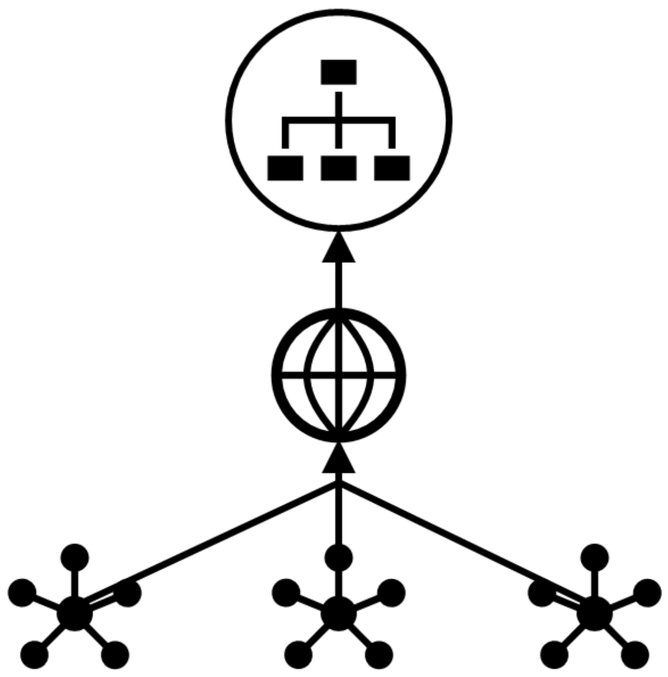
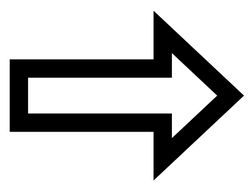
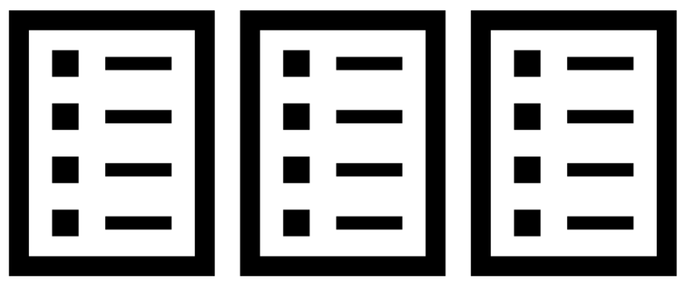
South African National Research Network

CSIRT Vulnerability Scanning Service

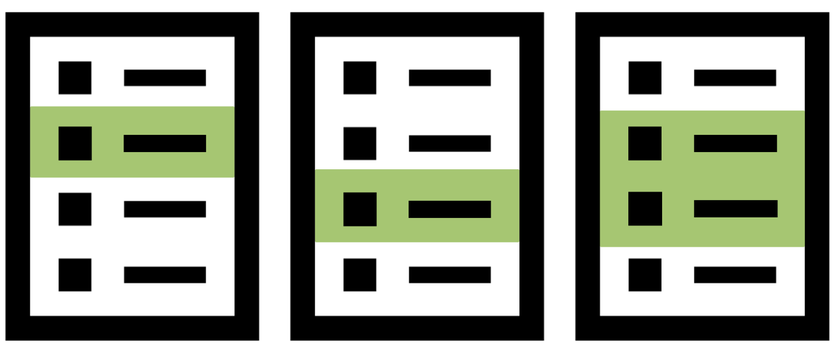
"ScanMan": Data aggregation and reporting







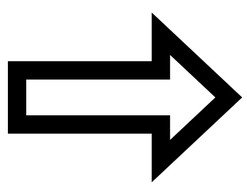
An effective external vulnerability assessment requires the use of multiple vulnerability scanners, each using it's own reporting format



Results from vulnerability scanners that address the same vulnerability type are aggregated into report items

Host 1

Report Item	Max CVSS	Confirmed
Report Code 1	9.8	✓
Report Code 2	7.3	✗
Report Code 3	7.3	?
⋮	⋮	⋮
Report Code N	2.0	✓
Host Max CVSS	9.8	

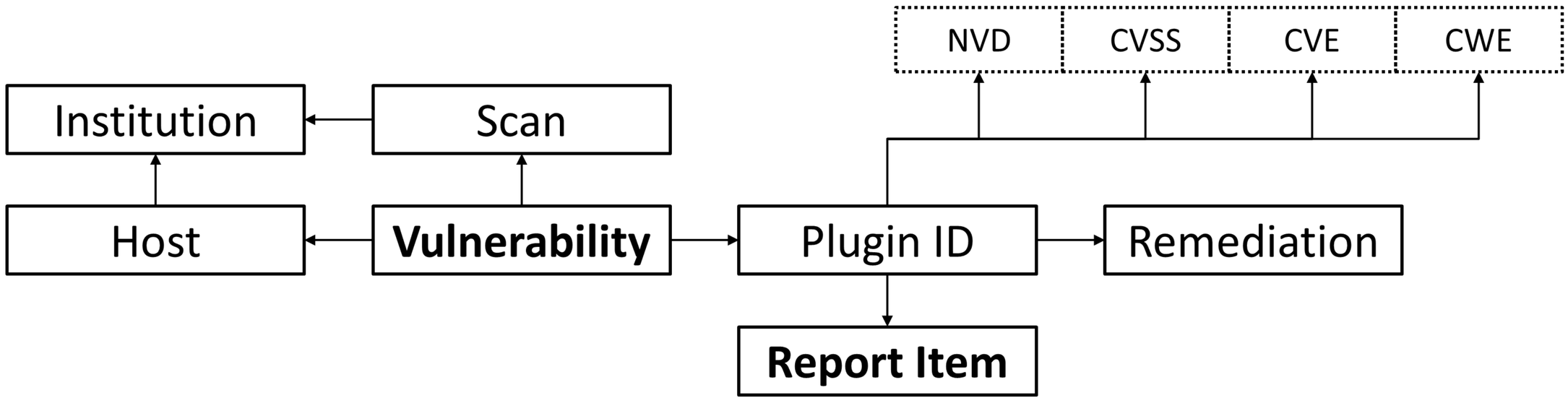


Institution 1 - Scan X

	Max CVSS	Critical	High	Medium
Host 1	9.8	8	2	20
Host 2	9.3	12	8	11
Host 3	7.1	0	1	13
⋮	⋮	⋮	⋮	⋮
Host N	4.3	0	0	9

Report items are verified per host to determine the host vulnerability

Per institution, the host results are aggregated into a holistic report



Enabling accurate reporting required a data model that can accommodate the results from any vulnerability assessment tool

The current data model focuses on a minimalistic approach to data aggregation, based on the remediation action that is required

Reporting on remediation actions ensure that system owners are presented only with the information required to mitigate vulnerabilities

Talk to me about "ScanMan" today! schalk@sanren.ac.za

science & technology
Department:
Science and Technology
REPUBLIC OF SOUTH AFRICA

Schalk Peach
CSIRT Analyst, SANReN
schalk@sanren.ac.za
csirt@sanren.ac.za

CSIR
our future through science