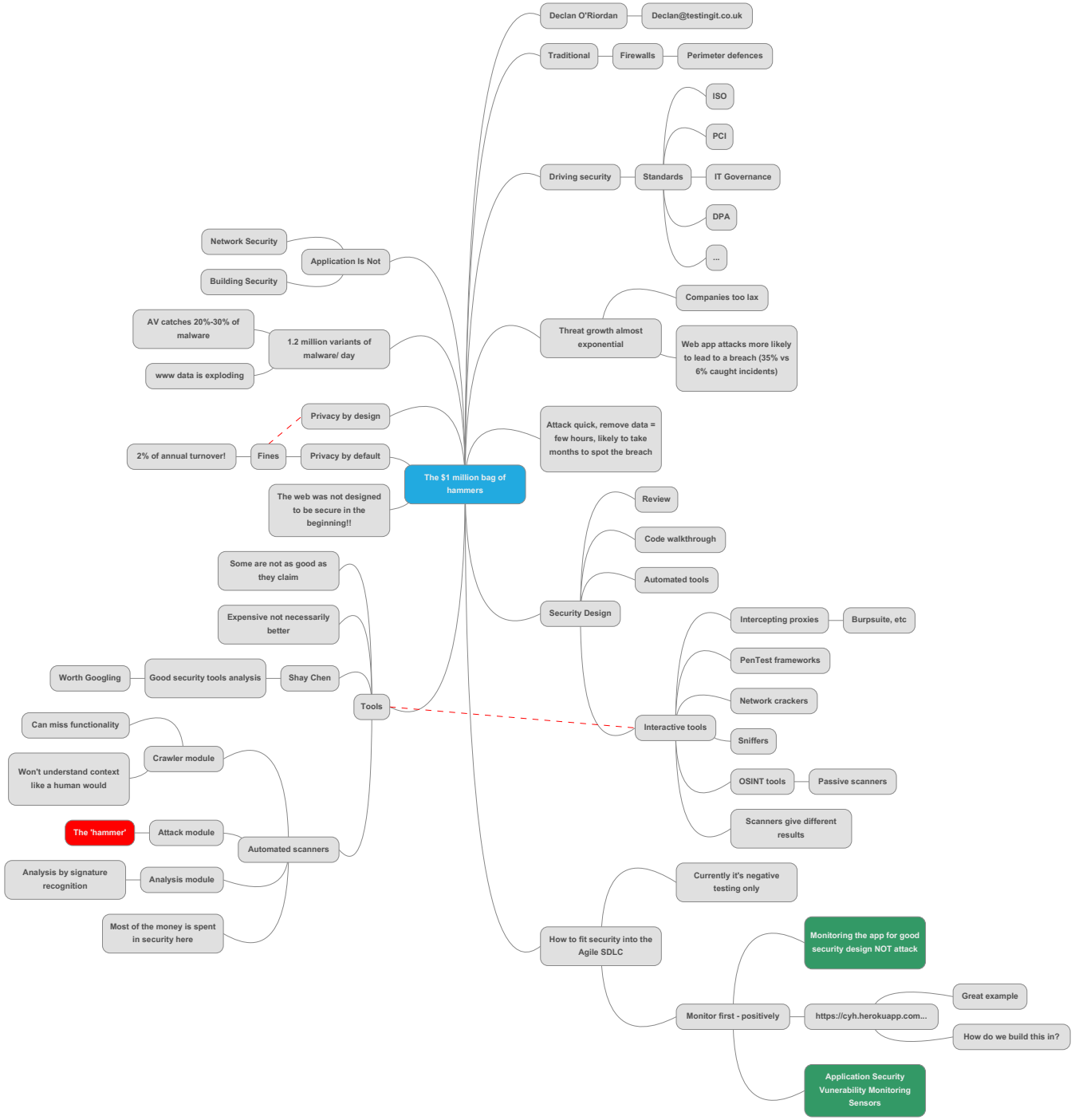
The $1 million bag of hammers
Declan O'Riordan
Declan@testingit.co.uk
Traditional
Firewalls
Perimeter defences
Driving security
Standards
ISO
PCI
IT Governance
DPA
...
Threat growth almost exponential
Companies too lax
Web app attacks more likely to lead to a breach (35% vs 6% caught incidents)
Attack quick, remove data = few hours, likely to take months to spot the breach
Security Design
Review
Code walkthrough
Automated tools
Interactive tools
Intercepting proxies
Burpsuite, etc
PenTest frameworks
Network crackers
Sniffers
OSINT tools
Passive scanners
Scanners give different results
How to fit security into the Agile SDLC
Currently it's negative testing only
Monitor first - positively
https://cyh.herokuapp.com...
Great example
How do we build this in?
Monitoring the app for good security design NOT attack
Application Security Vunerability Monitoring Sensors
Application Is Not
Network Security
Building Security
1.2 million variants of malware/ day
AV catches 20%-30% of malware
www data is exploding
Privacy by design
Privacy by default
Fines
2% of annual turnover!
The web was not designed to be secure in the beginning!!
Tools
Some are not as good as they claim
Expensive not necessarily better
Shay Chen
Good security tools analysis
Worth Googling
Automated scanners
Crawler module
Can miss functionality
Won't understand context like a human would
Attack module
The 'hammer'
Analysis module
Analysis by signature recognition
Most of the money is spent in security here