


killing the elephant in the room
enterprise vulnerability management tactics



RUXCON 2010 - Melbourne, Australia



overview

introduction

- vulnerability management presentations are rarely seen at technical conferences
- with the hype of zero-day vulnerabilities and attacks, many neglect fundamental practices
- enterprises have large IT estates ripe with technicalities, constraints, and politics
- vendor solutions often try to pitch themselves as comprehensive solutions for large complicated spaces
- the goal of this presentation is to analyze the primary building blocks of vulnerability management
- a practical overview of architecting and implementing customized security technologies

threats

- vulnerability classes, exploits, and mitigating controls have been evolving for well over a decade
- offensive and defensive tactics have gone through several waves of maturity
- cyber-espionage strategies and tactics evolve and adapt to many different factors
- organizations with significant value and/or intellectual property are in the spotlight
- vulnerabilities can effect every component, layer, and node of a networked environment
- most large networks would struggle to manage known vulnerabilities, let alone sophisticated threats

challenges

- estates can grow exponentially (e.g. acquisitions) that can increase volume and add technicalities
- layers of bureaucracy and political hurdles
- opportunistic attackers versus a financial crisis
- technology scalability, scope, and coverage issues
- VM is essentially a large-scale coordinated process, thus understanding all perspectives is important
- selling security strategies to senior management and shifting mindsets from regulatory to security

common pitfalls

- focusing on technologies whilst neglecting processes
- not understanding weaknesses of vendor technologies
- not understanding the current IT landscape
- deploying solutions in silos with poor architecture
- insufficient business context of vulnerability risks
- lack of awareness and resource prioritization
- responsive funding instead of preemptive strategies
- inadequate skills/training for security personnel

tactics

- establish a detailed and up-to-date inventory of publicized vulnerability threats
- build a customized asset inventory unique to the environment with business context
- support multiple tracking mechanisms to improve turn-around times and coverage
- add environmental context to threats and support intelligently prioritizing assets
- identify process flaws and enhance the workflow to be more efficient and effective
- enrich security personnel with vulnerability intel

agenda

part 1: custom technology



part 2: supporting components



part 3: conclusion



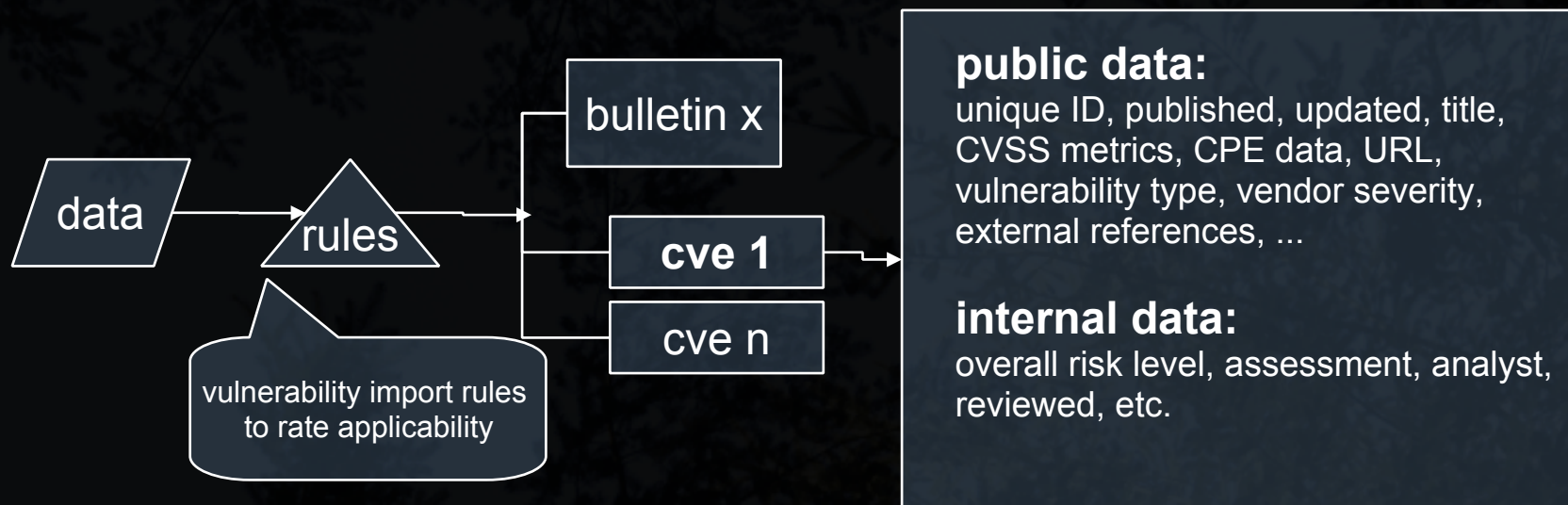
custom technology



inventory (1/3)

vulnerability data

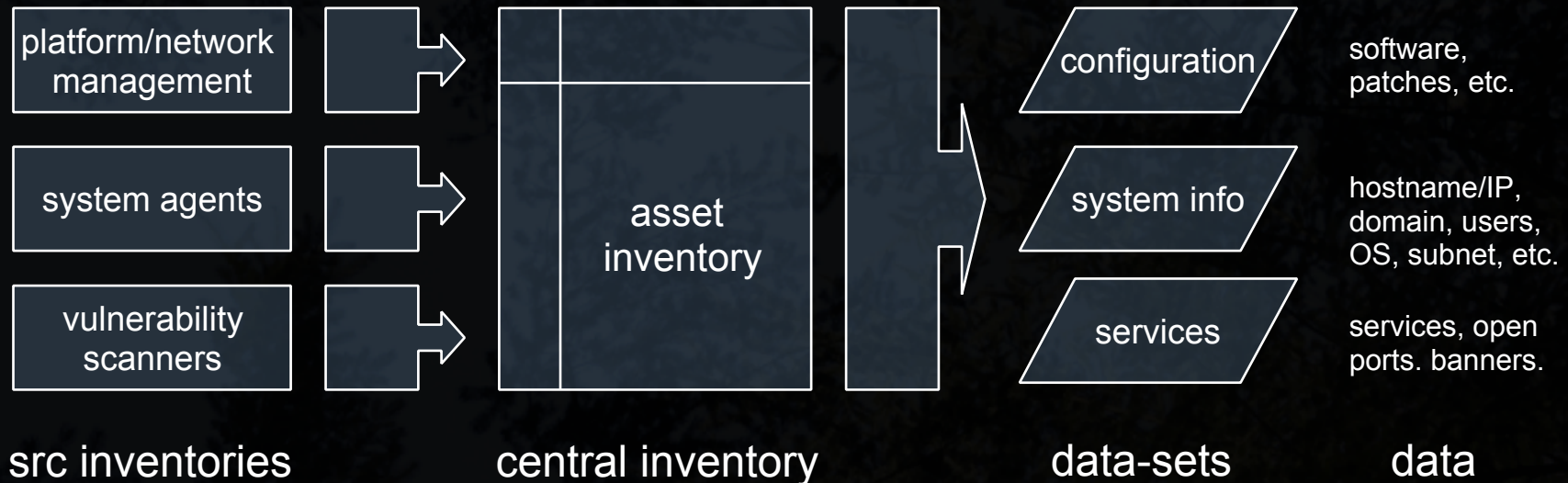
- vulnerability feeds can be synched from different places, such as NVD + vendors or commercial feeds
- cross-referencing vulnerability data via internal rule-sets can rate how susceptible each item



inventory (2/3)

asset data

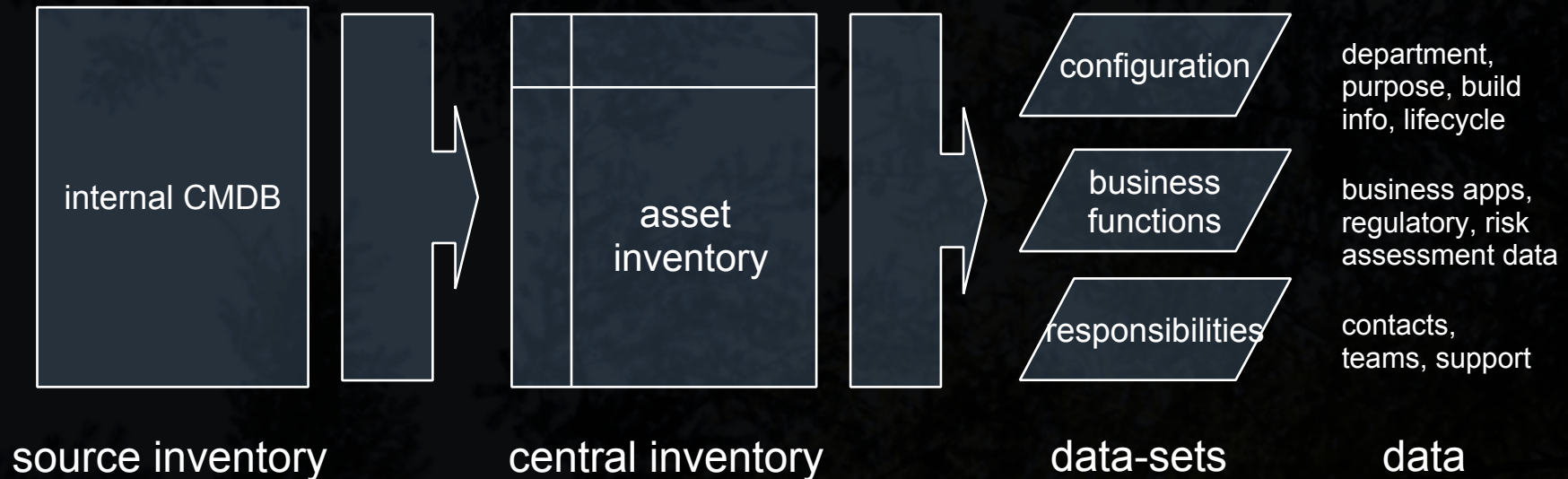
- collating assets to a centralized inventory can be a surprisingly time-consuming task
- requires a detailed understand of the IT estate - platform, software, device, and network inventories
- brings an in-depth insight into coverage and scope of all relevant source inventories



inventory (3/3)

business data

- nodes don't exist to be owned, they serve a purpose
- extending the asset inventory to introduce business context is when the game starts to change
- should involve the business in mapping out and translating the vital pieces and their meaning



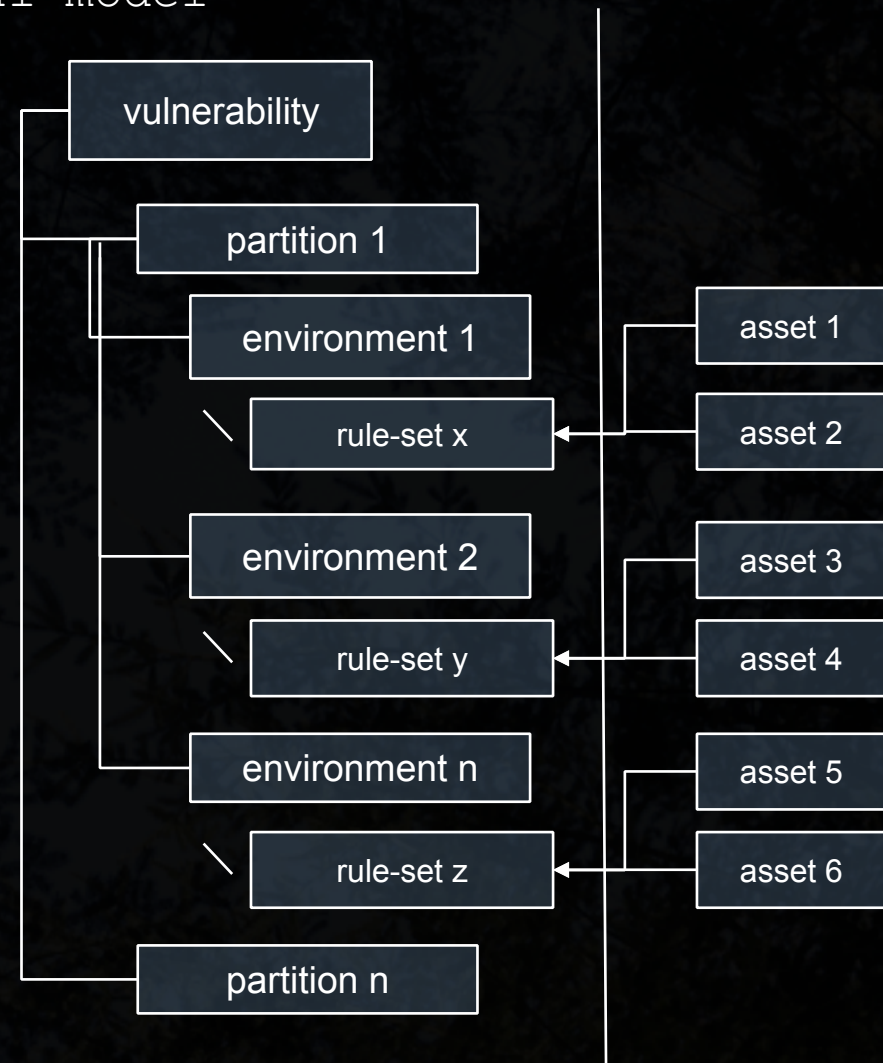
tracking

- host discovery and agent-less vulnerability checks is a core part of most COTS products
- scanning huge networks can have negatives – turnaround times, corporate processes, etc.
- but, do you really need to scan every node?
- a strong inventory can fill certain use-cases
- what about system agents/platform management?
- consider hybrid mechanisms for more critical issues requiring timely assessment and planning
- understanding coverage between source inventories allows for strategic identification

context (1/2)

hierarchal model

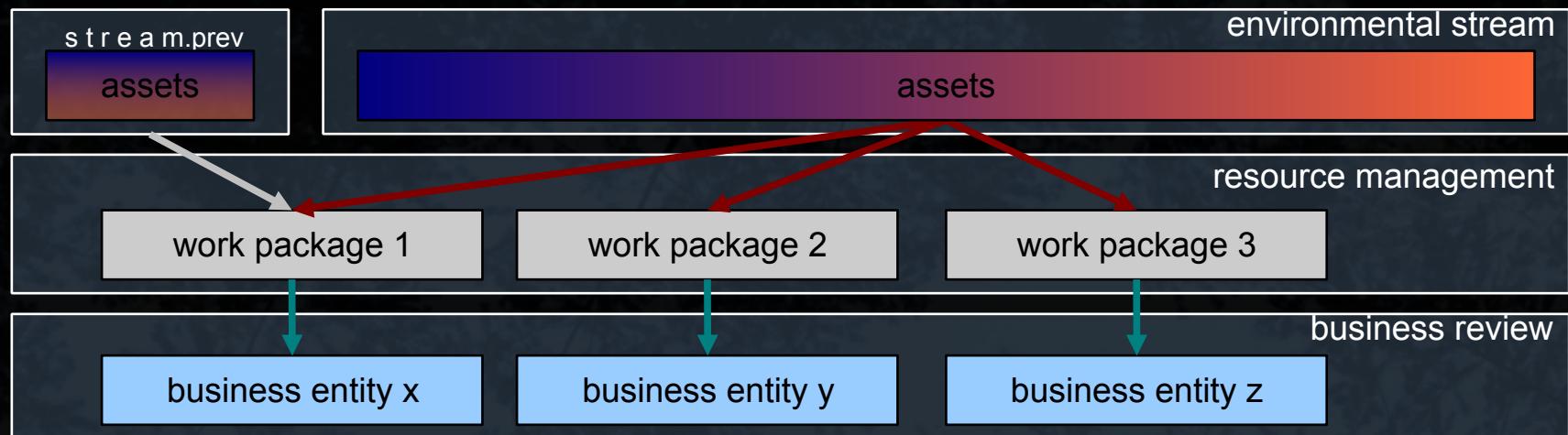
- a flat list of affected assets isn't always practical or scalable
- partitioning assets breaks them into containers and can be business aligned (e. g. Medical, Finance)
- each partition can in-turn be broken into manageable environmental streams
- a simple rule-based classifier can map assets to partitions and streams
- such a hierarchy can satisfy many use-cases



contextual data-model & asset classification

context (2/2)

environmental focus

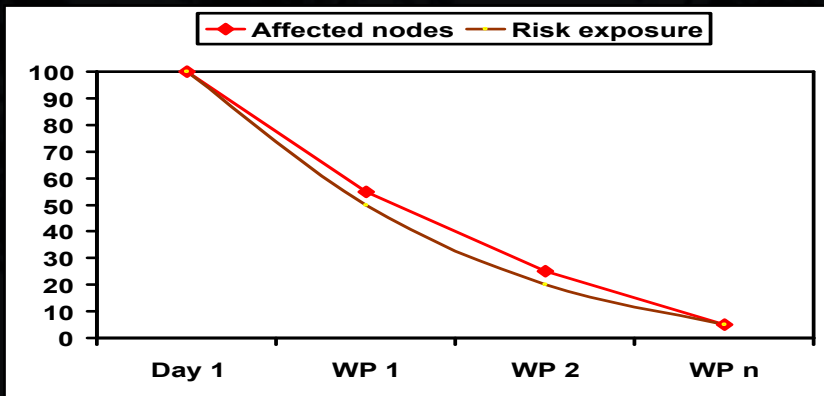


- each stream changes the focus of the vulnerability to an environmental level
- the responsible personnel can allocate work packages and bundle multiple environmental streams together
- affected business entities can then have transparency of vulnerabilities, impacts, etc.

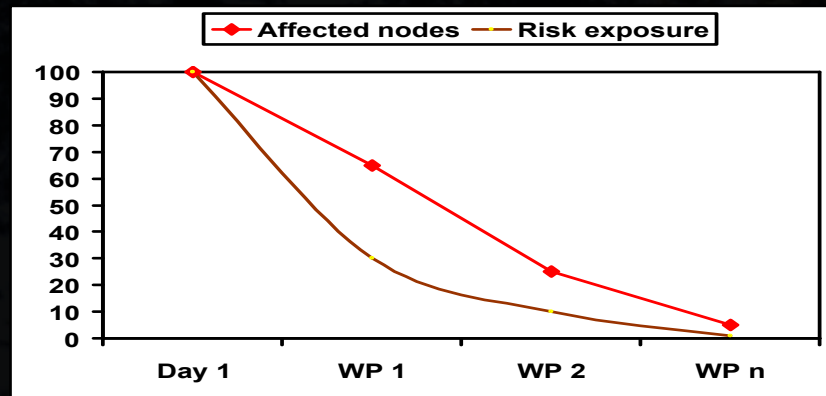
awareness (1/3)

prioritisation model

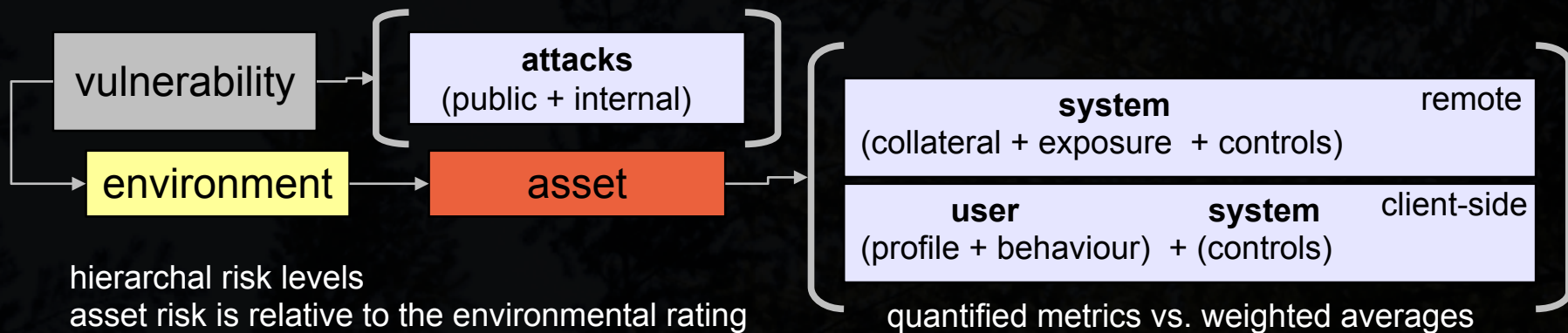
- without awareness, statistics are against large IT estates
- making each iteration more effective brings focus to resources and controls the outstanding exposure



exposure timeline (no awareness)

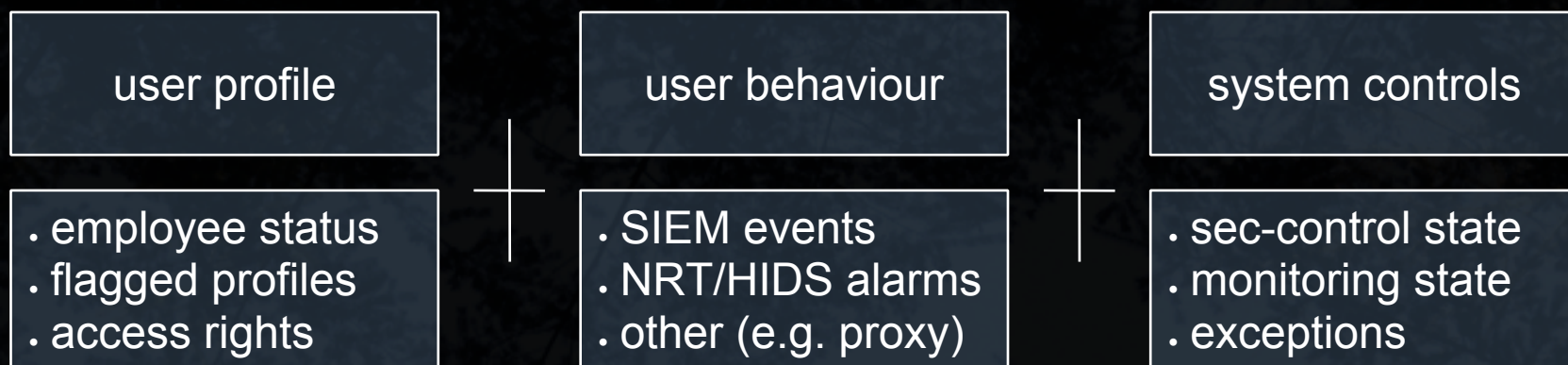


exposure timeline (with awareness)



awareness (2/3)

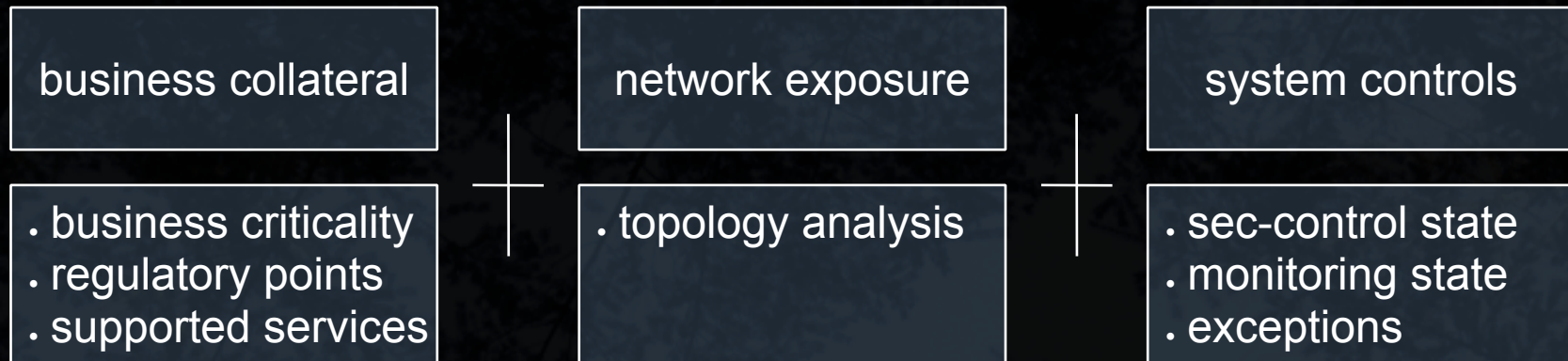
client-side prioritisation



- . user end-points have a high distribution percentage
- . understanding the end-user is important – their job profile, behavior, access rights, trends, etc.
- . the systems security controls are equally important
- . quantifiable metrics can be sourced already in most IT estates – end-point security, security monitoring, identity management, HR, the list goes on...

awareness (3/3)

remote prioritisation



- remote vulnerabilities can result in worms or used for tactical propagation, in general apply to network services
- the business collateral can be quantified via internally agreed rules (likely to be unique to each organization)
- network topology analysis engines can help determine attack paths and impacts of firewall rule-sets
- system/network controls influence the overall risk rating

supporting components



workflow

- a centralized VM workflow tool brings transparency of issues to stake-holders
- rule-based access control and contextual views help show users relevant data for their role
- KPI's for each phase helps identify bottle-necks
- better prioritization leads to tighter SLT's
- understand real-world scenarios that create delays (“too critical to patch”, shared infra, etc.)
- understand how management can help expedite issues
- investigate feasibility of integrating with patch management suites (good luck)

intel

*“In short, the heap is such a fascinatingly rich and intricate system that even the bleakest, most-constrained memory corruption vulnerabilities **may eventually prove to be reliably exploitable** by an attacker with **sufficient resources**.”* – John McDonald

- vulnerability research is a specialized industry
- historically, disclosed vulnerability details have been woeful (“a bad guy can... get on in there!”)
- exploits are threats, vulnerabilities are risks
- vendors are becoming more transparent and supporting (Microsoft EI rating, bug bounties, etc.)
- it's hard for large enterprises to get specialists
- an informed/unbiased 2nd opinion may save time/money

conclusion



remarks

- vulnerability maintainers have a challenging time to keep data up-to-date and comprehensive
- issues with inconsistent conventions, data-quality, scope/coverage, etc. were evident during development
- is there communication between VM practitioners?
- the evolution of centralized platform management has an opportunity to drastically change this space
- certain components discussed today would be difficult to abstract into a versatile solution
- in general, security technologies don't seem to have well laid-out API's to aid custom integration
- do any itsec people understand patch management?

epilog

- this presentation has attempted to give a realist overview on vulnerability management
- the custom technology can also be adapted to support adjacent areas (configuration flaws, etc.)
- a big piece of the challenge (the boring piece) relates to the process and resource constraints
- big organizations need to think through problems instead of throwing money blindly at technologies
- solutions can be a hybrid of build vs. buy
- it would seem as if there's a lot of room for development in standards, data quality, and products

thanks for listening!

matt volvent org

kudos to Ruxcon for organizing such a brilliant event.