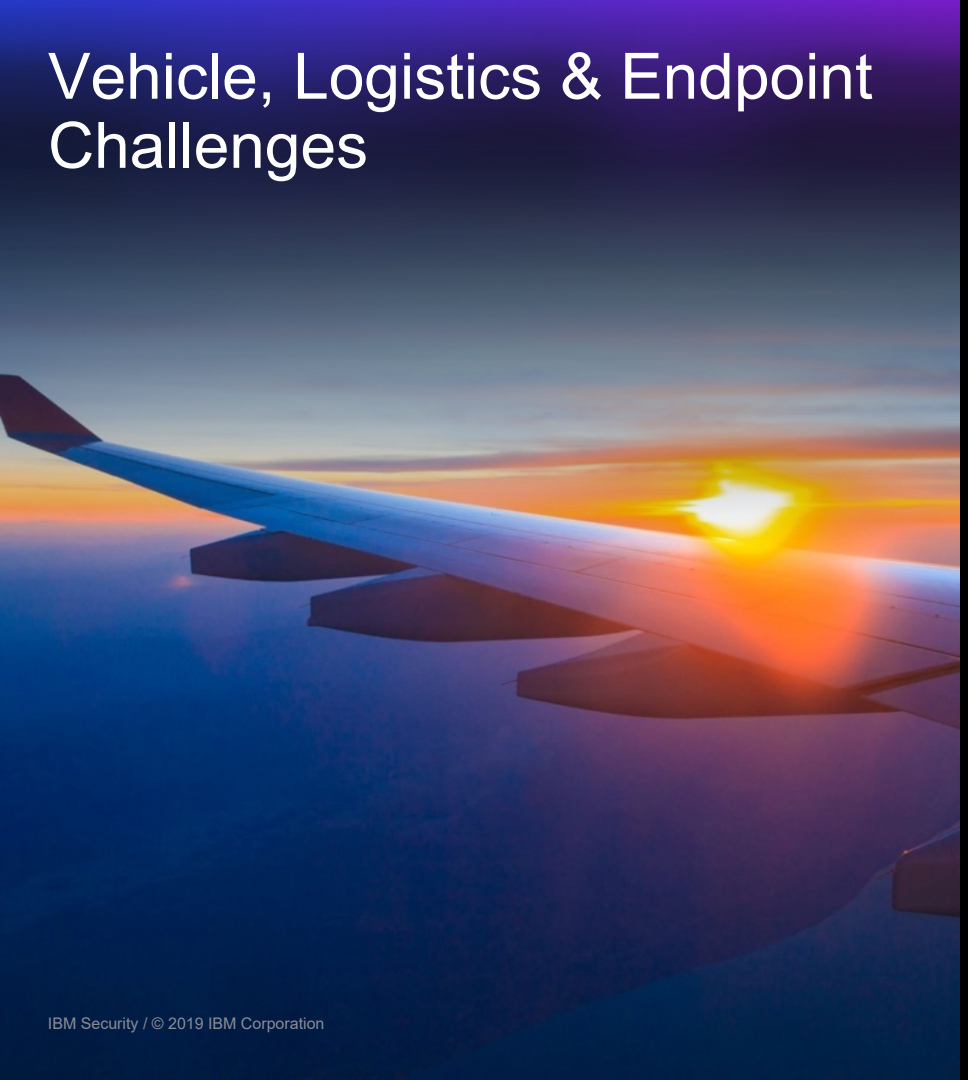
Security Strategy- **Fearless in the face of uncertainty**

Dr. Shue-Jane Thompson

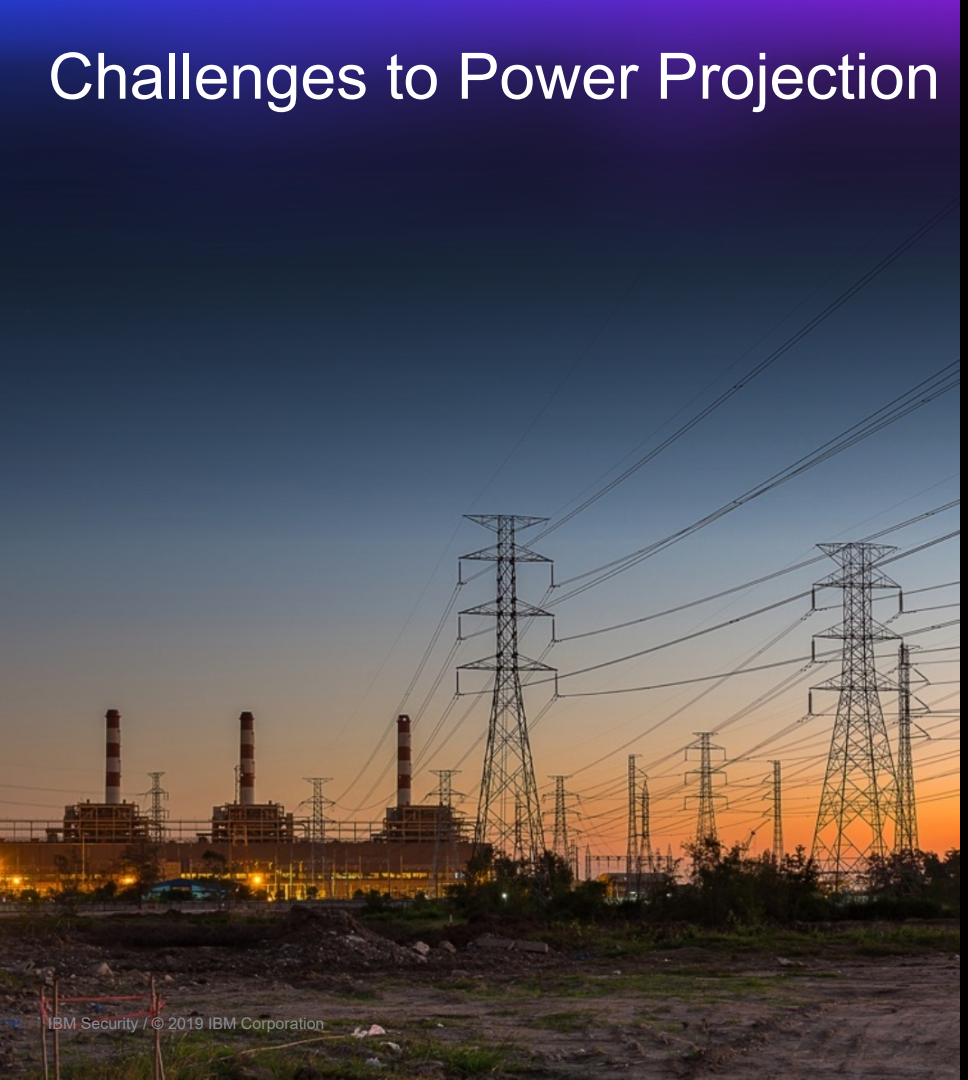
VP & Partner,
Cybersecurity & Biometrics
Global Business Services
shuejane@us.ibm.com

Vehicle, Logistics & Endpoint Challenges



- Mitigate against malware and advanced threats
- Improve real-time visibility, integrity and continuous monitoring
- Enable funding flow to match delivery requirements and timelines
- Ensure interoperability of IT (ex. IoT) and business systems

Challenges to Power Projection



- Address risks for IT, OT and IoT
- Harmonize the approach to IT-OT convergence
- Maintain regulatory compliance
- Increase security efficiency for detection to response
- Enable and protect digital transformation

Challenges to Infrastructure

- Enable new technologies (ex. 5G) and IOT
- Maintain regulatory compliance
- Meet the demands of digital transformation
- Address the rise in threats and attacks

Challenges to Stability

- Lack of sufficient skills and administration
- Meet the demands of digital transformation
- Ensure data privacy and compliance
- Mitigate insider and advanced persistent threats

Cybersecurity is a universal challenge

What's at stake…

20.8 billion
things we need to secure

5 billion
personal data records stolen

$6 trillion
lost to cybercrime over the next 2 years

What we face…

Compliance updates
GDPR fines can cost
billions
for large global companies

Skills shortage
By 2022, CISOs will face
1.8 million
unfulfilled cybersecurity jobs

Too many tools
Organizations are using
too many
tools from too many vendors

Elements of an evolving security program

Strategy and Risk

Advance Security Maturity
- Strategy and Planning
- Risk Assessments
- Advisory Services

Build Leadership and Culture
- X-Force Cyber Range
- X-Force Comes to You
- X-Force Cyber Tactical Operations Center

Threat Management

Detect and Stop Advanced Threats
- Security Operations Consulting
- X-Force Threat Mgmt. Services
- X-Force Red
- QRadar
- X-Force Detect

Orchestrate Incident Response
- Resilient
- X-Force IRIS

Master Threat Hunting
- i2 Intelligence Analysis
- QRadar Advisor with Watson

Digital Trust

Protect Critical Assets
- SDLC Consulting
- Data Protection Services
- AppScan
- Guardium
- Data Risk Manager
- Multi-cloud Encryption
- Key Lifecycle Manager

Govern Users and Identities
- Identity Mgmt. Services
- Identity Governance
- Cloud Identity
- Access Manager
- Secret Server

Deliver Digital Identity Trust
- Trusteer
- Cloud Identity

Secure Hybrid Cloud
- Infrastructure and Endpoint Services
- Hybrid Cloud Security Services
- QRadar Cloud Analytics
- Cloud Identity
- Guardium for Cloud

Unify Endpoint Management
- Endpoint Mgmt. Services
- MaaS360
- BigFix

Deploy meaningful innovations

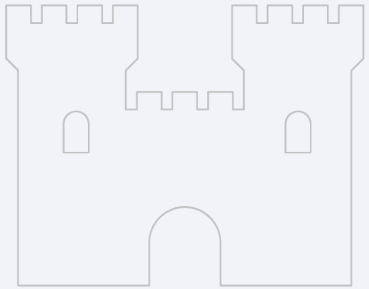
#SecurityFirst

AI and Orchestration

Collaboration

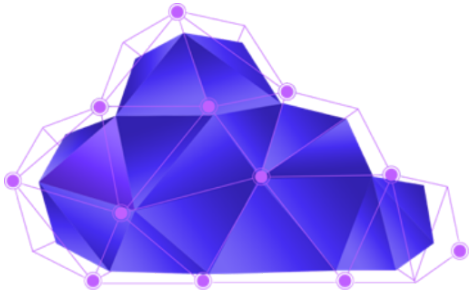
The future of security

Before 2011
Bolt-on security
for IT projects



2011-2018
Security intelligence
across the enterprise

2019+
Connected security for all,
at the “speed of digital
Transformation”



Beyond…
AI, quantum, blockchain
and IoT security

Leverage a global network of protection and training

Global Security Centers

Mobile Command Centers

Solution Development Centers | Security Research Centers

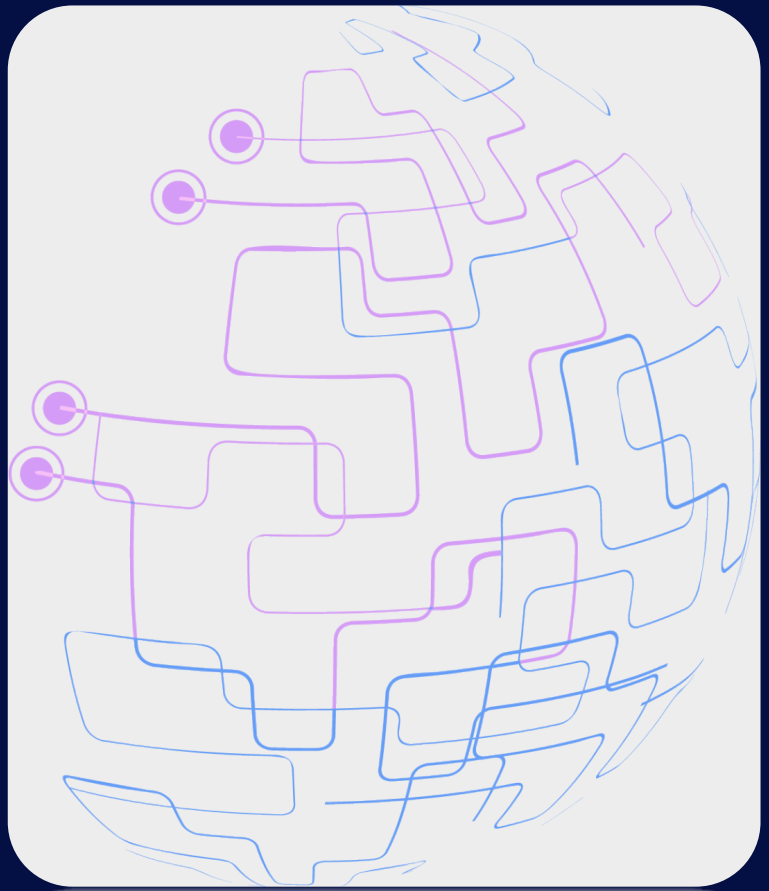
Identify and respond to threats with speed and confidence

When you connect people, process, and technologies with AI and continuous insights

What holds us back?

- Attackers evading rules-based solutions
- Empty seats and churn in the SOC
- Too many events, not enough time
- No way to operationalize response
- Not staffed to survive a breach

Security Operations Consulting | Threat Management Services | Security Analytics | Response and Orchestration | Threat Hunting



Ready for future battles

Security projects that will shape our future

Good AI versus bad

Address the weaknesses found in AI systems

Blockchain for security

Enables sharing threat intelligence that's anonymous and trusted

Post-quantum cryptography

Lattice cryptography will protect organizations from quantum-enabled hackers

Securing the "world of things"

Researchers are working on cryptographic algorithms and protocols, and key management to enable end-to-end IoT security

Blockchain

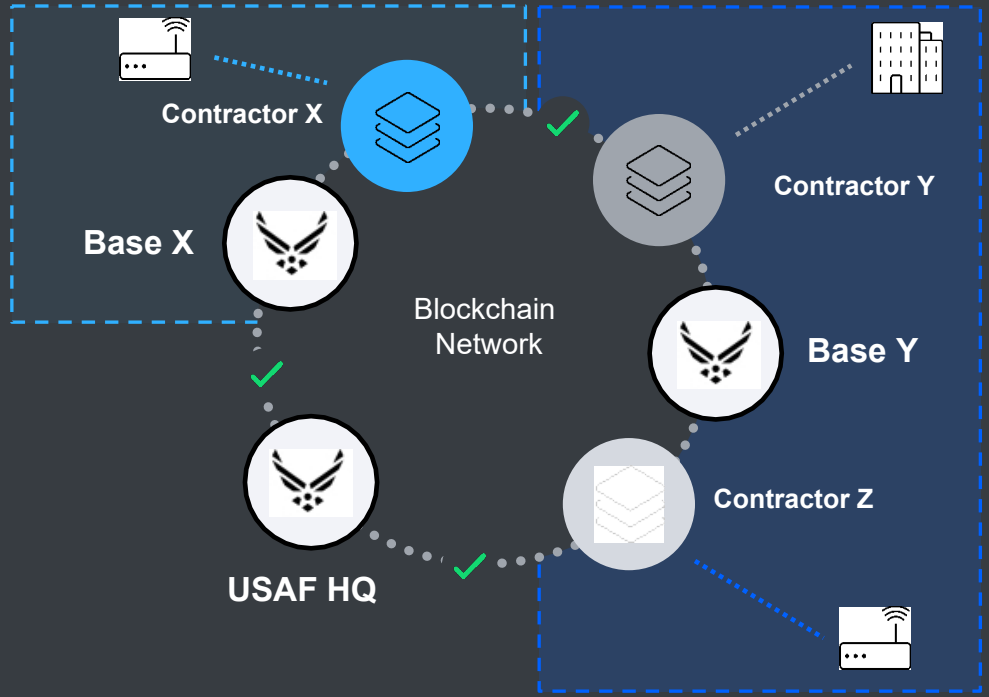
Outcomes

Provides a verified drilldown of information and alerts up the chain of command around a sensor set

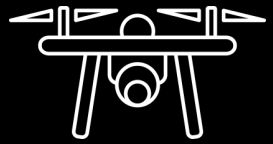
Automatically generated alerts based on inputs outside a set of given parameters

Demonstrated the ability of alerts over time to give insights which can assist staff in making occupancy decisions

Blockchain meets IOT



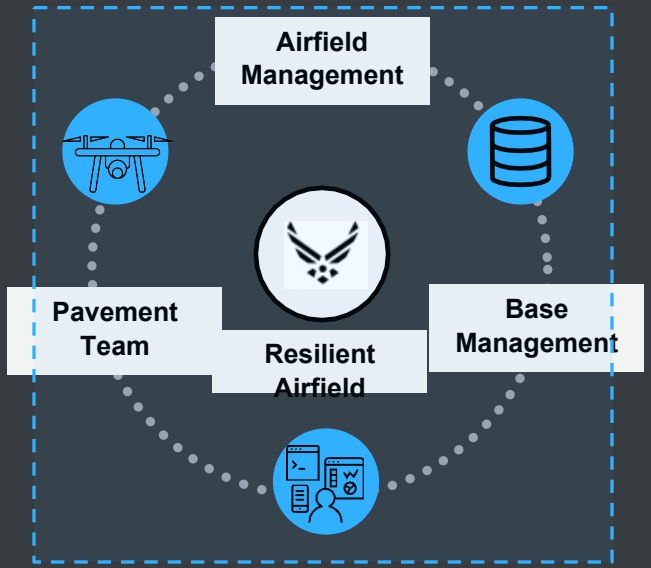
Drone Visual Recognition



Outcomes

The results from this analysis indicate that 85% of the used pavement was undamaged, and 1.6%, 8.0%, 4.7% of the pavement is considered of low, medium, and high severity, respectively. Furthermore, the North and South landing zone was the most damaged used feature area; 24.7% of its area was damaged. This is to be expected, because planes landing exerts the high force, which in turn, causes higher stress in the pavement.

USAF Case Study



- *Dashboard with prioritized list of damage assessment and change in conditions overtime*
- *Tailored insights for airfield management based upon Air Force Base mission*
- *Autonomous drone inspection, real time results, efficient work orders, remote analysis*
- *Airfield health data managed across USAF*
- *Predictive maintenance to make quicker and informed decisions*
- *Real time AI and automated insights*

Defend missions with end-to-end threat management

X-Force Red

Hacking anything to secure everything

170 Renowned veteran hackers and experts

X-Force IRIS

Gain the expertise needed to deal with *"Right of Boom"*

$1M+ Savings when a breach is contained within 30 days

Managed Security Services

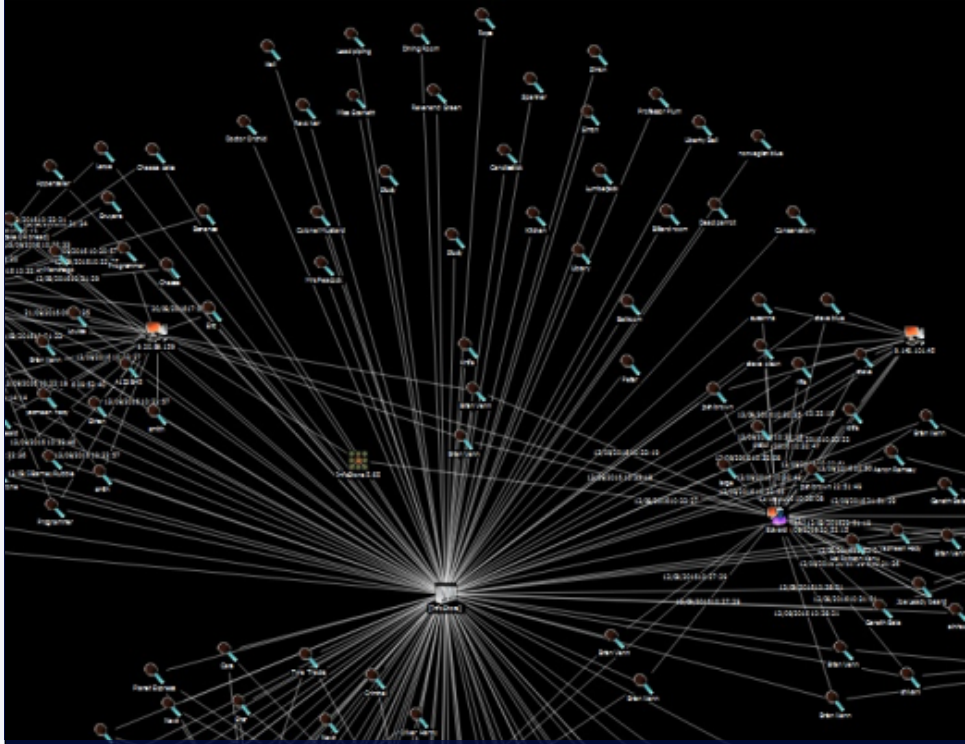
Extend coverage with 24x7 security expertise

20+ Years of experience through thousands of engagements

Detect and stop threats

IBM QRadar

User and entity profiling
Statistical analysis
Pattern identification
Entity and user context
Network-based anomaly detection
External threat correlation
Real-time analytics
Risk-based analytics
Threat hunting
DNS analytics
Business context



#1 SIEM for
Advanced Threat Defense

- Gartner

"3 billion security events per day are accurately analyzed and condensed into 25 prioritized offenses, enabling analysts to focus on what matters most."

- Large energy company

Enterprise Insight Analysis

Use intelligence to find the attacker

- Ingest structured and unstructured data including OSINT and the dark web
- Uncover hidden connections and patterns
- Deliver actionable intelligence and accelerate data to decision

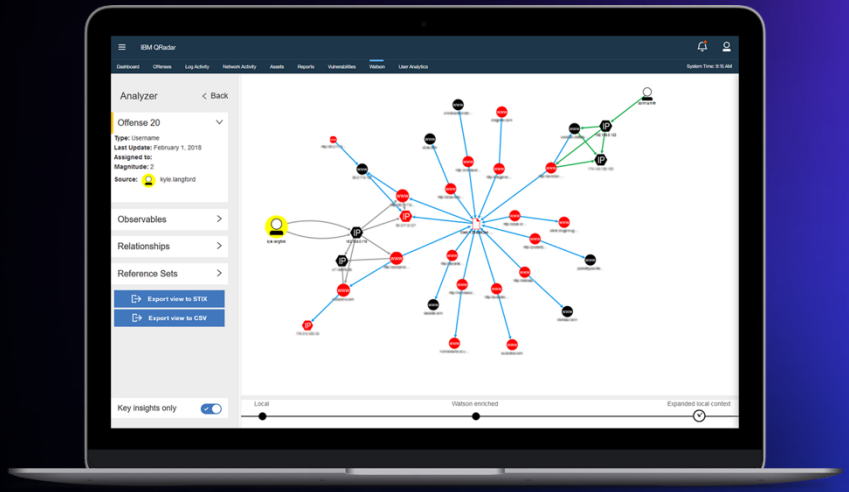
Speed up your SOC with AI

User Behavior Analytics

Detect insider threats with machine learning

- Continuously learns behaviors to predict malicious users
- Generate detailed risk scores for individual users
- 16K+ free downloads from X-Force App Exchange

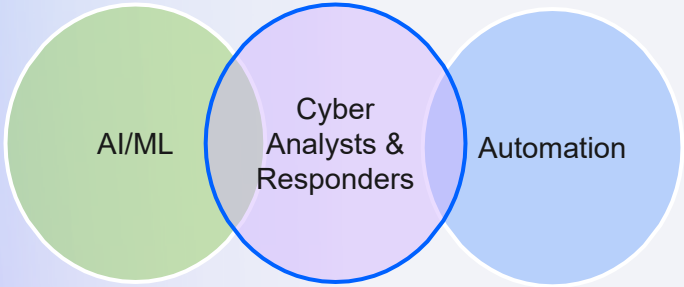
Advisor with Watson



Force multiply your team's effectiveness with AI

- Automatically connect the dots for more decisive threat escalation
- Speed response and visualize attack stages using MITRE ATT&CK
- Gain insights from Watson's 10B+ security data points

How you respond matters



Arm your team with the industry's leading Incident Response Platform

40x

Faster overall response using dynamic playbooks that orchestrate your people, process and technology

IBM Resilient

Cyber Range - Test yourself in an immersive and safe environment and learn from live fire incident responses

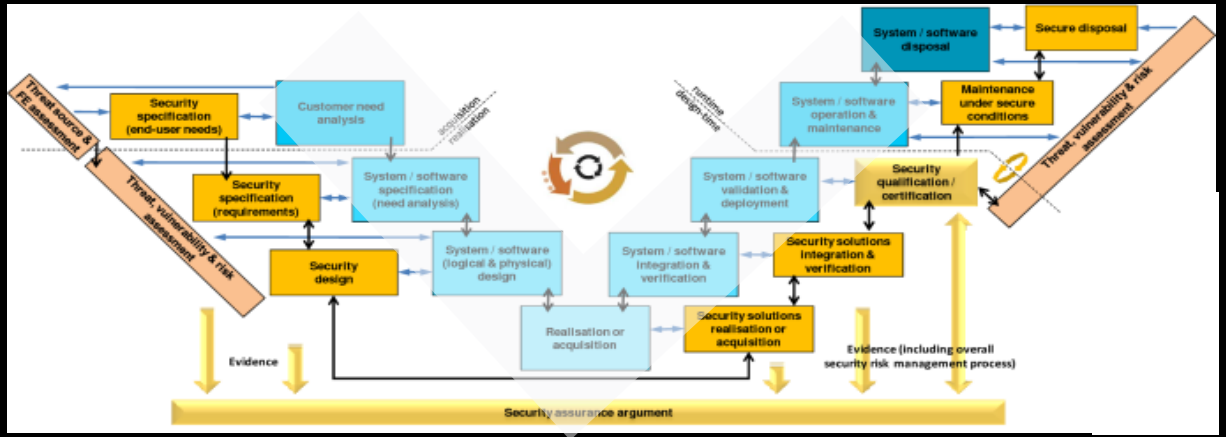
IBM X-Force Command Center

Move to the cloud with confidence

Cloud Security Services

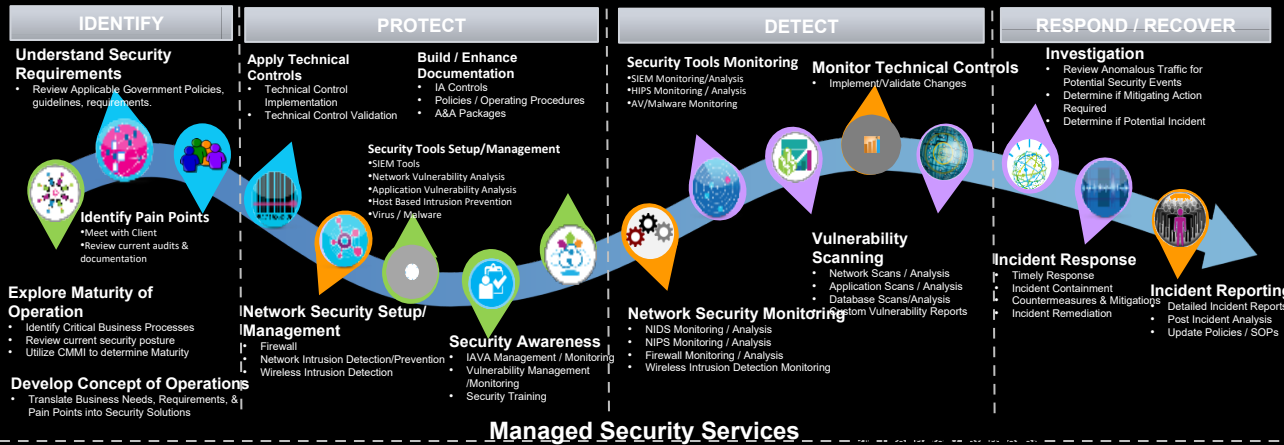
- Cloud Security Strategy
  Security transformation, strategy, and baselining
- In-the-Cloud-Security
  Policy management and segmentation, shadow IT discovery, data security and more for your in-the-cloud workloads
- Managed Security Services
  DISA Impact lvl 5 & FEDRAMP accredited Cloud Security Services – 24X7 SIOC services and proven managed portfolio backed by best-of-breed partnerships plus threat management solutions

Security Strategy and Trend



System Engineering fusion with Security Engineering (Paul & Delande, 2012)

Managed Security Service



DoD Account Executives

Joe Woodward:
Jwoodwar@us.ibm.com
910-381-7792

Rebecca Schollenberger-Cherouny:
Rebecca.Schollenberger-Cherouny@ibm.com
703-795-6788