SR (securit)E

Tom Schmidt • March 14, 2017

Security Engineers

What is a security engineer?

Software Engineer

Security training / experience

“Belief in and aptitude for developing software systems to solve complex problems”

… why is it worth hiring a team of them?

But...

… system administrators are less expensive!

… we don’t have time for that!

… I already have a security focal!

… none of my engineers want to install patches!

Security is not a checkbox

As scope expands, so too do security and compliance requirements

Many security and compliance requirements are ongoing

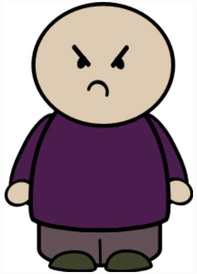
Toil: “Manual, repetitive, automatable, devoid of enduring value, and scales linearly”

Monitoring and Logging: Meeting the Requirement

Dump all logs to event manager (QRadar)

Monitoring and Logging:
Scaling out of control

Mandate components to send relevant, well-formatted logs



Monitoring and Logging: Engineering a solution

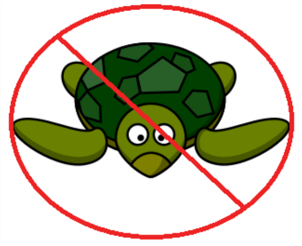
Design and develop a common solution (Node middleware, Java servlet filter)

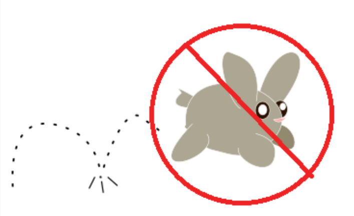
Easy integration / configuration for every component

Scalable, efficient, effective

Bonus: Contribute to the open source community

Secure Engineering = (Maintainable) Velocity





Say NO to “Stop and Go”

(Also, say no to slow)

Automation and common solutions as the DEFAULT approach

Consistency, Efficiency

(Tempered) Acceleration

Thanks!