CSN19: SOC 2.0: Trends, Tips and Tricks

CUSTODIAN

network security

Dereck L. Haye|Co-Founder

ArcSight and HP Protect 2011

Agenda

- Why SOC2.0
- Typical SOC architectures
- Weaknesses of the SOC model
- Evolution to SOC2.0
- Typical SOC architectures
- How to balance SOC2.0
- ArcSight in the SOC2.0
- Training analysts
- Taking a SOC2.0 to maturity
- Initial results
- Threats we are detecting
- Where we go from here

Why SOC 2.0

- Lets look into what we are up against
- Scrape the internet for security buzzwords
- Then dump the results into some word clouds

Why SOC 2.0

CUSTODIAN

network security

What's really
going on in
your network?

CUSTODIAN

network security

What's really going on in your network?

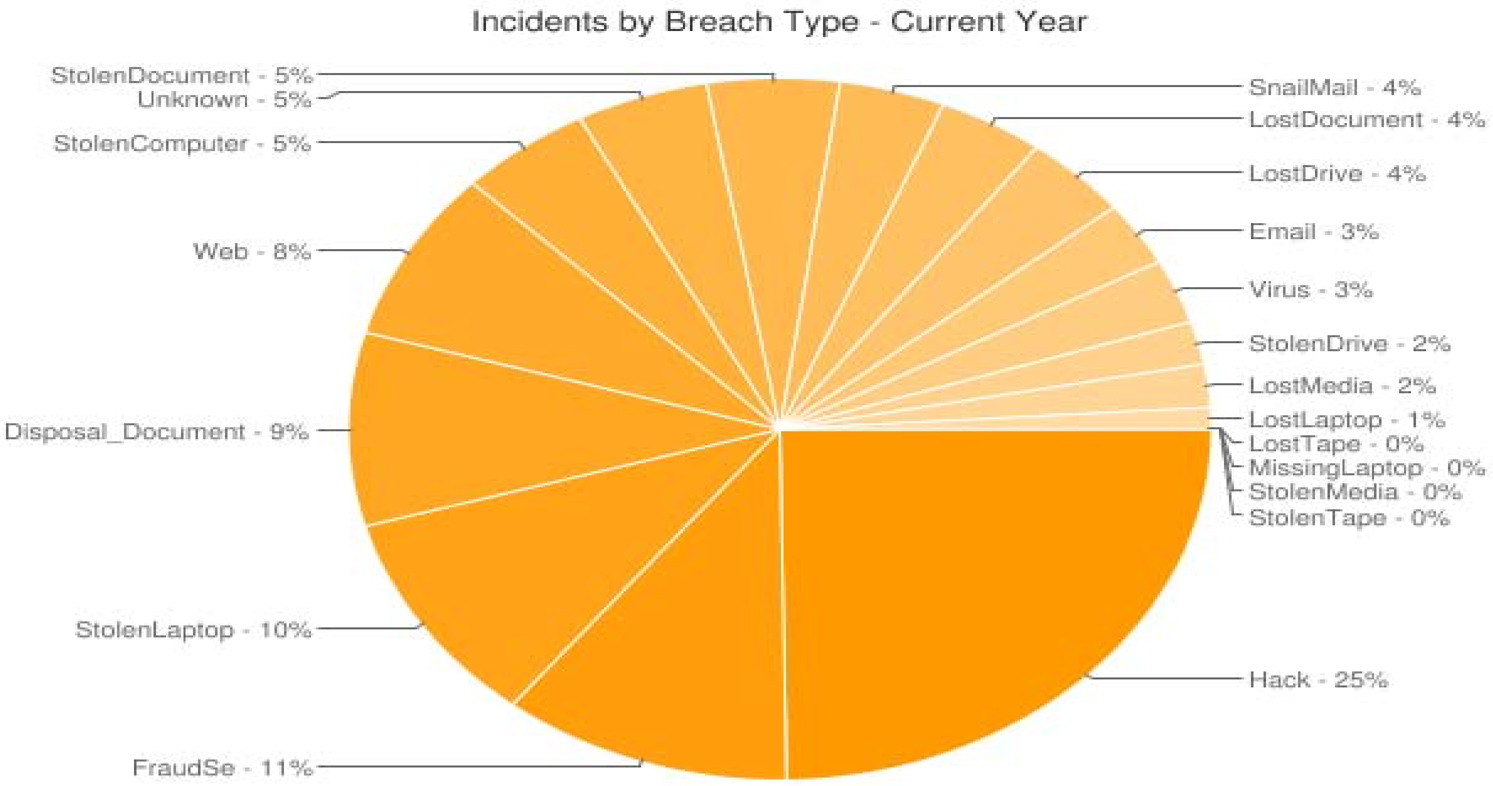
CUSTODIAN

network security

What's really
going on in
your network?

Why SOC 2.0

- Threats are evolving incredibly quickly and grow in sophistication

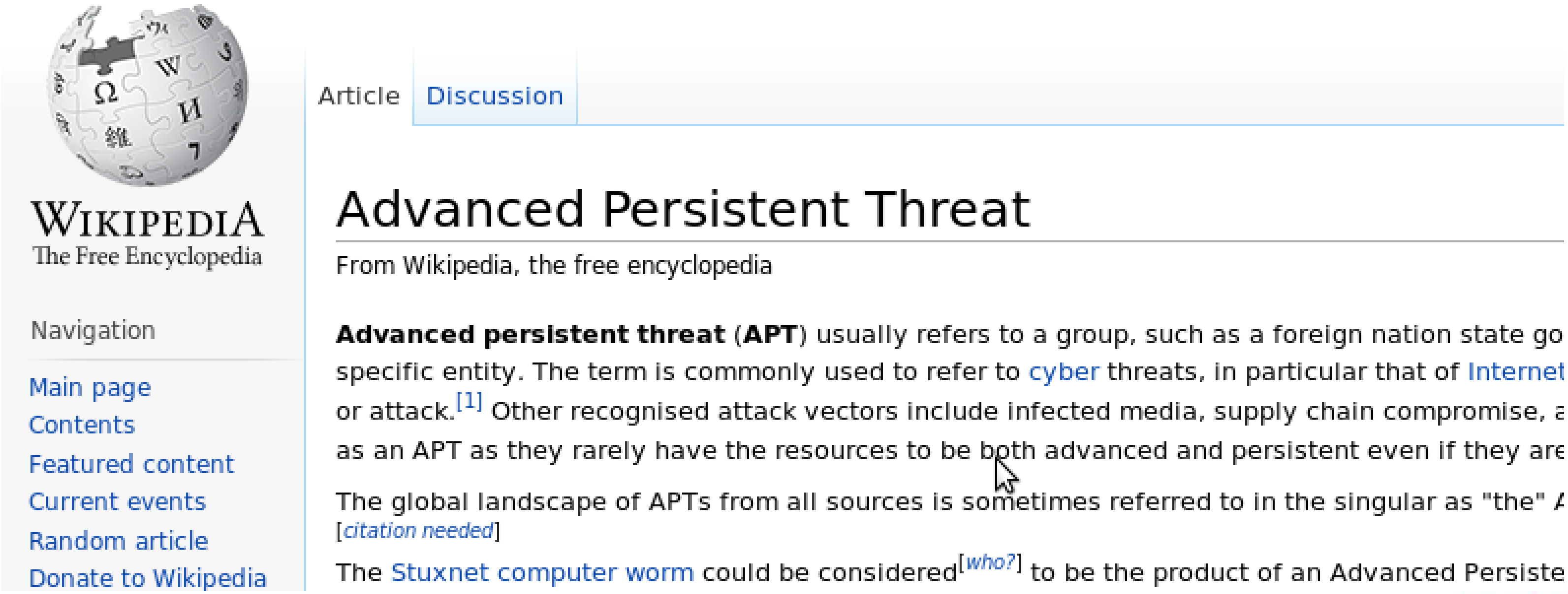


- For the security vendor its like trying to punch a cloud.
- Data source is data loss DB....

What's really going on in your network?

Why SOC 2.0

- Lately security companies targeted and breached
- Confidence in perimeter defence does not fall it plummets....
- Does the perimiter have a signature for the dreaded....



Advanced Persistent Threat

From Wikipedia, the free encyclopedia

Advanced persistent threat (**APT**) usually refers to a group, such as a foreign nation state go specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet or attack.[1] Other recognised attack vectors include infected media, supply chain compromise, a as an APT as they rarely have the resources to be both advanced and persistent even if they are

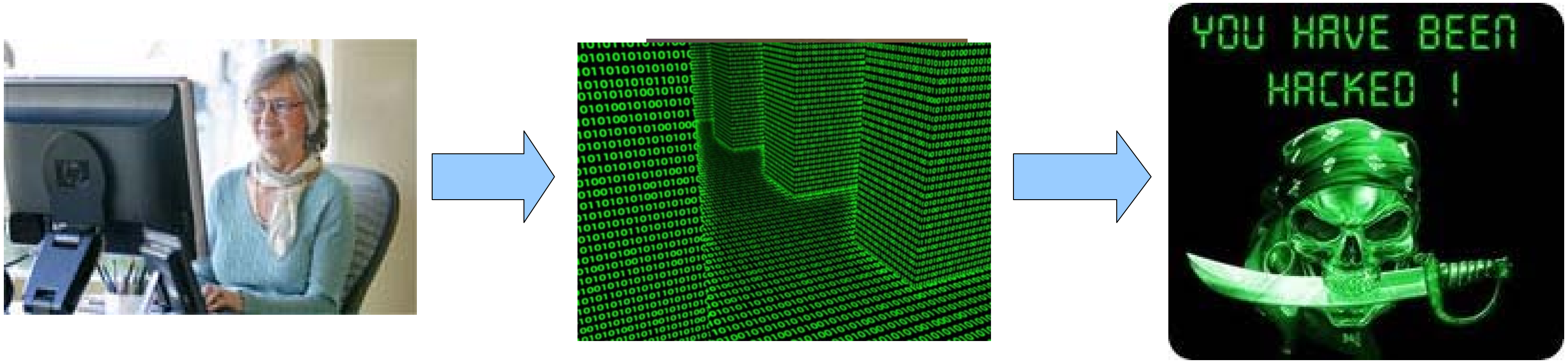
The global landscape of APTs from all sources is sometimes referred to in the singular as "the" A [*citation needed*]

The Stuxnet computer worm could be considered[*who?*] to be the product of an Advanced Persiste

What's really
going on in
your network?

Why SOC 2.0

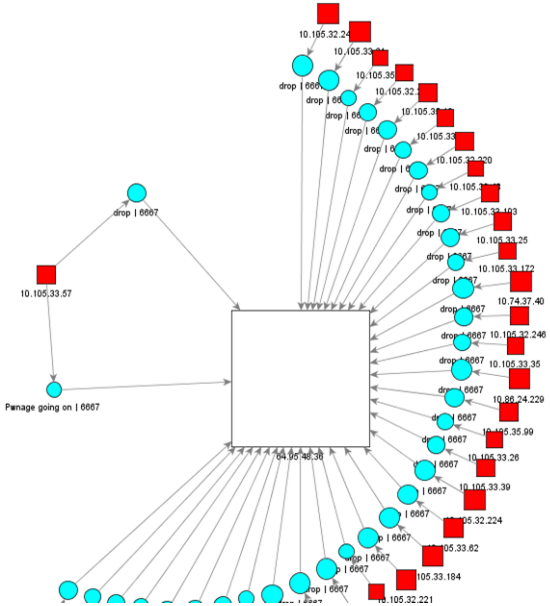
- Previous presentation evolution in malware detection
- How many data leaks have you detected at your company?
- What is a data leak anyway?

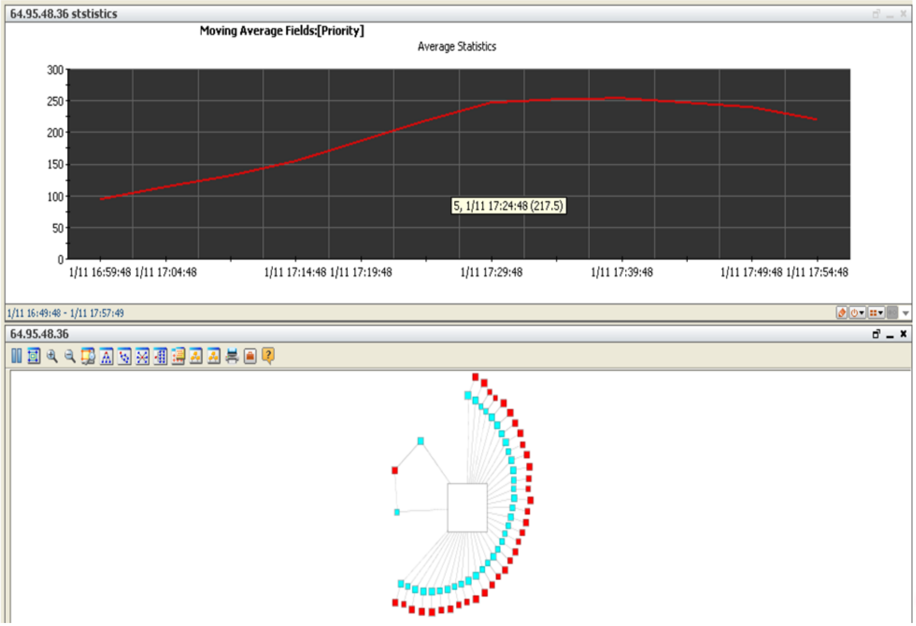


- Facts are: many breaches go unnoticed

Why SOC 2.0

- SIEMs like ArcSight allow an expansion in tactics
- Defensive focus can be rapidly re-deployed
- Having ArcSight makes migrating to SOC 2.0 quicker than you think





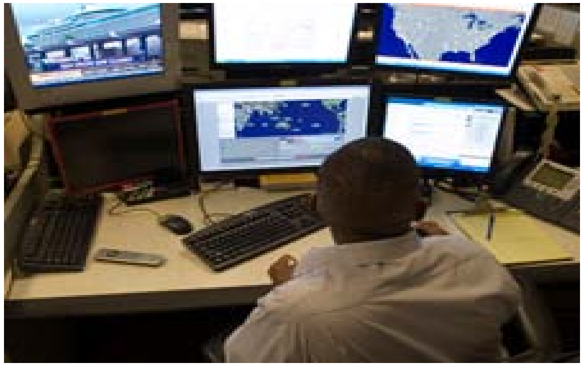
What's really going on in your network?

Typical SOC architectures

CUSTODIAN

network security

- People sitting in a 'goldfish bowl'
- Focus on managing devices
- Functions are quite static
- Technology segregates SOC
- Firewall-AV-IDS-SIEM group
- Inherently reactive
- Assumes devices prevent infections
- Output is limited

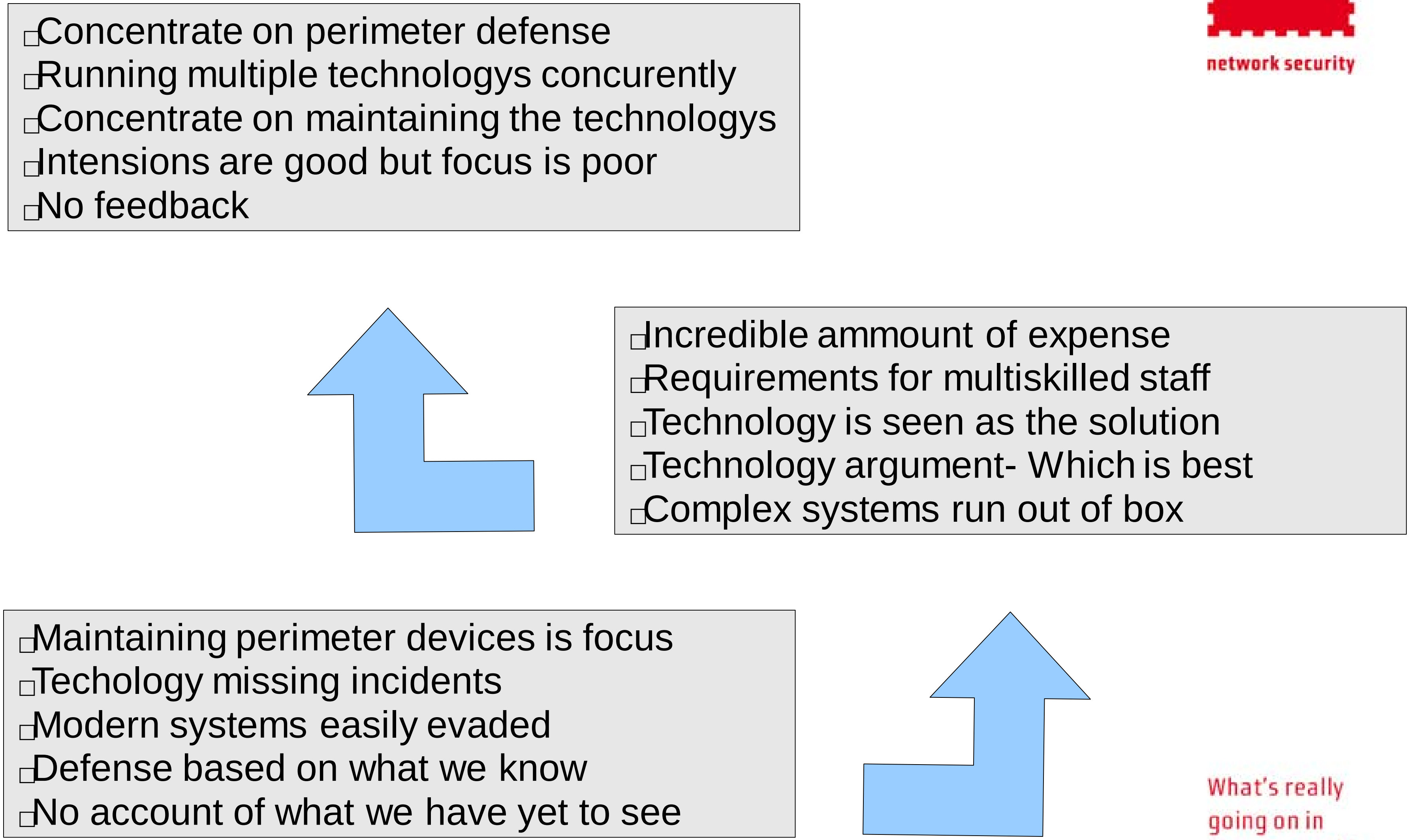


What's really going on in your network?

CUSTODIAN

network security

Weaknesses of SOC



- □Concentrate on perimeter defense
- □Running multiple technologys concurently
- □Concentrate on maintaining the technologys
- □Intensions are good but focus is poor
- □No feedback

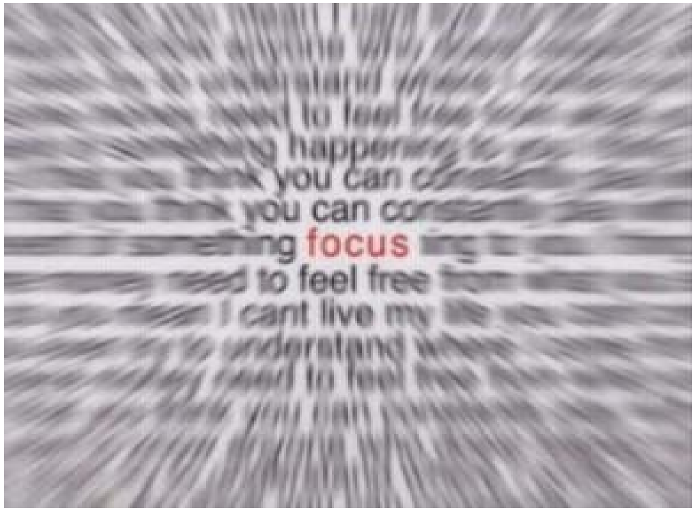
- □Incredible ammount of expense
- □Requirements for multiskilled staff
- □Technology is seen as the solution
- □Technology argument- Which is best
- □Complex systems run out of box

- □Maintaining perimeter devices is focus
- □Techology missing incidents
- □Modern systems easily evaded
- □Defense based on what we know
- □No account of what we have yet to see

What's really
going on in
your network?

Evolution to 2.0

It can be as simple as a little change in...

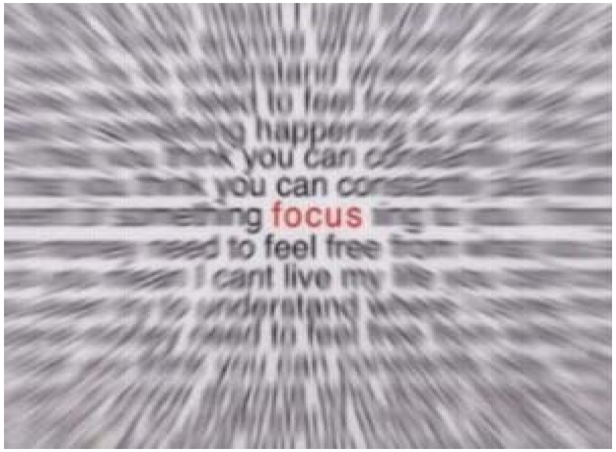


Lets face it, most ArcSight solutions sold

- Are used for log collection
- Run out of the box
- That’s great….
- But what on earth could be in those logs

Evolution to 2.0

- It’s not about the devices you have; it’s about data going through them
- Incidents balanced and information rich
- Investigation is proactive
- Instead of buying in blackists, create your own
- Intelligence is created for organisations
- Encourage diverse participation
- Analysts should spend the bulk of their time on analytics

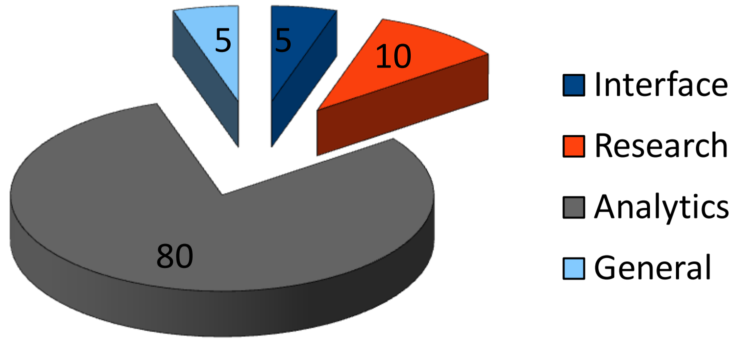


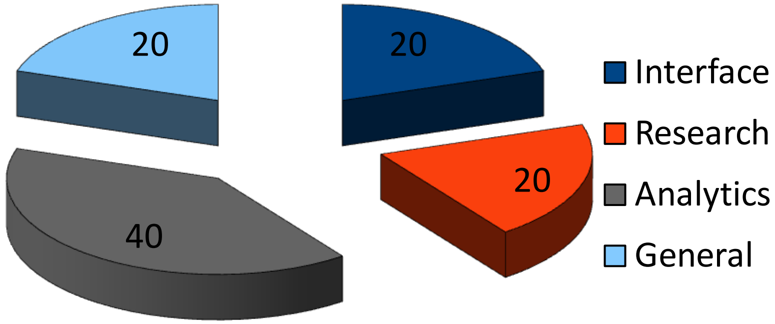
Achieve balance in SOC 2.0

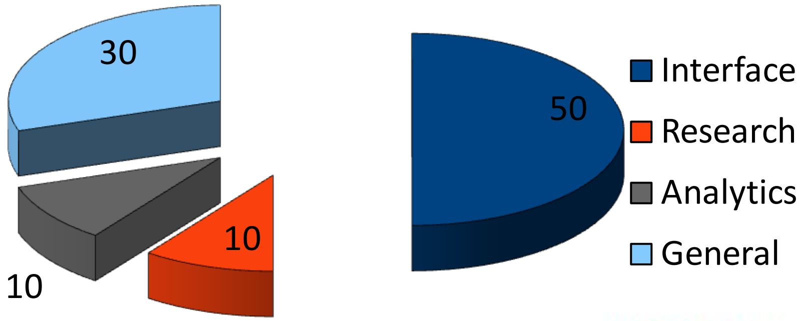
CUSTODIAN

network security

- Time investment is a challenge
- SOC must concentrate on analytics
- However other essential functions
- Balance is critical
- Otherwise SOC stagnates

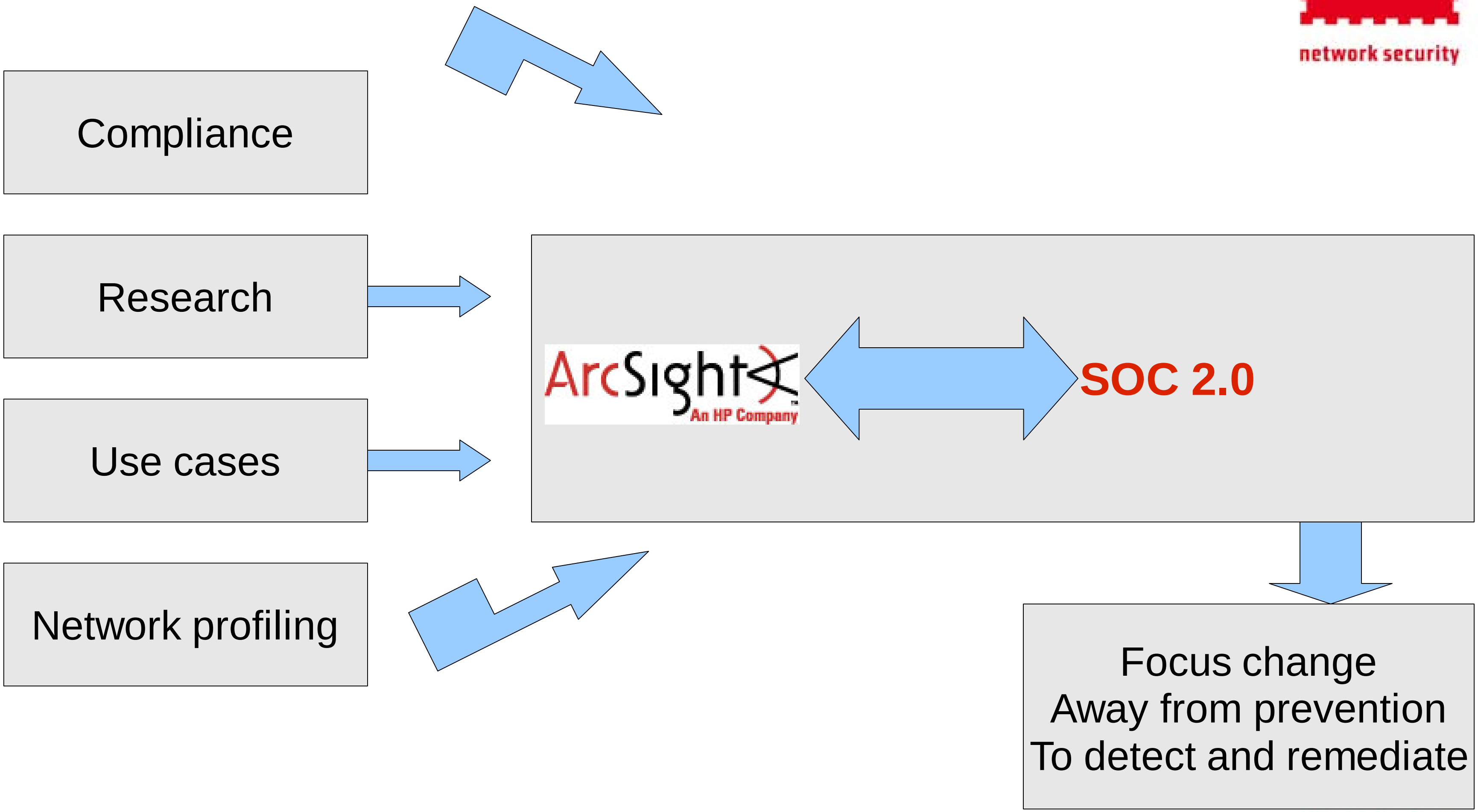






What's really going on in your network?

ArcSight’s role in SOC 2.0



Compliance

Research

Use cases

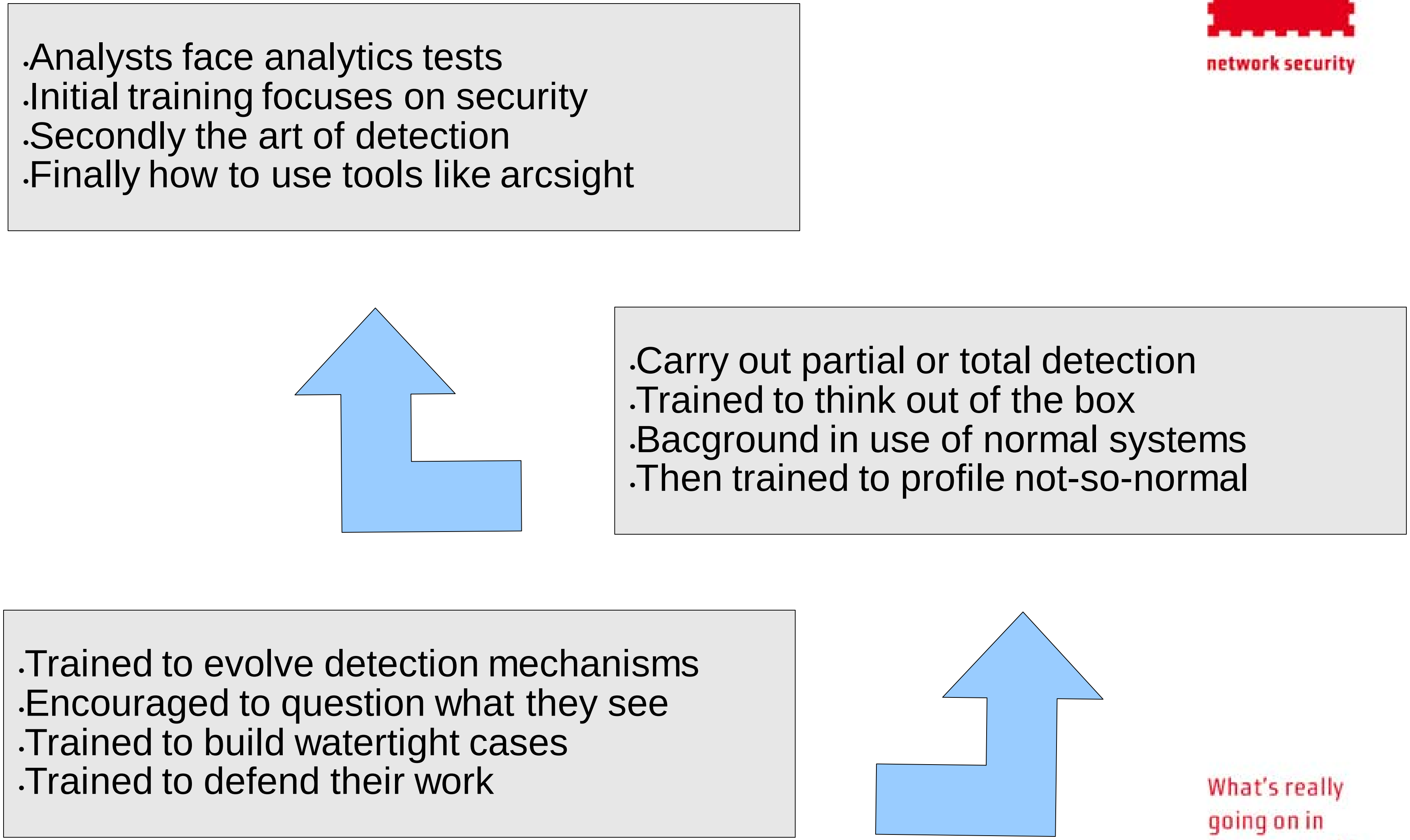
Network profiling

ArcSight
An HP Company

SOC 2.0

Focus change
Away from prevention
To detect and remediate

Training

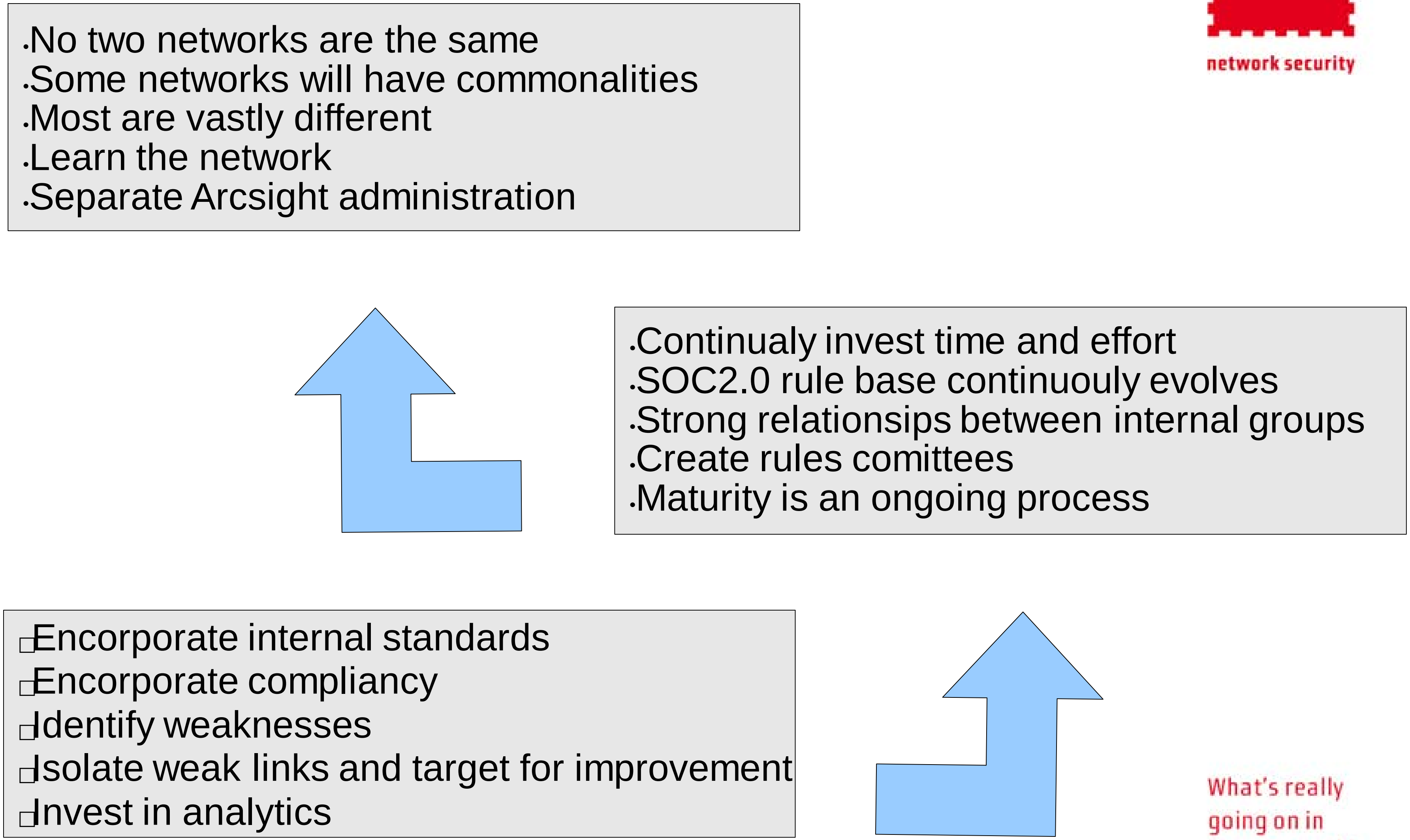


- Analysts face analytics tests
- Initial training focuses on security
- Secondly the art of detection
- Finally how to use tools like arcsight

- Carry out partial or total detection
- Trained to think out of the box
- Bacground in use of normal systems
- Then trained to profile not-so-normal

- Trained to evolve detection mechanisms
- Encouraged to question what they see
- Trained to build watertight cases
- Trained to defend their work

Leading SOC 2.0 to Maturity



- No two networks are the same
- Some networks will have commonalities
- Most are vastly different
- Learn the network
- Separate Arcsight administration

- Continualy invest time and effort
- SOC2.0 rule base continuouly evolves
- Strong relationsips between internal groups
- Create rules comittees
- Maturity is an ongoing process

- □Encorporate internal standards
- □Encorporate compliancy
- □Identify weaknesses
- □Isolate weak links and target for improvement
- □Invest in analytics

CUSTODIAN

network security

What's really going on in your network?

Initial results

- Tracking cookies
- The run AV guy
- Just to check we downloaded a new AV from the internet
- We could not find the machine in our network
- Why on earth would we investigate this?
- It’s just a couple of firewall drops and failed auth attempts
- Way to go you detected a Smartphone – it’s a false positive

What’s really
going on in
your network?

Initial results cont....

- Creating detailed incidents for SOCs
- MSSP - First ever true positive
- My first persistant Botnet infection
- Botnets themselves are getting smaller
- But……….there are more of them
- Mobile devices show a sharp increase in participation
- Building and establishing trust
- Being honest and defending our work

Threats we are detecting

- Hydra
- Detected via ‘anti pattern’ with statistics
- Initial interest through proxy systems
- 250 infections
- Detected 1 year ago
- Confirmed true positive after 3 months of internal investigation
- 250 infections with OVER 30 different binaries
- So far 30+ infections were mobile devices
- Some malicious binaries adapted local programs
- One of them was the Anti virus system itself
- Still alive

Where we go from here

- Current SOCs are looking through a very small piece of a very big window
- Many SOCs do not fully understand their own environment/networks
- Infection should be assumed
- Many SOCs have no feedback loops in place

Thank you

CUSTODIAN

network security

Find us at:

Whatisreallygoingoninyournetwork.com

Or

www.custodian.nl

Email:

info@custodian.nl

What's really
going on in
your network?