Behaviors and Processes for Maximizing Return on Investment within Threat Modeling

Planet Cyber Sec Conference

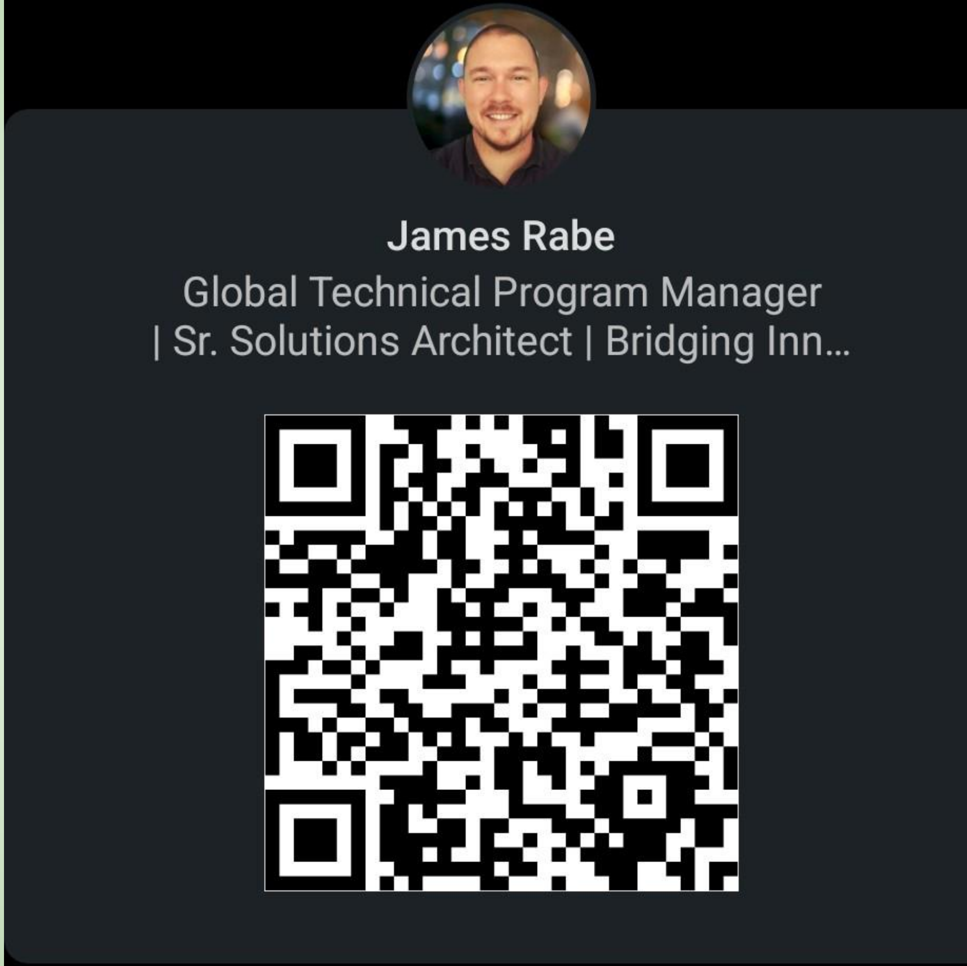
Bio

Threat Modeling, Cybersecurity

TMC - Founding Member

James Rabe

linkedin/in/jrabe3



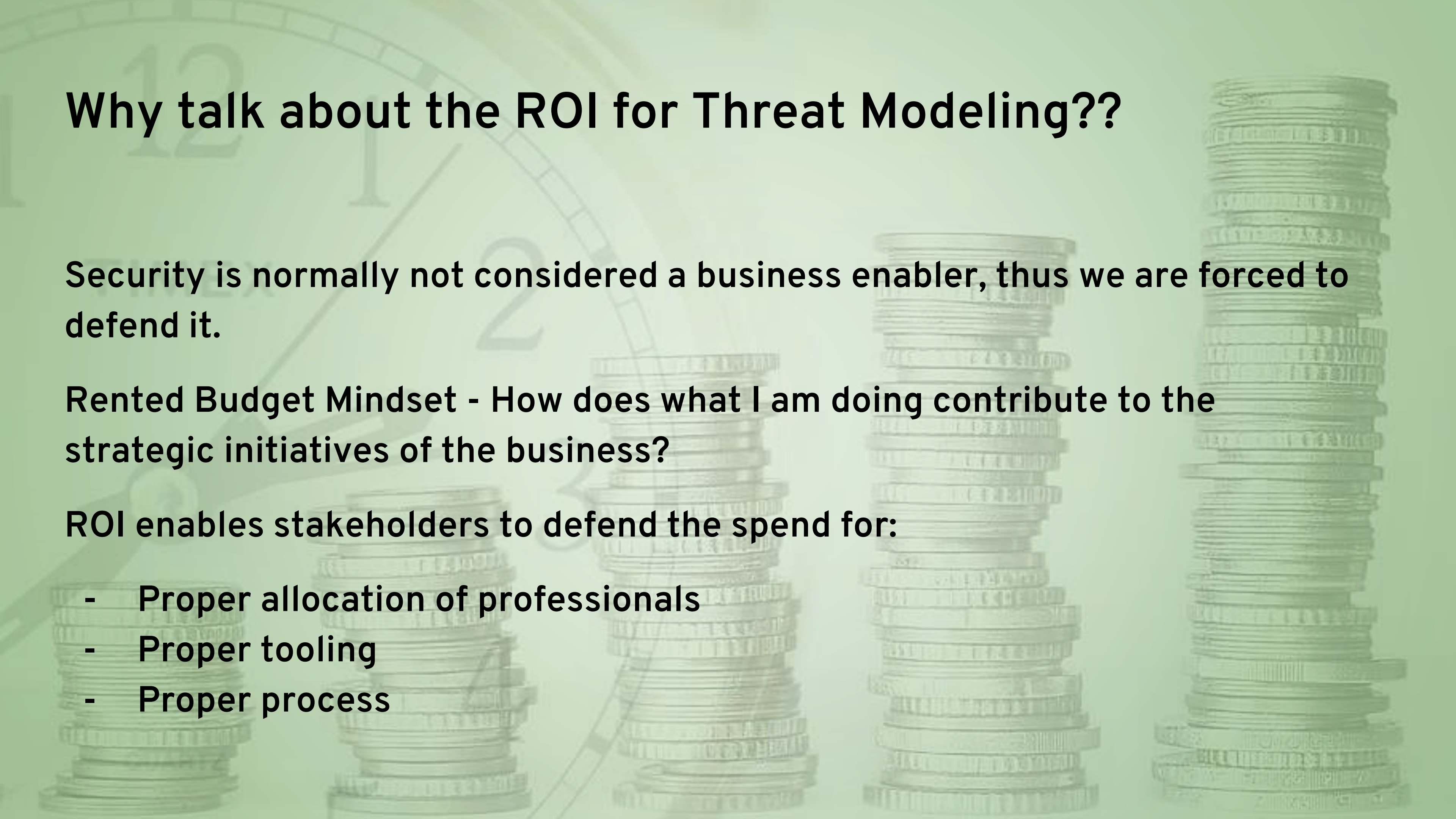
James Rabe

Global Technical Program Manager | Sr. Solutions Architect | Bridging Inn...

Discussion Topics

What is ROI in Threat Modeling

Maximizing ROI through best in class behaviors



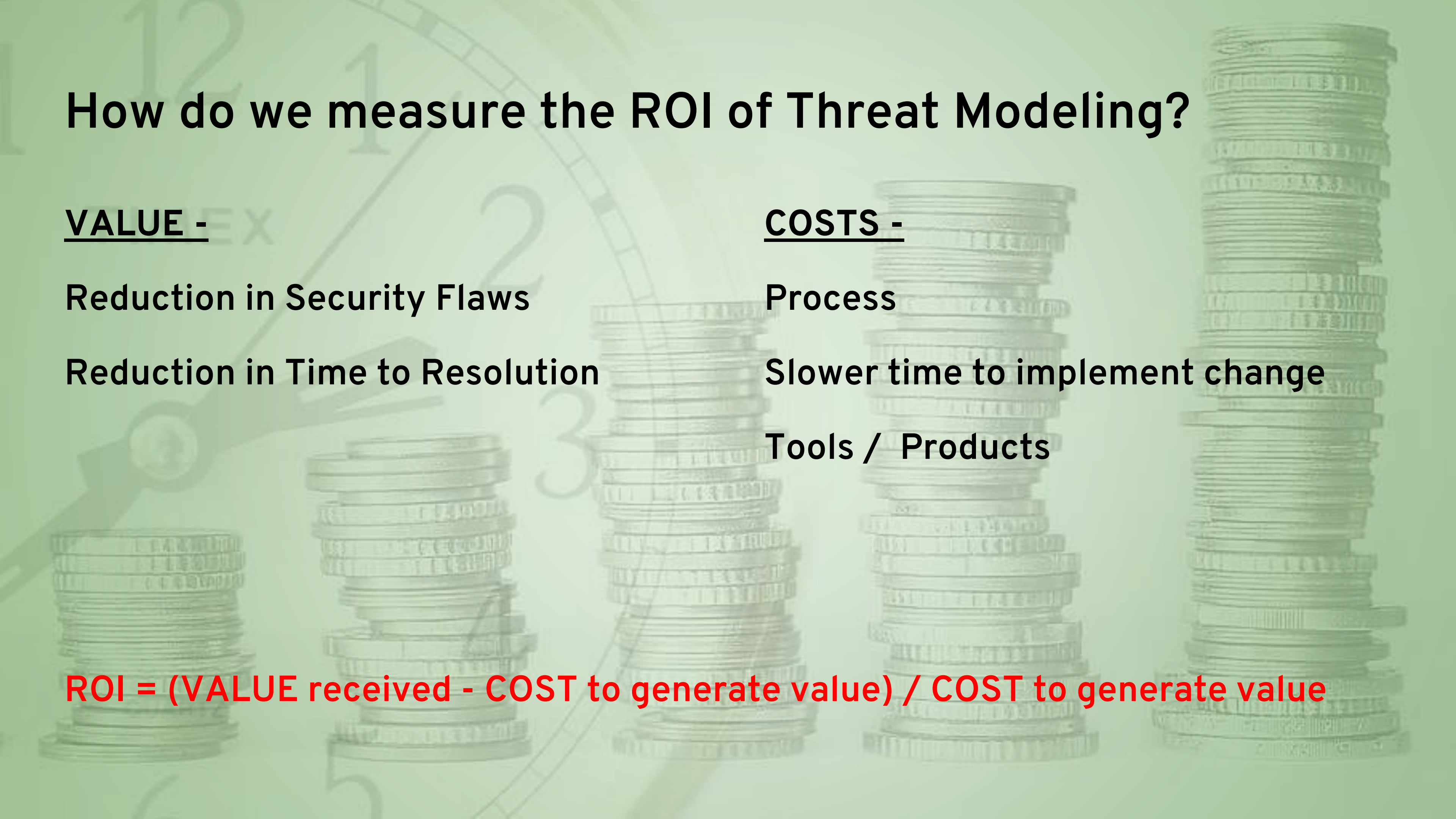
Why talk about the ROI for Threat Modeling??

Security is normally not considered a business enabler, thus we are forced to defend it.

Rented Budget Mindset - How does what I am doing contribute to the strategic initiatives of the business?

ROI enables stakeholders to defend the spend for:

- Proper allocation of professionals
- Proper tooling
- Proper process



How do we measure the ROI of Threat Modeling?

VALUE -

Reduction in Security Flaws

Reduction in Time to Resolution

COSTS -

Process

Slower time to implement change

Tools / Products

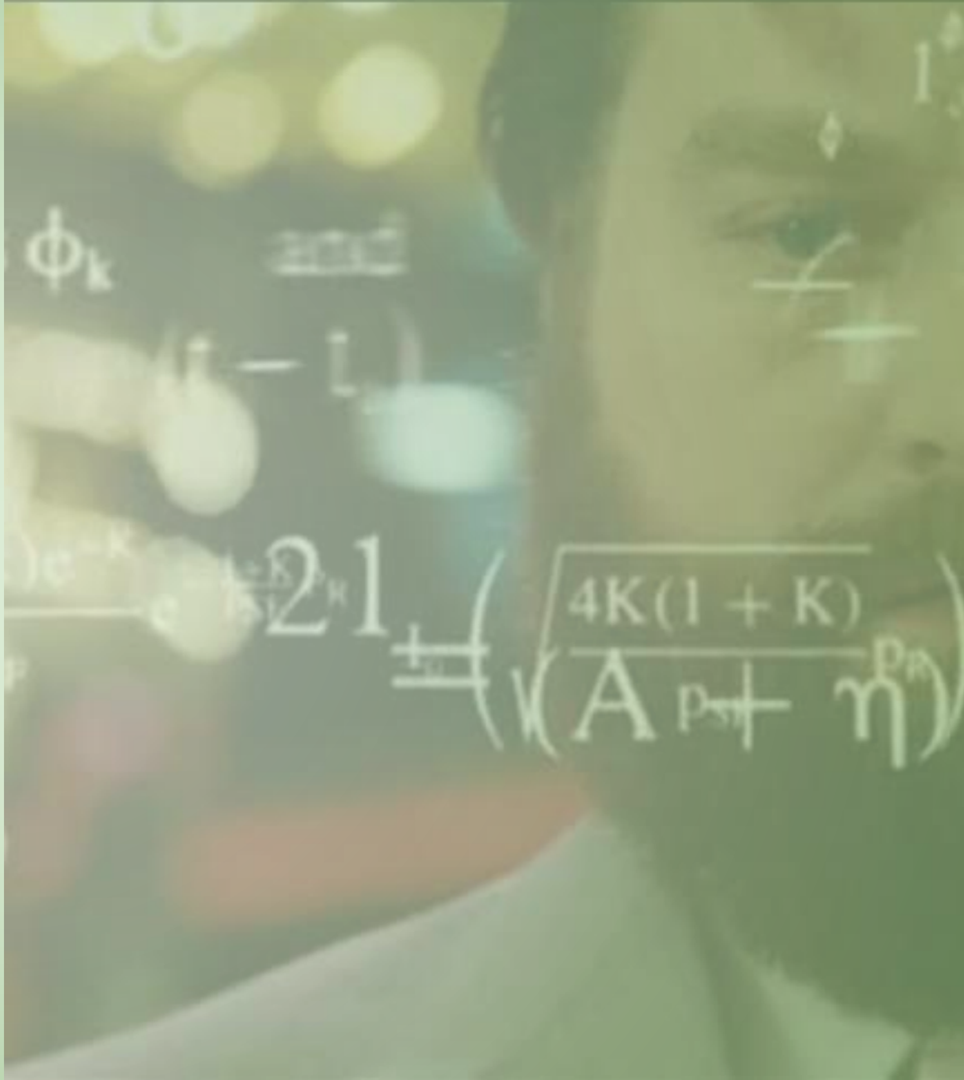
ROI = (VALUE received - COST to generate value) / COST to generate value

How does this impact the overall ROI of the business?

ROI for the Threat Model is a function of the overall product ROI which is then a function of the business ROI

In reality, this is a weighted ROI inside of a weighted ROI, inside of a weighted ROI…

Should we actually pursue this calculation?



How do we maximize ROI?

INCREASE THE VALUE & DECREASE THE COSTS

- Secure by design
- Decrease time to resolve issues
- Faster process (remove waste)
- Standardized Process
- Standardized tooling

Secure by Design – Laying the foundation

Security in Context - Right sized security

Defense in Depth - Layered defense

Standardized Components

Connections - Interconnectivity + Ecosystem

Secure Code - Make secure code the easy path

Decrease time to resolve issues

Design stage threat modeling highlights security flaws at their most cost effective point

Fixing the same flaw in production can cost 5x to 100x more than fixing it in the design phase

Standardized Process

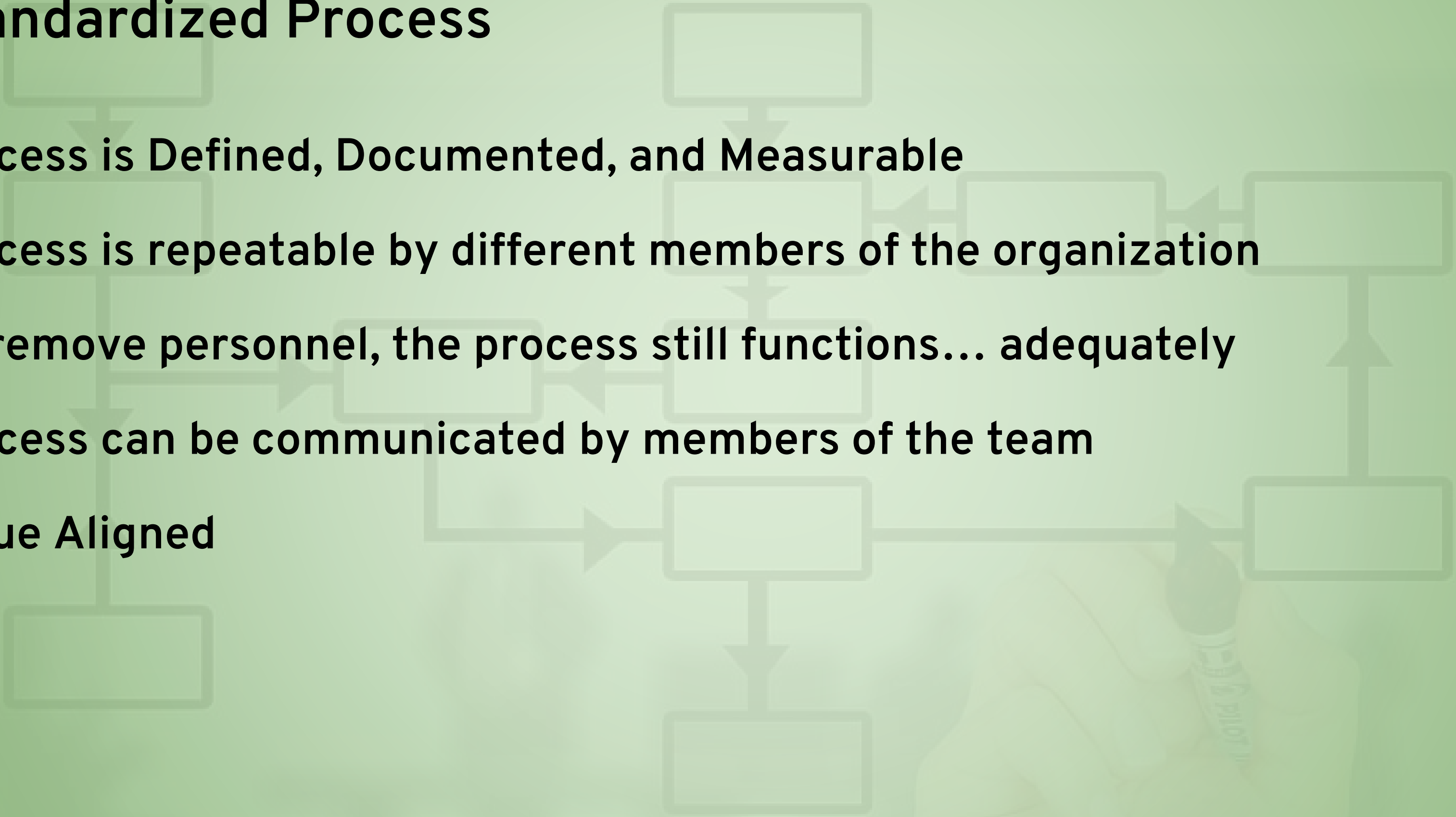
Process is Defined, Documented, and Measurable

Process is repeatable by different members of the organization

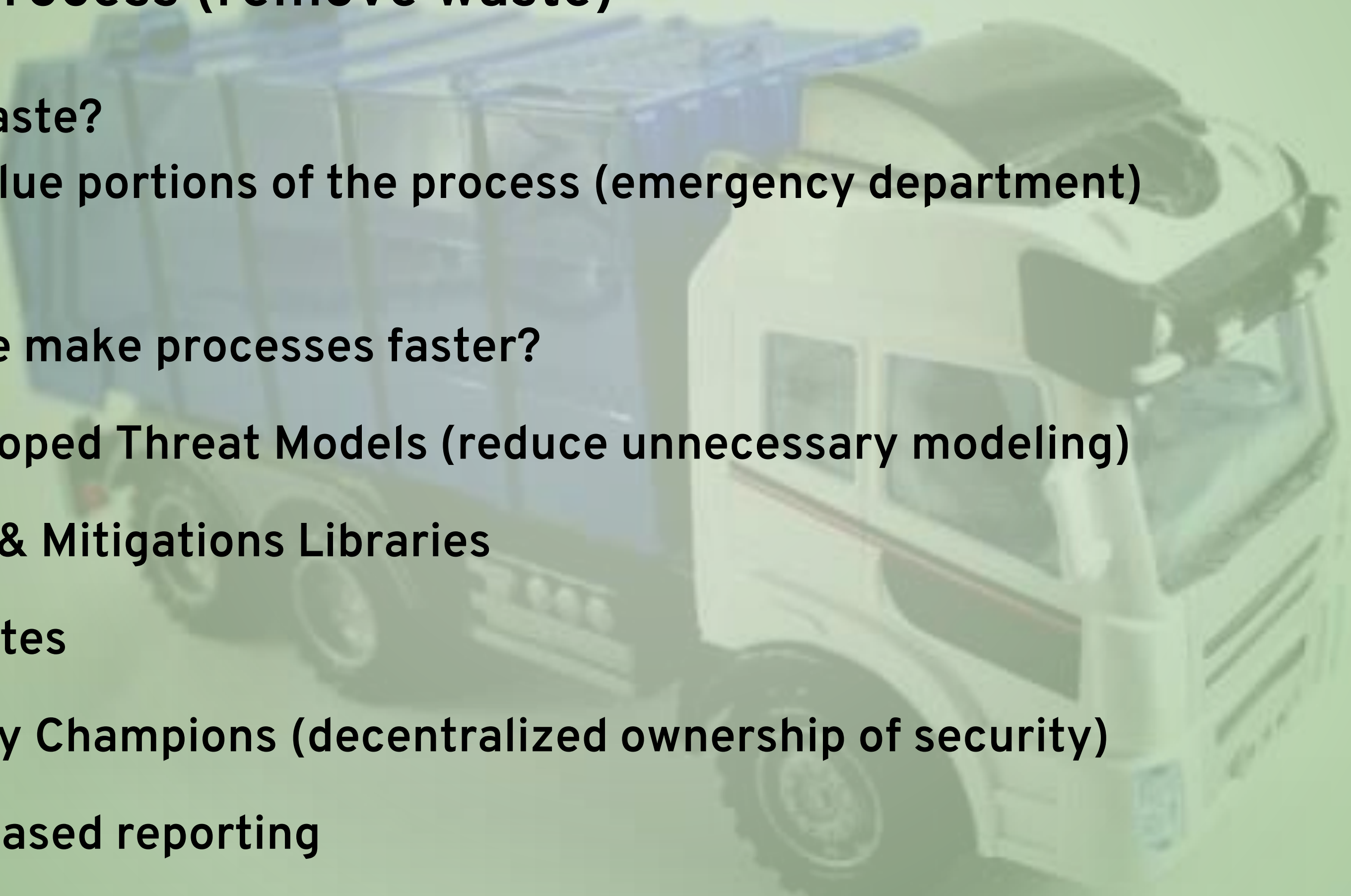
If I remove personnel, the process still functions… adequately

Process can be communicated by members of the team

Value Aligned



Faster Process (remove waste)



What is waste?

- Non-value portions of the process (emergency department)

How do we make processes faster?

- Well Scoped Threat Models (reduce unnecessary modeling)
- Threat & Mitigations Libraries
- Templates
- Security Champions (decentralized ownership of security)
- Value based reporting

Standardized Tooling

Improves Interoperability

Easier to measure

Transferrable

Single Language for communication

Exchangeable Templates

Env & Architectural Sharing

Freesources (Free + Resources)

Free Platform for Threat Modeling - https://community.iriusrisk.com

OWASP Threat Modeling Cheat Sheet - https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html

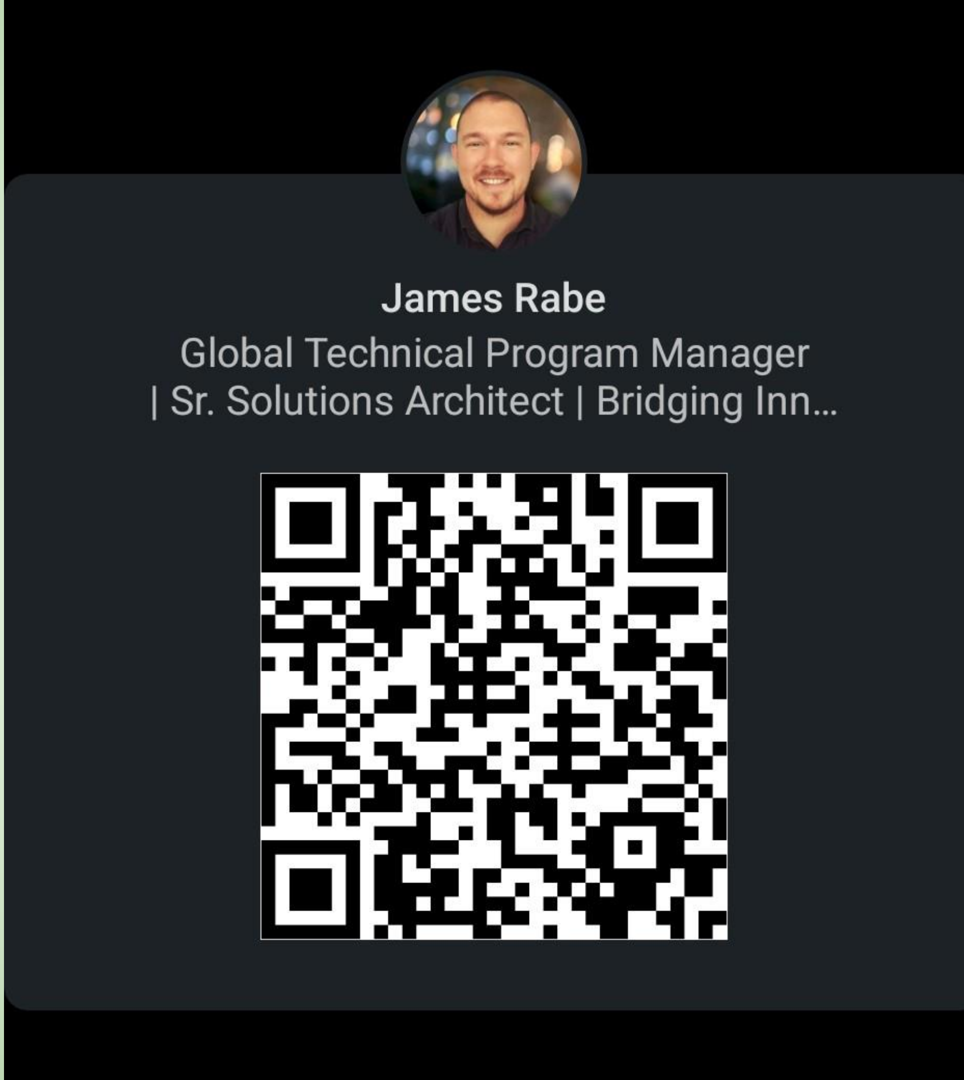
World's Shortest Threat Modeling Course - https://www.youtube.com/watch?v=2pvprvsr1lo

*Threat Modeling Connect - https://*threatmodelingconnect.com

Connect with me

James Rabe

linkedin/in/jrabe3



James Rabe

Global Technical Program Manager
| Sr. Solutions Architect | Bridging Inn...