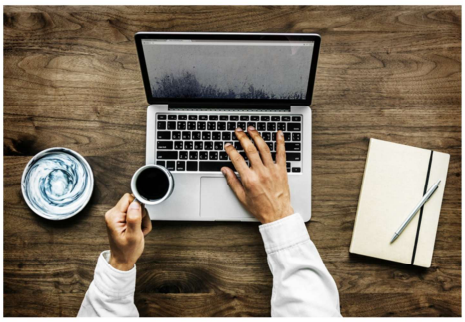
Consequence-Based Risk Assessment

MLM-019-C

Industry	– All
Principal Role	– All
Professional Role	– All
Enterprise Phase	– All



Turn on your audio and click start to begin video

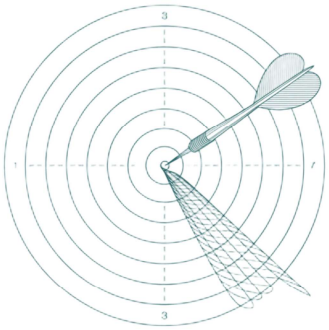
START

This Micro-Learning Module describes what MLMs are and how they are used in PERA.

It is intended for anyone interested in exploring new ways to share information on cybersecurity.

Click the START or NEXT button to advance to the next page.

Profiling Attackers (The Threat Approach)



Many standards categorize threats by the adversary.

- **SL-1:** Casual or coincidental violation.
- **SL-2:** Intentional violation using simple means (hackers).
- **SL-3:** Sophisticated attack with moderate resources (hacktivists).
- **SL-4:** State-sponsored attack with extensive resources.

If you open the standard, you will see that Security Levels are defined by who is attacking you. SL-1 is a casual violation, all the way up to SL-4 which is a state-sponsored attack. The buried assumption here is that you can predict your adversary and that their sophistication directly dictates your operational severity.

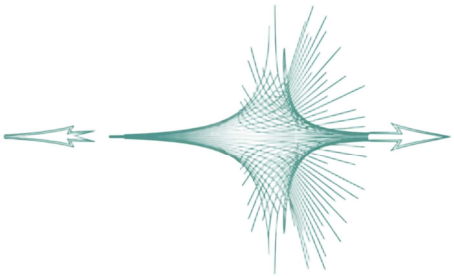
This is academically elegant but practically useless in the field.

The Flaw in Attacker-Based Models

- Categorizes threats by the attacker rather than operational impact.
- Assumes you can accurately predict adversaries and their motivations.
- Equates the sophistication of the attacker with the severity of the consequence.

Attacker-based models look great on a whiteboard but fail entirely on the plant floor. They force operators to play intelligence analyst by guessing who might attack and why, rather than focusing on the actual physical impact to the facility. The biggest danger in this framework is the assumption that a low-level hacker can only cause low-level damage. In reality, a control system does not check an attacker's resume or budget before executing a command.

Physics Doesn’t Care Who Hacked It



- The physical consequence is identical regardless of the attacker.
- The laws of thermodynamics do not adjust to the attacker's budget.
- **A boiler does not care who hacked it.**

The boiler does not care who hacked it.

If a command opens a relief valve when it shouldn't, the pressure vessel fails. The explosion that follows does not pause to check whether the attack originated from a state-sponsored actor or a bored teenager.

The consequence is identical.

Yet many risk-management frameworks would have you believe that defending against the script kiddie somehow requires less rigor than defending against the nation state actor.

The Real-World Mismatch

The Scenario: Unpatched safety system controlling a high-pressure process.

Attacker-Based View: A script kiddie using a trivial exploit is classified as an SL-2 threat.

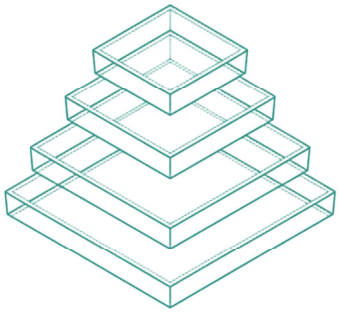
Operational Reality: A successful exploit results in an SL-4 consequence.

The Solution: Categorize operational outputs (consequences) rather than inputs (attacker capability).

Consider an unpatched safety system controlling a high-pressure process. The vulnerability is trivial to exploit. Under an attacker-based model, a script kiddie using that exploit is an SL-2 threat. But if they succeed, you get an SL-4 consequence.

The operational reality is obvious once you see it. It is just common sense to categorize outputs and operational consequences rather than trying to categorize inputs like attacker capability.

Consequence-Based Security Levels



SL-1: Was it inconvenient?

SL-2: Did it cost us money?

SL-3: Did it stop us or break something?

SL-4: Can it hurt someone?

Consequence-based classification is immediate. Attacker-based classification requires a crystal ball.

In operations, we only care about what happens when the attacker wins. Security Levels should act like Safety Integrity Levels. They should be based purely on the unmitigated consequence of failure. Look at the escalation thresholds on the screen. Did it cost us money? Did it break something? Can it hurt someone? These are observable questions any operator can answer without threat intelligence.

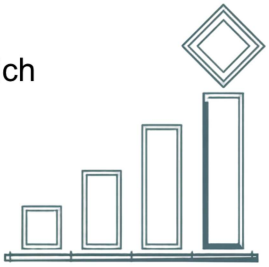
The Budget Conversation

Securing Leadership Buy-In

The wrong conversation: "We need to defend against nation states." (Leadership assumes this is impossible to fund).

The right conversation: "This system can kill people if compromised by anyone. It requires SL-4 controls."

This shifts the focus to engineering against failure modes, which operations leadership inherently understands.

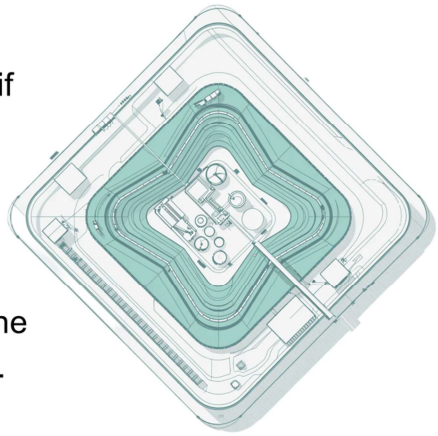


This shift fundamentally changes your budget conversations. When you ask leadership to fund defenses against nation states, they check the budget, realize they cannot outspend a foreign government, and end up doing less. But when you explain that a system can kill people if compromised by anyone, you are engineering against failure modes. That is a conversation operations leadership understands and will fund.

Practical Application

1. Identify exactly what each system controls.
2. Ask: "What is the worst thing that happens if an adversary gains full control?"
3. Assign the Security Level based strictly on that operational consequence.

Example: A critical relief valve gets SL-4 treatment because a teenager stumbling into the network can cause nation state consequences.



So how do we apply this? Walk your facility. Identify what each system controls and ask what the absolute worst outcome is if an adversary gains full control. Assign your Security Level based on that consequence. A system controlling a critical valve needs SL-4 protection, simply because a teenager stumbling into your network can cause a catastrophic event if the architecture allows them access to that valve.

The Bottom Line

1. We do not spend money to stop nation states. We spend money to stop explosions.
2. Security is not the ultimate goal. Operational continuity is the goal, and safety is the constraint.
3. Define Security Levels by consequence because the physics do not care who sent the command.

To wrap up, we do not spend money to stop nation states. We spend money to stop explosions. Security is not the ultimate goal for us. Operational continuity is the goal, and safety is the constraint. Start defining your Security Levels by consequence, not by the enemy. The physics of your plant simply do not care who sent the malicious command. Stay safe out there.

Author

River has two decades of experience as a network engineer, consultant, and cybersecurity strategist, specializing in Operational Technology (OT) and Industrial Control Systems (ICS).

As a renowned sector author and the founder of River Risk Partners, he has applied his deep research and technical expertise to secure critical infrastructure. His hands-on background includes network administration in rugged environments like coal mining, alongside the design of resilient OT architectures.

His strategic approach bridges the gap between technical execution and business risk, supported by his MBA and finance background. He also develops and delivers comprehensive OT security training, drawing on years of dedicated research and frontline incident response.