SOC ReLoad
#SOCReLoad21

TRACK 2 - OPERATIONS

Why Getting the Fundamentals Right is Key for Establishing a Modern SOC

RoseAnn Guttierrez
Business Development,
Technical Enablement Specialist

IBM Security

Gaye Güven
Technical Alliances &
Partnership Specialist

PICUS

SOC Challenges?

SOC Challenges – The 4 V’s

VISIBILITY

VOLUME

VERIFY

VACUUM

Attack the challenges with fundamentals:

> “Fundamentals, fundamentals, fundamentals. You've got to get the fundamentals down because otherwise the fancy stuff isn't going to work.”
>
> **– Randy Pausch.**

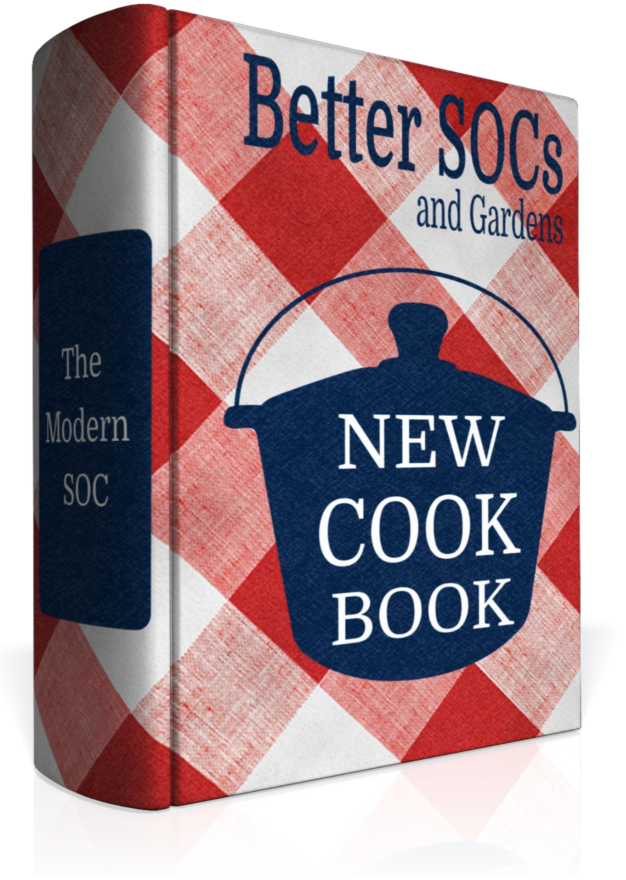
The "fancy stuff"

Automation
Forensics
Threat Hunting
Threat Intelligence

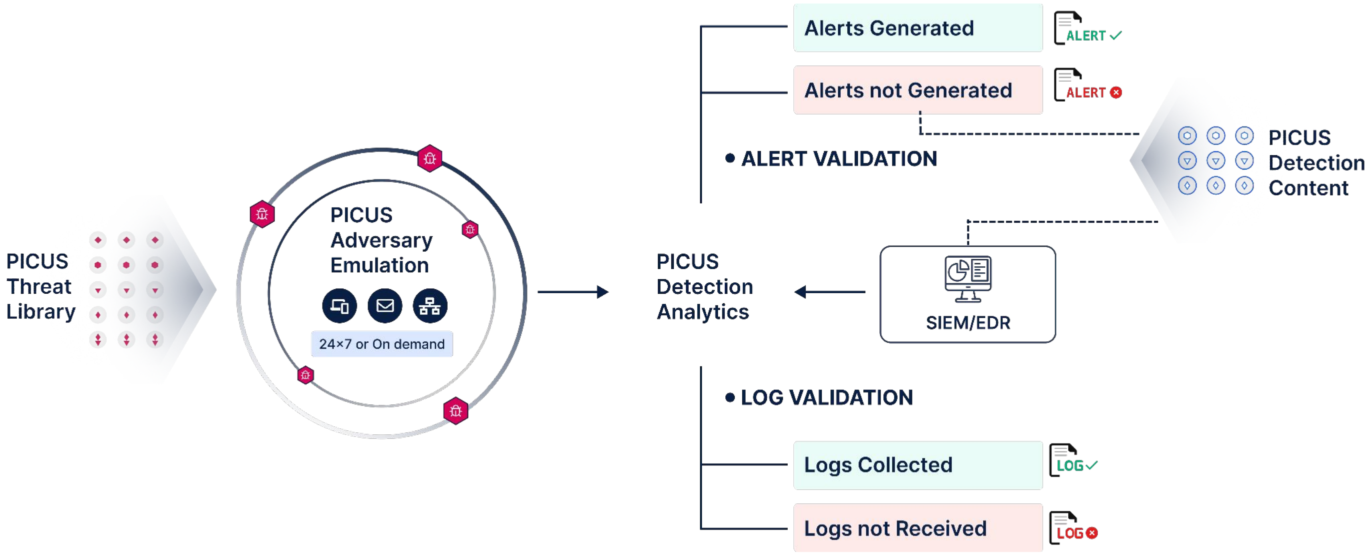
Recipe for a Modern SOC

2 cups	People
1 cup	Business objectives
½ cup	Security controls
⅓ cup	Compliance
3 Tbs	Documented processes
2 cups	Carefully considered tools
⅓ cup	Automation
1 cup	Fancy stuff

Bring to a simmer and then season to taste.



“Prevent — Detect — Response”



THANK YOU!