Metrics: Beyond ROI

Shawn Chakravarty & Kevin Tyers

SANS SOC Summit 2015

Table of Contents

To maintain privacy for our current and previous employers, numbers have been changed.

Who we are

Shawn Chakravarty

Sr. Manager of Security Incident Response

Kevin Tyers

Information Security Engineer

Concepts

Concepts

High Level

- What does your business find most valuable?
- Does ROI always have to be represented in money?
- Do you have a top to bottom metric strategy?

Technical

- Do you have the means to gather metrics?
- Do you visualize your metrics?
- Are you consistent in your data collect?

"What's measured improves"

Peter F. Drucker

Value Scale

Different Metrics mean
Different Things to
Different People at
Different Levels

C-Level and Board Metrics

(Or Why are we paying for this?)

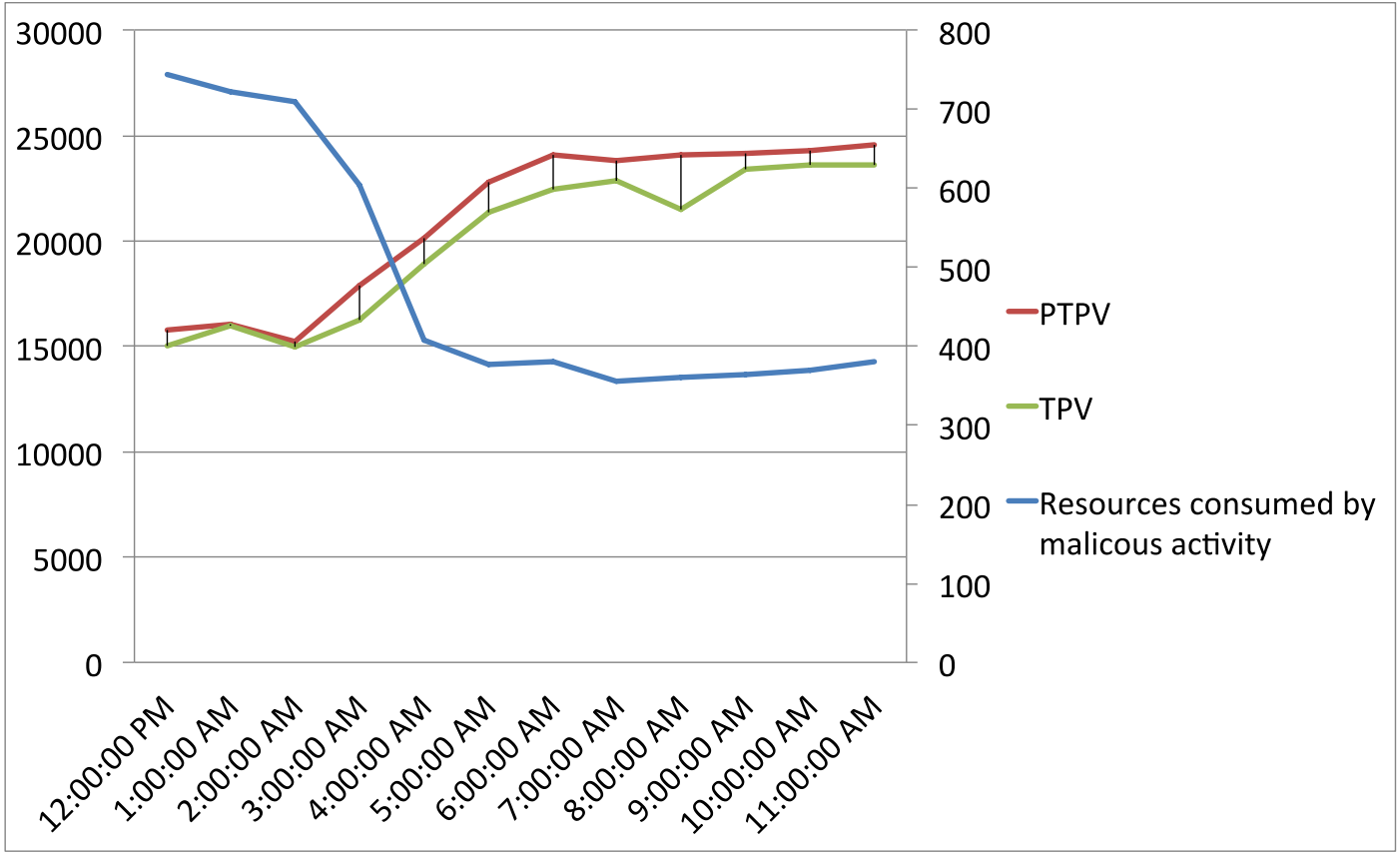
C*

What is valuable for the business?
How do we measure this?
How much does one *x* cost to protect *y* units of value?

C Suite - Aggregate Available Resources

Var	R = RAM BW = Bandwidth C = CPU A = Aggregate Available Resources
Eq	(R + (BW * .01)) * C = A
Ex	(10 + (1 * .01)) * 2 = 20.02

C Suite - Aggregate Available Resources v. (P)TPV



Director and VP

(Or how do we plan?)

Dir/VP

How do we enable the business?
What can we measure for guidance?
Where are resources best spent?

Force to Load - Basic

Var

M = Mean time to restore
A = Analyst
T = Tickets
H = Hours

Eq

(T * M))/(A * H) = Force to load (F)
F = 1.0 is perfect

Ex

(500 * 4)/(50 * 40) = 1.0 Perfect
(500 * 4)/(25 * 40) = 2.0 Need more resources!
(500 * 4)/(75 * 40) = .67 Need more work!

Force to Load - Advanced

Weighted ticket types

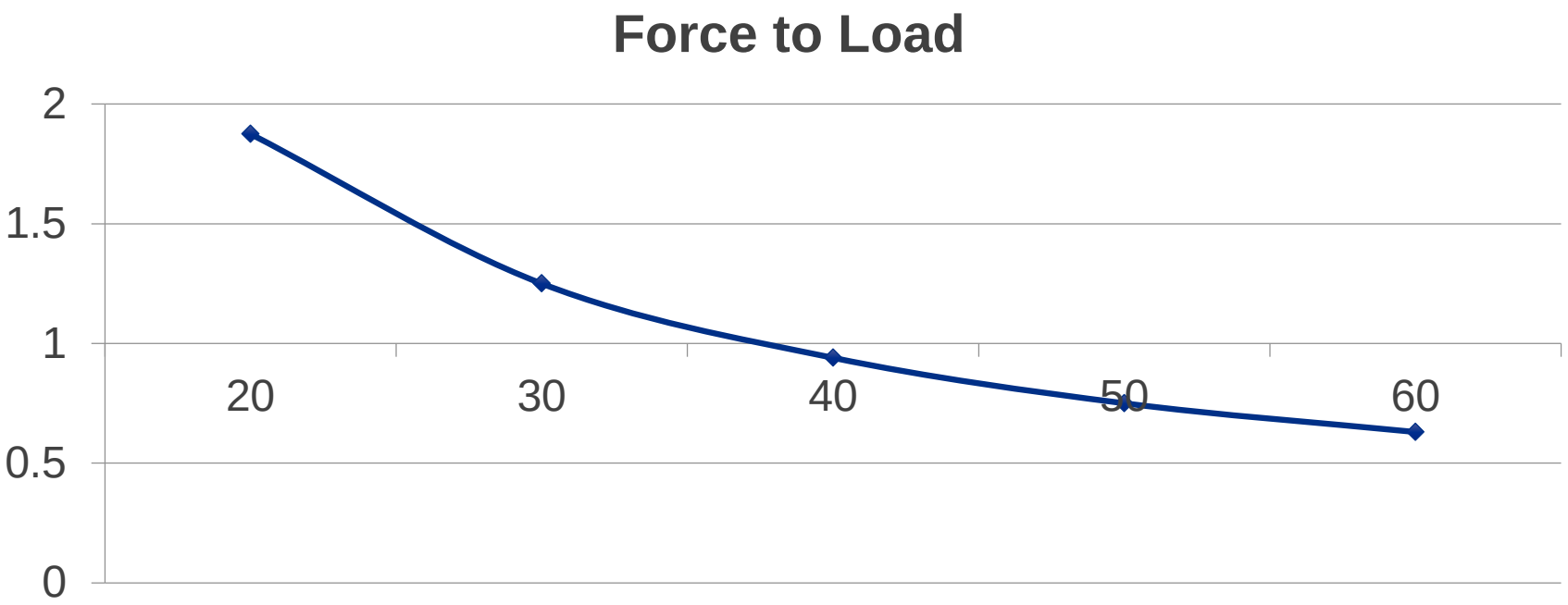
Eq

$$(T1 * M1) + (T2 * M2) + \ldots (T_n * M_n)/(A * H) = F$$

Ex

((25*8)+(300*4)+(200*.5))/(50 * 40) = 0.75
((25*8)+(300*4)+(200*.5))/(25 * 40) = 1.5
((25*8)+(300*4)+(200*.5))/(75 * 40) = 0.5

Force to Load: Visually



Multi-tier Metrics

Force to Load

Director

- What are my budget needs?
- What is our security effectiveness?
- What does my threat landscape look like?

Manager

- Where is our time going?
- Where can we automate?
- What training do we need?

Managers

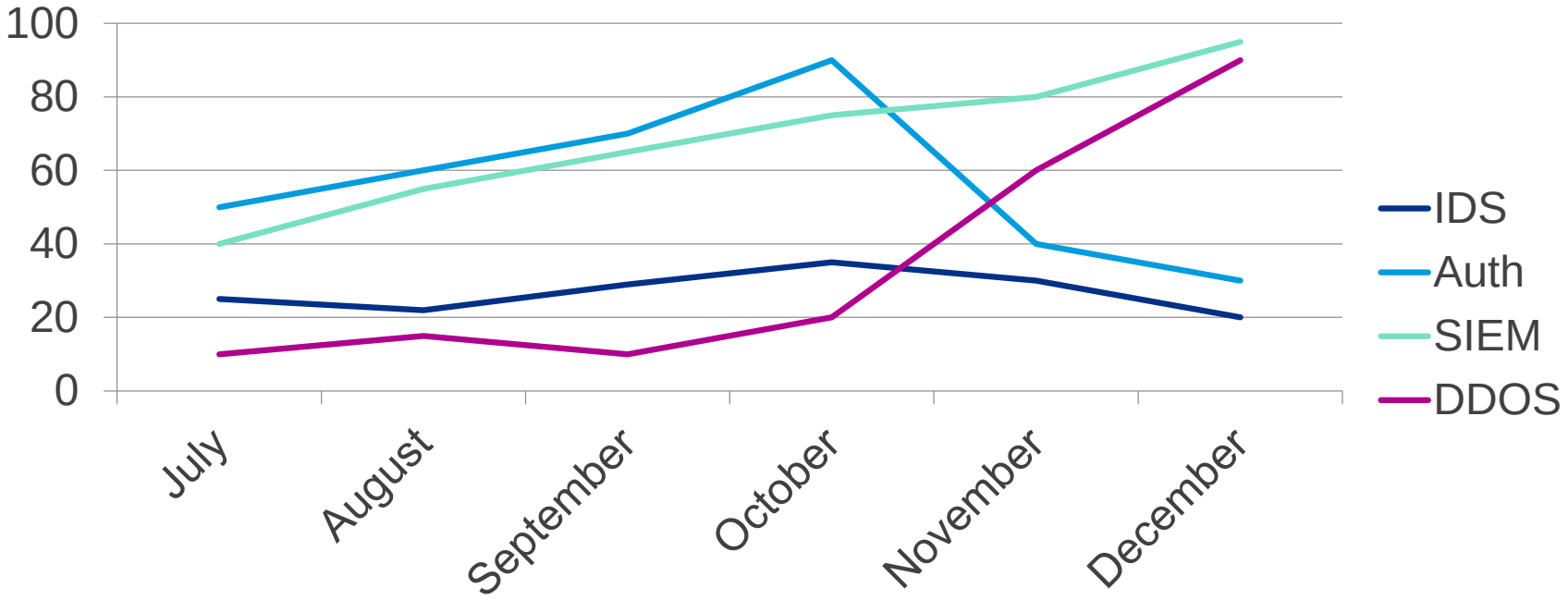
(Or how do we execute?)

Mgr

Encourage IC development
Addressing bad behaviors
Maximizing tactical capacity

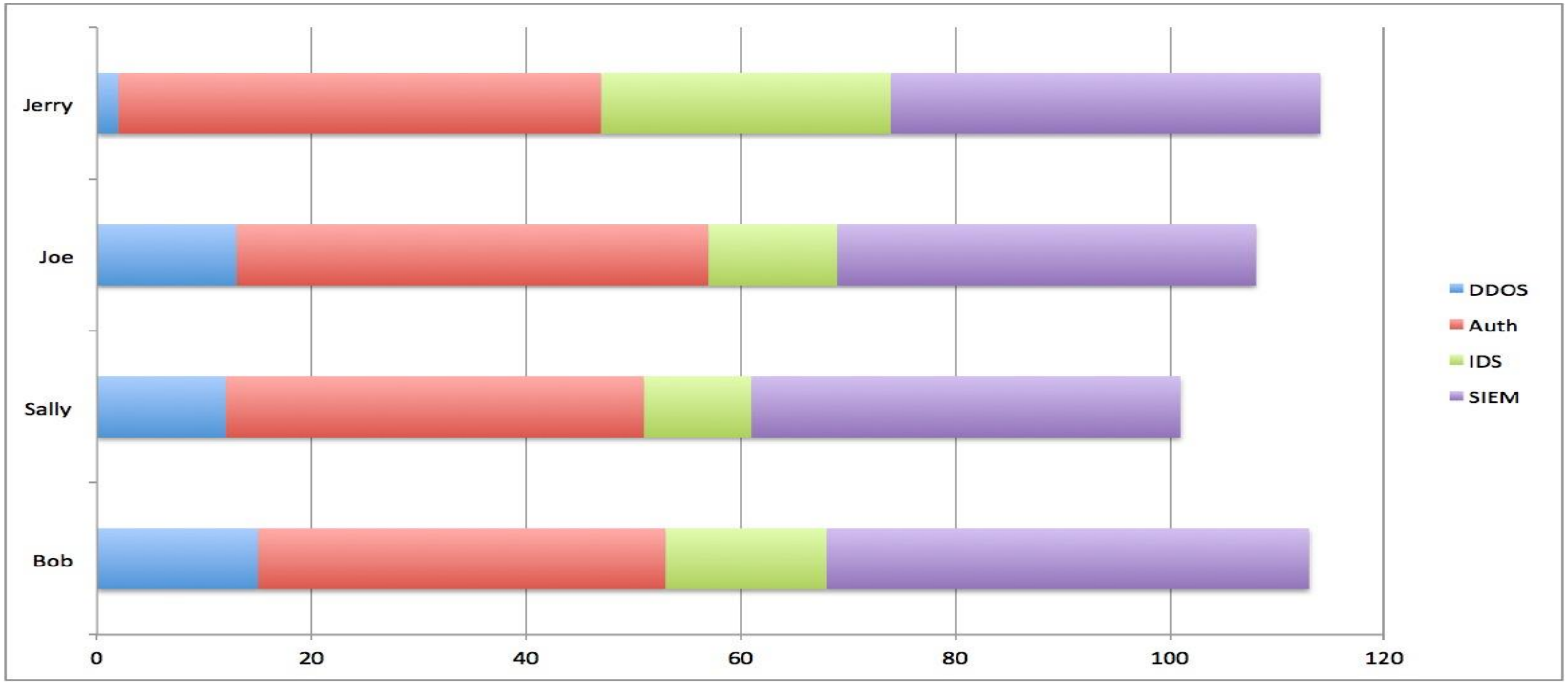
Roadmapping: Tickets by Analyst Hours

Where are we spending our hours?



Roadmapping: Tickets Worked by Analyst

Who is working what issues?



Analyst/Individual Contributor

(Or how can I help?)

IC

What am I contributing?
Where can I improve?
What is my career roadmap?

IC Knowledge Roadmap

Var

S = Subject
C = Comfort (1-10)
R = Required knowledge (1-10)

Eq

$[C(S) < R(S)] \rightarrow Study(S)$

Ex

C(Networking) = 8 – Learn as needed
C(Linux Admin) = 4 – Prioritize

Knowledge Matrix

Subject	C(S)	R(S)	Diff	Plan
Networking	8	6	+2	Learn as I go
Coding	8	3	+5	Pick up stuff as needed
Linux Admin	4	5	-1	Take the GCUX
Data Science	3	6	-3	Take Coursera Stats class
Documentation	5	5	0	Take a business writing course
Leadership	6	2	+4	Mentor new analysts

Thank you for your time

Questions?