

# BEYOND THE OBVIOUS: WHY $|+| = 3$ IN THIRD-PARTY RISK

SUBJECTIVE &  
DEDUCTIVE  
REASONING  
WITH THE MITRE  
ATT&CK  
FRAMEWORK TO  
UNCOVER  
HIDDEN  
VENDOR RISKS

# ABSTRACT

Traditional third-party risk management often relies on basic compliance checks, missing critical risks. This session introduces subjective and deductive reasoning methods within the MITRE ATT&CK framework to deeply assess vendor security. Real-world examples illustrate how these techniques effectively uncover hidden vulnerabilities and strengthen proactive risk management.

# SESSION HIGHLIGHTS

---

Introduction

---

Core Principles

---

MITRE ATT&CK Framework

---

Deductive Reasoning Case Study

---

Subjective Reasoning

---

Integration Approach

---

Practical Application

---

Summary and Q&A

# INTRODUCTION

- ❖ WELCOME
- ❖ INTRODUCTION
- ❖ OBJECTIVES

# INTRODUCTIONS & OBJECTIVES

## Welcome & Introductions

## Session Objectives

- Learn I+I=3 risk model, practice deductive + subjective methods, apply ATT&CK lens.

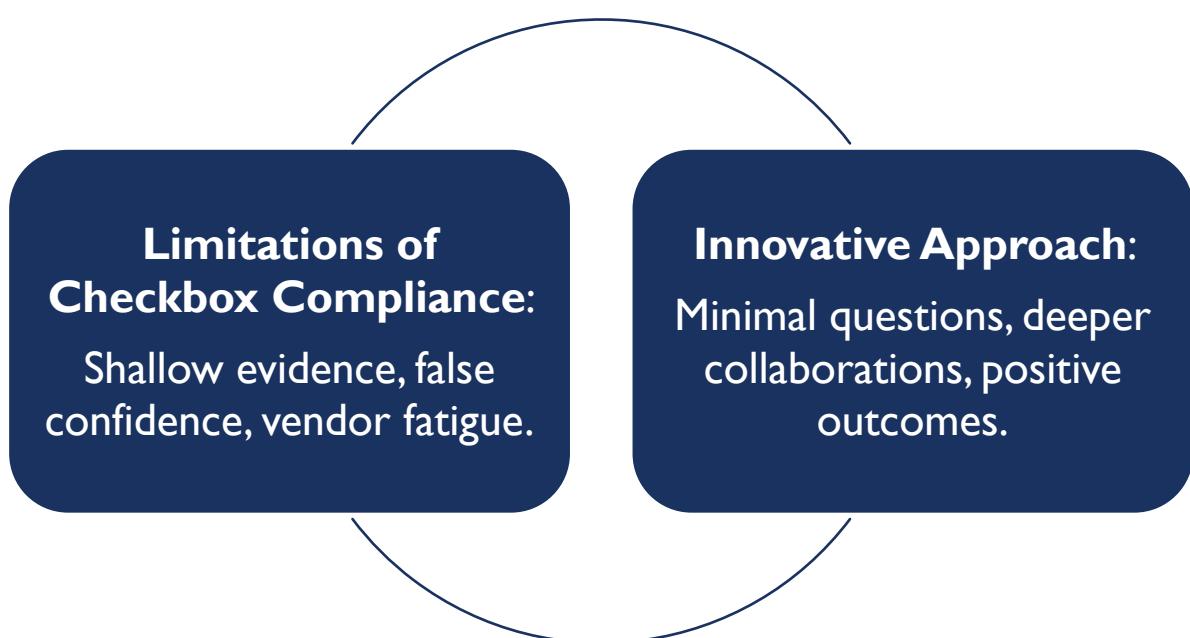
## Ground Rules

- Interactive, questions welcome!

# CORE PRINCIPLES

WHY CHECKBOX  
COMPLIANCE FAILS

# CORE PRINCIPLES



## Blend Methods:



→ Defensible Conclusions



→ Practical Relevance

# MITRE ATT&CK FRAMEWORK

USE TACTICS AS A  
QUESTION MAP

# ATT&CK OVERVIEW, RELEVANCE, & KEY TACTICS

## Why it matters:

- Aligns questions to real attack chains; avoids blind spots.

Use tactics to structure vendor questions and artifact requests.

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Exfiltration

Command & Control

Impact

# DEDUCTIVE REASONING CASE STUDY

SMART THERMOSTAT  
SCENARIO

## CASE SCENARIO & ARCHITECTURE



### Scenario:

Vendor solution for lighting controls, room HVAC, occupancy detection.



### Architecture:

Vendor in DMZ; simple PMS link; cloud platform; on-prem reaches out for reporting/monitoring.

## DATA GATHERING & GAP IDENTIFICATION

Missing protections across 8 of 12 ATT&CK categories.

No dedicated cyber team; month-to-month MSSP reliance.

AV choice raised concerns; missing SEG, PAM, NIDS/NIPS.

# EVALUATION, VALIDATION, DOCUMENTATION



## Logical evaluation & scoring:

Map controls to ATT&CK;  
weight by likely lateral-  
movement and data exposure  
impact.



## Validation:

Validate via joint working  
sessions – challenge  
assumptions, exercise  
compensating controls, and  
capture proof of effectiveness



## Documentation:

Document a clear risk story:  
findings, ATT&CK mapping,  
evidence, and decision (H/M/L).

# SUBJECTIVE REASONING

QUALITATIVE  
SIGNALS, SMES,  
SCENARIOS

# SUBJECTIVE METHOD (STRUCTURED)

## Qualitative Data:

The 'why' behind design choices; look for effective pairings and compensations.

## Expert Opinions:

Architects, Engineers, peer intel; triangulate insights.

## Scenario Analysis:

Chain tactics to see how ' $1+1=3$ ' emerges.

## Contextual Factors to Consider:

- Regulatory Compliance Posture
- Financial Stability & Viability
- Security Policies & Cultural Alignment
- Data Sensitivity
- Geography
- EoS / EoL
- IR / BCP / DR Maturity

# INTEGRATION APPROACH

BLEND METHODS +  
KEEP RATINGS  
ADAPTIVE

# INTEGRATION & LIFECYCLE



## Bring

*Bring the Analysis Together*

- Combine evidence-based findings (deductive) with contextual judgment (subjective) into one risk narrative.
- Link findings to likely attack paths to show how gaps interact and amplify risk.



## Decide & Document

*Decide and Document the Outcome*

- **Approve** – no conditions.
- **Approve with Conditions and a Plan of Action and Milestones** — list actions, owners, due dates, and how completion will be verified.
- **Do Not Proceed** — state the specific risk drivers and what must change.



## Keep

*Keep the Review Current*

- Refresh evidence on a schedule that matches the vendor's criticality level (for example: high-criticality every 12 months; lower-criticality every 24 months).
- Re-open the review when a trigger occurs: security incident, new data flows, architectural change, or negative news.



## Adapt

*Adapt the Risk Rating Over Time*

- Update the rating using incident history, results of effectiveness tests, monitoring alerts, change requests, and external threat intelligence.
- Adjust safeguards and review frequency whenever the rating moves up or down.

# PRACTICAL APPLICATION

START USING THE  
FRAMEWORK

# HOW TO START

## Quick Start (Next 2 Weeks)

- Pick 1 in-flight vendor; map use-case questions to ATT&CK tactics (12 tiles).
- Gather evidence: VRA, SOC/Bridge Letter, Diagrams; co-review SMEs.
- Historical Incident Analysis: pick 1-2 relevant incidents; extract the ATT&CK techniques and expected countermeasures.
- Impact weighted scoring (scope x severity) across the chain; call out compounding risk ( $I + I = 3$ ).
- Validate findings with vendor to ensure understanding.
- Document a clear risk story: findings, ATT&CK mapping, evidence, and decision.

## Techniques for Deeper Assessments

- Ask of evidence of efficacy (test results) – not policy statements.
- Trace one attack path end-to-end (Initial Access → Lateral Movement → Impact).
- Weigh contextual factors: data sensitivity, geography, EoL/EoS, IR/BCP maturity, regulatory fit.
- Engage with SMEs (Architects, Engineers, etc.) to challenge assumptions.
- Set adaptive risk ratings + triggers for re-review (scope change, incident, pen-test results, etc.).
- Watch for Red Flags: MSSP-only security, no PAM/SEG/NIDS, etc.

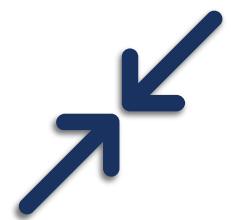
# SUMMARY AND Q&A

## BENEFITS • FINAL TAKEAWAYS • Q & A



### Benefits:

Fewer blind spots,  
earlier detection,  
better vendor  
partnerships.



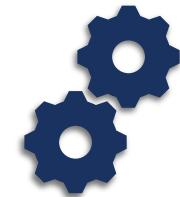
### I+I=3 Lens:

Evaluate how controls  
interact, not just if they  
exist.



### Next Steps:

Pilot the method on one  
high-impact vendor;  
define gates and Plan of  
Action & Milestones  
(POA&M).



### Q & A:

Discussion and  
Audience Insights.



## **ALICIA GRISTMACHER, CRVPM V, CVMPRA, CLP**

Manager, IT Vendor Risk Management

[alicia.gristmacher@hyatt.com](mailto:alicia.gristmacher@hyatt.com)

[www.linkedin.com/in/alicia-gristmacher](https://www.linkedin.com/in/alicia-gristmacher)

# THANK YOU