# Security Engineering

## A manifesto for defensive security

Tim (Wadhwa-)Brown
Head Of Research, CX EMEAR Security Architecture
June 2019

# # whoami

- Tim (Wadhwa-)Brown
  - 14+ years at Portcullis (and now Cisco)
  - Head Of Research & Security Architect, CX EMEAR Security Architecture
    - Ex-NCSC CHECK Team Leader (9 years)
    - CREST Registered Threat Intelligence Analyst
    - CREST Practitioner Intrusion Analyst
    - ISO 27001 LA
- >150 CVEs to my name
  - Covering Windows, Linux, AIX and Solaris platforms
    - Userland through to kernel
  - Most recent research: Where 2 Worlds Collide: Bringing Mimikatz et al to UNIX, Black Hat Europe 2018
- I own an ISP ☺

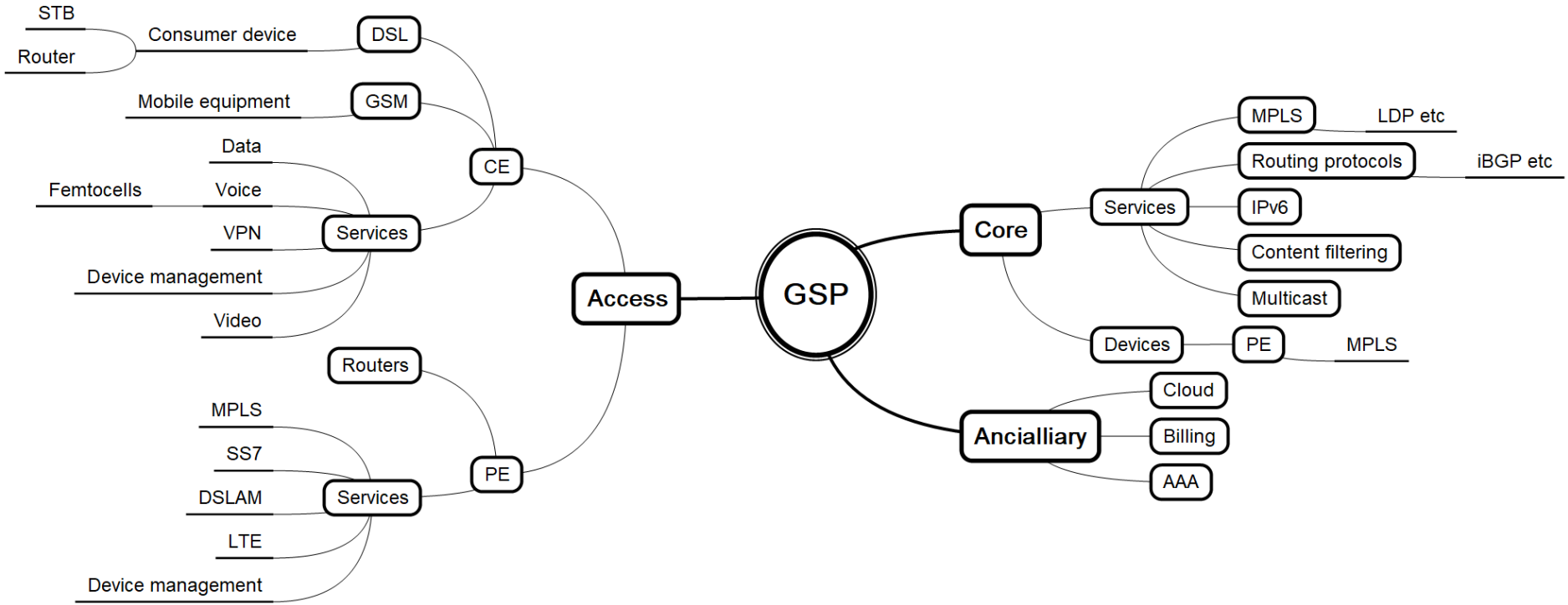
# # cat .plan

- Some apologies
- Personal lessons
- About you
- The blue team isn’t improving quickly enough
- Doing things differently
- Making money out of MITRE

# Who are CX Security Architecture?

# CX Security Architecture

- Professional services aligned to security
  - Advisory & implementation
    - SOC
    - Incident Response
    - Red Team
    - Security Engineering
      - Cisco's products…
        - And a whole heap more


GSP
Access
CE
DSL
Consumer device
STB
Router
GSM
Mobile equipment
Services
Data
Voice
VPN
Device management
Video
Femtocells
PE
Routers
Services
MPLS
SS7
DSLAM
LTE
Device management
Core
Services
MPLS
LDP etc
Routing protocols
iBGP etc
IPv6
Content filtering
Multicast
Devices
PE
MPLS
Ancialliary
Cloud
Billing
AAA

# Some apologies

# Helping the blue team – a case study in 3 parts

# Abstract bug classes

- Active Directory on UNIX
  - We shared IOCs
- Run-time linkers
  - We wrote patches for ld.so
- Shared memory
  - We provided source code analysis tooling

# Blue team can’t adapt quickly enough

# GSP examples from Ross Anderson's book*

* Security Engineering, first published in 2008

# “Phone phreaking”

- Metering
- Signaling
- Switching and configuration

# The mobile landscape

- Identity
- Connectivity
- Platform

Nothing much has really changed!

# Adoption of improvements

# Architecture

- Still largely taken to mean “using a firewall”
  - How do SDNs affect us?
- Often network rather than data centric
  - Do we consider what the value of the data is when we choose where to keep it?
- Don’t consider what happens when we don’t own either the data and/or the platform

# Identity and access management

- Relies on password strength and lifetime
  - Can we spot password usage and other bug classes in protocols?

# Vulnerability management

- Relies on vulnerability blacklists
  - What do we do if a critical patch comes out the day after a scan?
- Technical observations don't give appropriate context
  - Can we answer the question "where is this exploitable from"?

# Binary hardening

- Expect the appropriate compiler flags to be utilized
  - Are we helping bug classes die?
- Choose memory safe languages wherever possible
  - Are we keeping bug on life support?
- Require reproducible builds?
  - How do we trust our vendor?

Like Ross’ book, the CIS top 20 controls are over 10 years old

*“Offensive security = vulnerabilities = blacklists.”*

Me

# Offensive security…

- Introduces fatigue
  - Patching is hard
- Results in tactical fixes
  - Spot fixes don’t tackle root causes
- Makes it hard to quantify risk
  - How do we put a cost on 400 arbitrary vulnerabilities

# How to we improve faster?

- Protocols and technologies in general show signs of weakness way before the vulnerabilities come to light
  - We’re not benefitting from this, either at…
    - Procurement
    - Design
    - Deployment

Just like you, Cisco is keen to improve the way organisations are secured

# Moving the dial

- Risk modelling
- Threat modelling
- Intelligence gathering

# What are we looking at?

- Identification of revenue impact
- Quantification of risk
- Validation of loss frequency
- Decreasing contact and increasing resistance
- Recognising transformation opportunities
- Removing toil
- Reducing loss

# Looking at the way we report

# Why don’t businesses leaders listen to “security experts”?

- We should identify revenue impact
  - We need to understand
    - Service lines
    - Dependencies
  - Which of C/I/A matters?

# Transformation needs to be business aligned*

* e.g. eTOM, SID, TAM etc

# Re-examining how we think of and talk about risk

# Combining loss frequency and loss magnitude?

- We should quantify risk
  - We can’t do much about actor’s capability and actions
  - We can effect contact frequency and resistive strength

# Leveraging threat intelligence

# How do we simulate GSP associated threat groups?

- We should study the news
  - What are GSPs reporting?
- We should decompose the attacks
  - What TTPs were in play?
- We can then build hypotheses
  - Might these be relevant to our customers?
- This will allow us to understand…

# Are our revenue generating services exposed?

- We should validate loss frequency
  - Building risk and threat models to reflect on case studies

# Using technical activities more effectively

# What controls are effective?

- We should invest in decreasing contact and increasing resistance
  - Architectural analysis of control set
  - Resistive property analysis of products
  - Use of DevSecOps to drive continuous improvement

# We can help augment your internal skills

- We’re specialists at operationalising Cisco product
  - If you need support to take StealthWatch from the NOC to the SOC
  - To deploy Umbrella at scale
  - Or to enable Duo for your customers
- We’re here to help!

# Treating enterprise, legacy and greenfield differently

# Can we leverage this information as we shift left?

- Enterprise
  - Endpoints, mail, file shares etc
  - Need to reliably deliver critical controls
- Legacy
  - Systems that generate revenue
    - May not be legacy at all
  - Need to integrate with service aligned platform and application teams
- Greenfield
  - Systems that you hope will generate you revenue in the future
  - Need to shift left
    - DevSecOps
    - CI/CD

# Using orchestration to augment operation

# Does this help us use our limited human capacity more effectively?

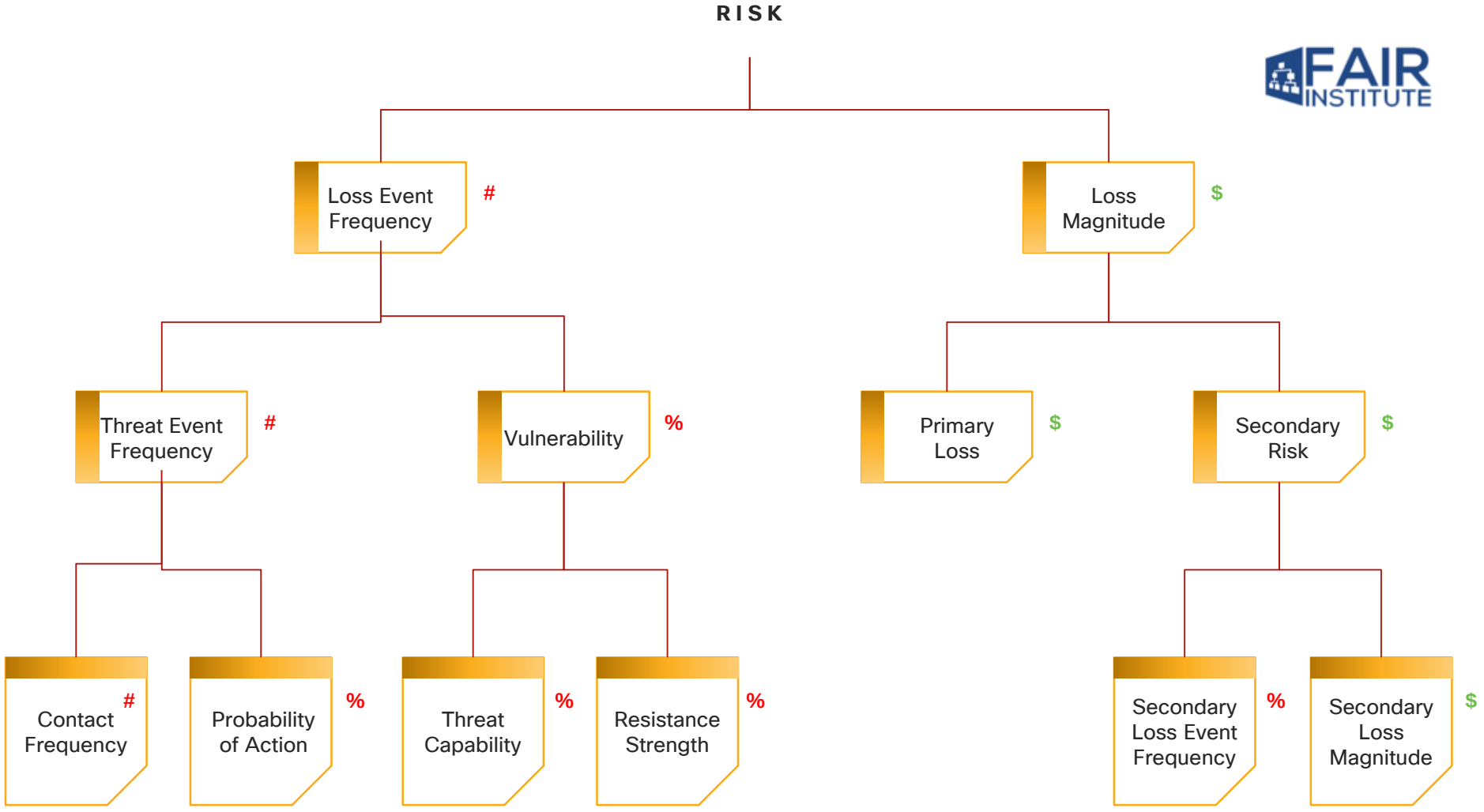
- Automation
  - Enables reliable delivery of critical controls
- Orchestration
  - Allows service aligned integration into wider organisation
- Both will help you scale but only orchestration allows scale outside of the technical space

# Helping to set and measure KPIs with adversary simulation

# Are we being FAIR*?

* Factor Analysis Of Information Risk

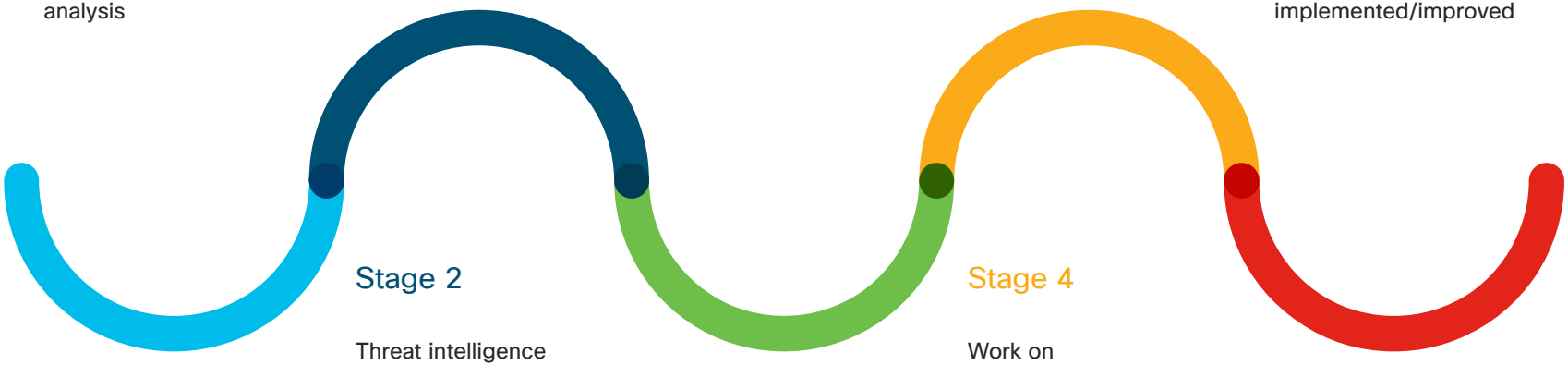
*“You can’t effectively and consistently manage what you can’t measure, and you can’t measure what you haven’t defined.”*


RISK
FAIR INSTITUTE
Loss Event Frequency
#
Loss Magnitude
$
Threat Event Frequency
#
Vulnerability
%
Primary Loss
$
Secondary Risk
$
Contact Frequency
#
Probability of Action
%
Threat Capability
%
Resistance Strength
%
Secondary Loss Event Frequency
%
Secondary Loss Magnitude
$

# FAIR enables decision making using an analytical model

# What might a typical customer journey look like?

# Example project



# Challenges we will all face

- Asset management and change control
- Understanding threat groups
- Developing synthetic data to build scoring models
- Dwell time isn’t considered
- Scaling

# Conclusions

- What have we learnt?
- Next steps?

# What have we learnt?

- Blue teams will continue to have a hard time
  - We can only engineer better systems if we truly understand what's wrong with those we already build
- Justifying change is about more than technical impact
  - FAIR is just a methodology, you need the maturity to apply it
- Don't stop testing and patching
  - But…
    - Consider both the cost and value of your efforts

# Next steps?

- Buy and read Security Engineering
- Read up on FAIR
- Come talk to us about making $$ with MITRE ☺

# How Cisco can help?

- Cisco Security SOC Advisory
  - Help with planning
- Cisco Security Incident Response Services (CSIRS)
  - Help with breaches (even on z/OS)
- Cisco Security Red Team
  - Benchmark your SOC and IR capabilities
- Cisco Security Architecture
  - Let us engineer your solutions
- Cisco Talos
  - The world's biggest private intelligence platform
- Cisco product...

# Links

- TM forum
  - https://www.tmforum.org/
- FAIR institute
  - https://www.fairinstitute.org/
    - https://www.fairinstitute.org/learn-fair
- ATT&CK
  - https://attack.mitre.org/groups/
- TBEST
  - https://www.ofcom.org.uk/__data/assets/pdf_file/0020/128810/Proposed-Annual-Plan-2019-20.pdf

# Questions?

twadhwab@cisco.com / @portcullislabs


CISCO

# Bonus material

# How might we tackle these?

# Asset management and change control*

* the right hand side isn't magic

- FAIR as a tool relies upon…
  - Effective asset management
  - Robust change control

# Understanding threat groups

- We can model ATT&CK's different threat groups
  - Allows us to distinguish between types of actor
  - Allows us to understand level of motivation when combined with naked hypotheses
    - e.g. state actors and financial services vs state actors and service providers

# Developing synthetic data to build scoring models

- We can leverage CVEs/CVSS data
  - Allows us to develop synthetic data

# Dwell time isn't considered

- I don't really have any answer to this
  - But…
    - Detective and reactive controls not factored into resistance metric
  - Consider that the average cost of breach is $500k over 6 months*
    - Might applying FAIR deter investment in SOC/telemetry?

* Cisco 2018 Annual Cybersecurity Report

# Scaling

- We can take CVE and CVSS data and construct the ultimate threat catalogue database by inference
  - Allows us to create a market for controls
    - It will be imperfect
  - It might be an interesting target for ML
    - Vulnerability <> control gaps
    - Development of ground truth