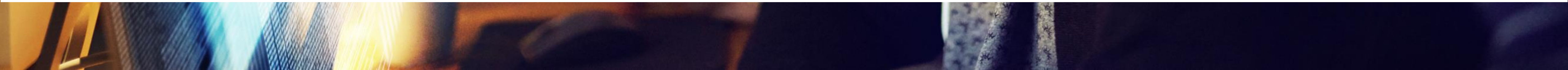
Vulnerability management consultancy

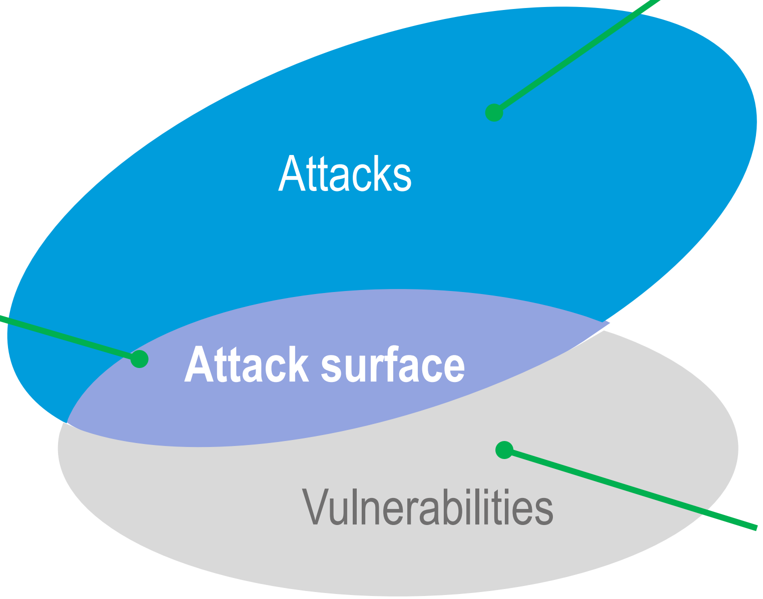
From Computacenter

Computacenter



Vulnerability management

The objective of vulnerability management



The objective of Vulnerability Management is to reduce the attack surface

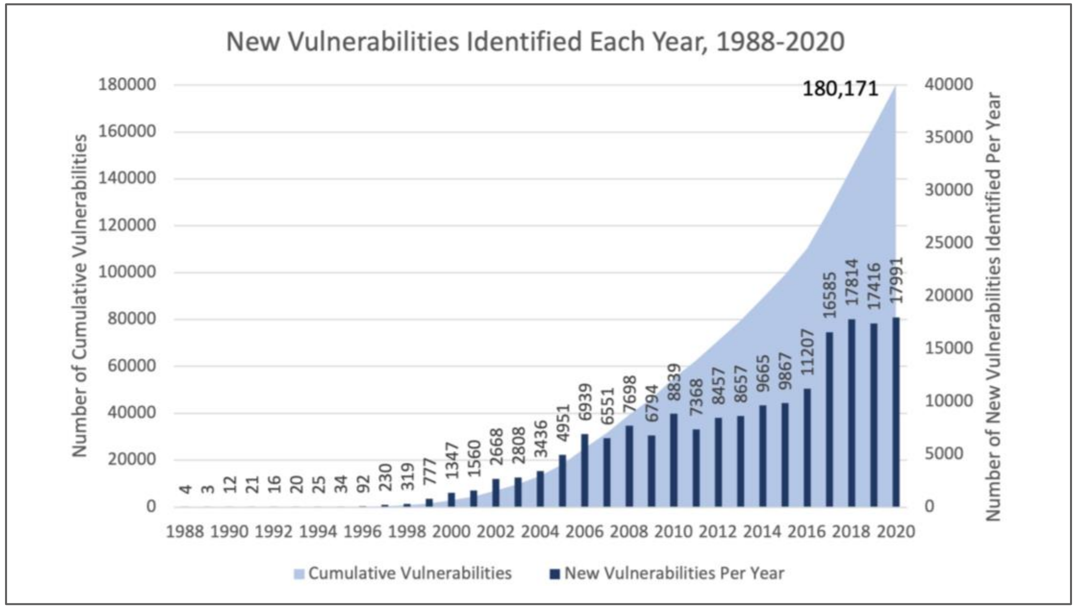
Attackers can exploit certain Vulnerabilities

There are many vulnerabilities that are easy to identify with scanners – not all of them are critical!

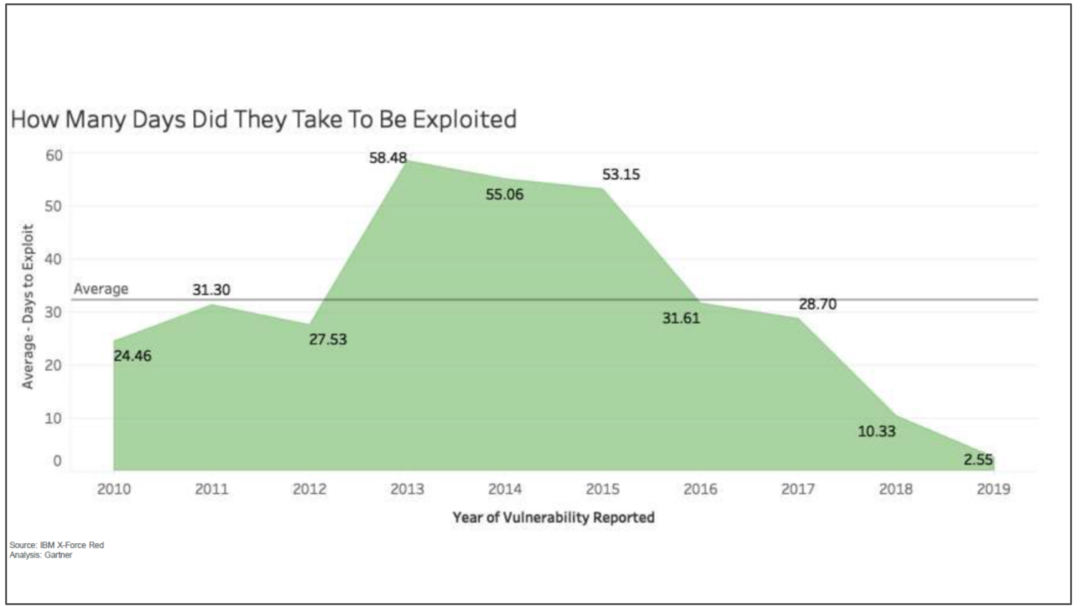
Vulnerability management

20,000 New vulnerabilities are discovered each year…

Number of new vulnerabilities


New Vulnerabilities Identified Each Year, 1988-2020

Time to exploit


How Many Days Did They Take To Be Exploited

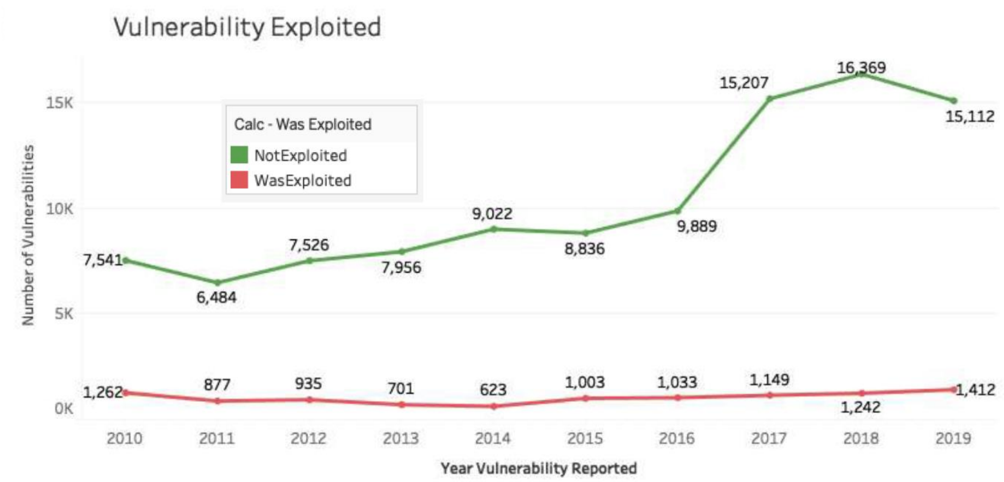
Source: IBM X-Force Red
Analysis: Gartner

…and attackers only need a few days to exploit them.

Vulnerability management

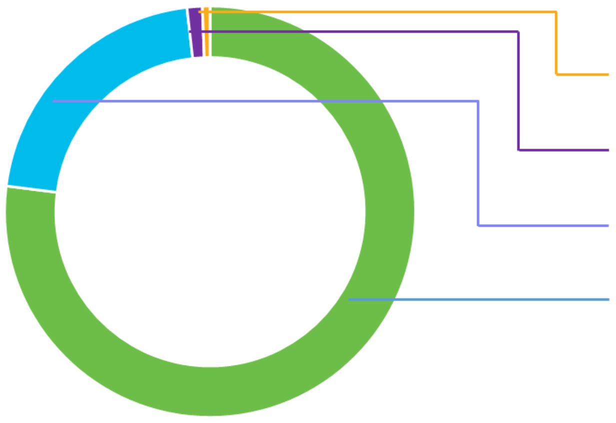
But not all vulnerabilities are critical

The number of exploited vulnerabilities is low



Source: IBM X-Force Red
Analysis: Gartner

The number of critical vulnerabilities is even lower



0.6% of CVE's just have executed exploits in the wild

1.2% of CVE's have published and observed exploits

21.2% of CVE's just have an exploit publicly released

77% of CVE's have no published or observed exploit

Source: Cisco / Kenna

Vulnerability management

The challenge

One scan can result in 100,000's of vulnerability events

System owners are not always easy to identify

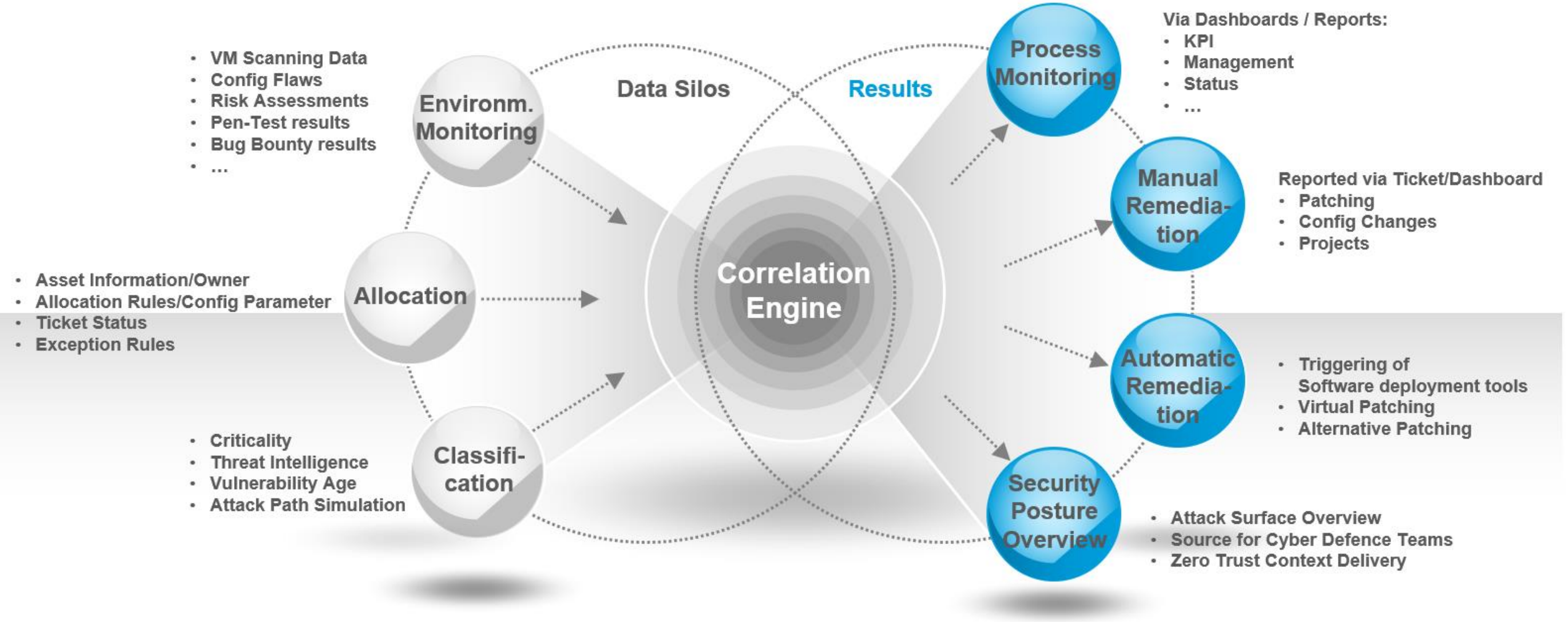
IT Operations have SLA driven goals that are incompatible with vulnerability resolution

There is an operational gap between the scan and the application of the patch

Vulnerability management

The answer?

Automated Vulnerability correlation engine



- VM Scanning Data
- Config Flaws
- Risk Assessments
- Pen-Test results
- Bug Bounty results
- …

Environm. Monitoring

- Asset Information/Owner
- Allocation Rules/Config Parameter
- Ticket Status
- Exception Rules

Allocation

- Criticality
- Threat Intelligence
- Vulnerability Age
- Attack Path Simulation

Classifi-cation

Data Silos

Correlation Engine

Results

Process Monitoring

Via Dashboards / Reports:
- KPI
- Management
- Status
- …

Manual Remedia-tion

Reported via Ticket/Dashboard
- Patching
- Config Changes
- Projects

Automatic Remedia-tion

- Triggering of Software deployment tools
- Virtual Patching
- Alternative Patching

Security Posture Overview

- Attack Surface Overview
- Source for Cyber Defence Teams
- Zero Trust Context Delivery

Vulnerability management

Computacenter service offerings

EVALUATION

- Delivered by expert professional service teams
- Assess current processes, deployed technology and risks
- Provide a detailed recommendation and overview of how correlation engine would support

IMPLEMENTATION

- Design and deployment of correlation engine technologies and process
- Integration of core systems (CMDB, ticketing etc) to enable automation
- Programming of interfaces & middleware

OPERATION

- Operational support (tracking, queries, report generation)
- Available using on prem engineering resources or   nearshore / offshore remote support

Qualys.

tenable

TANIUM

servicenow

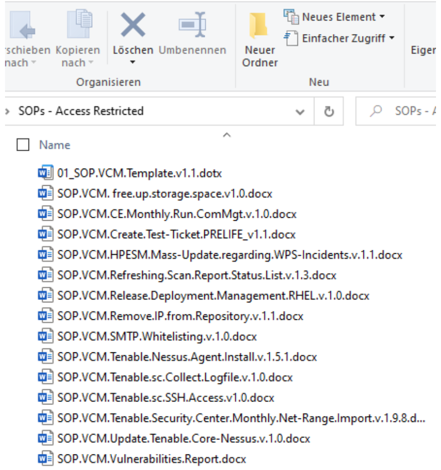
splunk>

Supported by our Vulnerability management toolbox

Pre-defined process standards

- Generic process blueprints
- Pen testing processes
- VM for Infrastructure
- VM for Applications
- Industrial Cyber Security

Pre-defined operating concepts



```
01_SOP.VCM.Template.v1.1.dotx
SOP.VCM. free.up.storage.space.v1.0.docx
SOP.VCM.CE.Monthly.Run.ComMgt.v.1.0.docx
SOP.VCM.Create.Test-Ticket.PRELIFE_v1.1.docx
SOP.VCM.HPESM.Mass-Update.regarding.WPS-Incidents.v.1.1.docx
SOP.VCM.Refreshing.Scan.Report.Status.List.v.1.3.docx
SOP.VCM.Release.Deployment.Management.RHEL.v.1.0.docx
SOP.VCM.Remove.IP.from.Repository.v.1.1.docx
SOP.VCM.SMTP.Whitelisting.v.1.0.docx
SOP.VCM.Tenable.Nessus.Agent.Install.v.1.5.1.docx
SOP.VCM.Tenable.sc.Collect.Logfile.v.1.0.docx
SOP.VCM.Tenable.sc.SSH.Access.v1.0.docx
SOP.VCM.Tenable.Security.Center.Monthly.Net-Range.Import.v.1.9.8.d...
SOP.VCM.Update.Tenable.Core-Nessus.v.1.0.docx
SOP.VCM.Vulnerabilities.Report.docx
```

Standardised implementation steps

Phase 1 - Basic installation (server and clients)

Phase 2 - Integrate production

Phase 3 - Integrate network devices & databases

Phase 4 - Integrate perimeter scans

Phase 5 - Integrate cloud scans

Phase 6 - Integrate mobile device

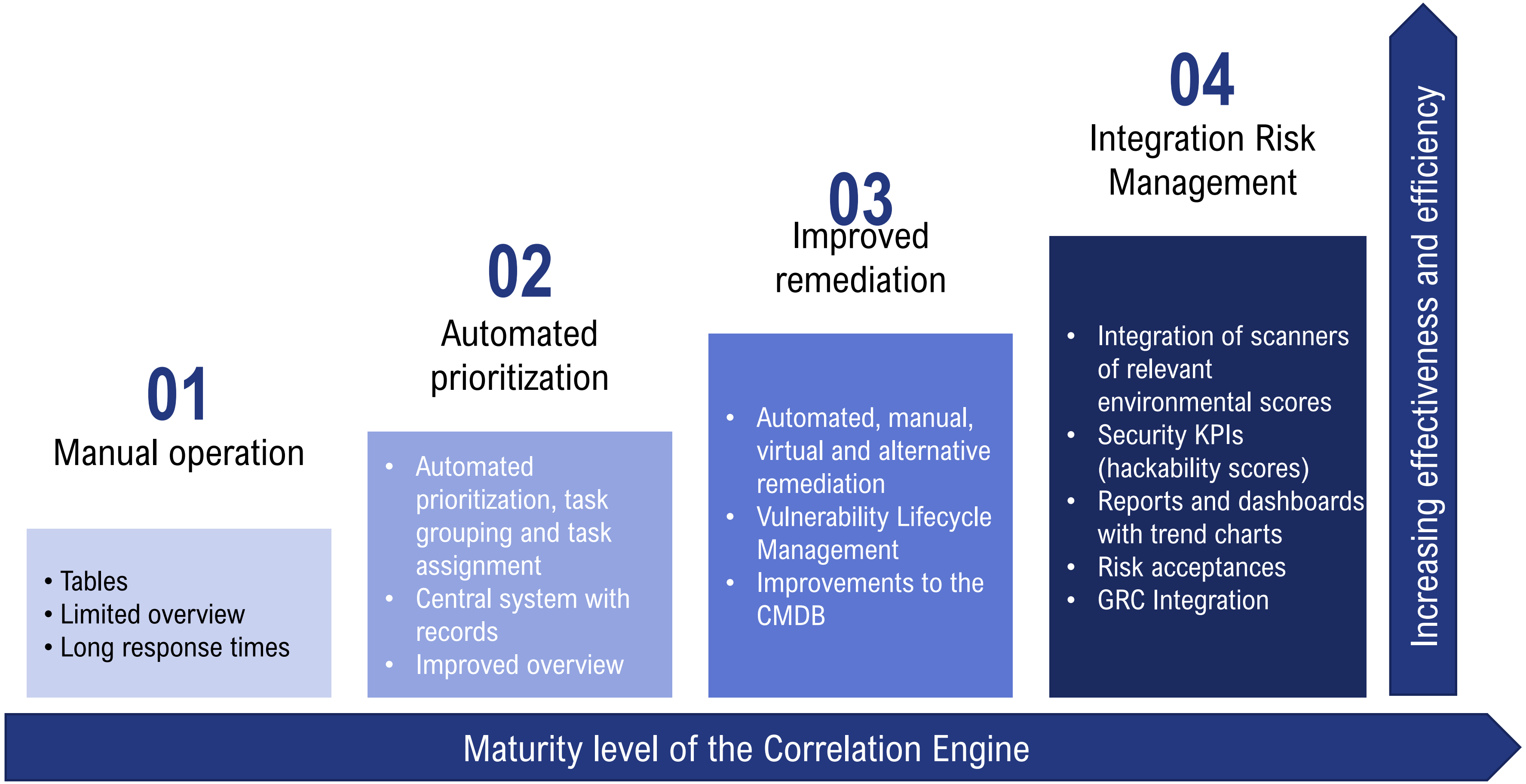
Phase 7 - Integrate compliance scans

Phase 8 - Integrate pen test

Phase 9 - Optimisation of remediation

Vulnerability management maturity levels

Roadmap



01
Manual operation

- Tables
- Limited overview
- Long response times

02
Automated prioritization

- Automated prioritization, task grouping and task assignment
- Central system with records
- Improved overview

03
Improved remediation

- Automated, manual, virtual and alternative remediation
- Vulnerability Lifecycle Management
- Improvements to the CMDB

04
Integration Risk Management

- Integration of scanners of relevant environmental scores
- Security KPIs (hackability scores)
- Reports and dashboards with trend charts
- Risk acceptances
- GRC Integration

Increasing effectiveness and efficiency

Maturity level of the Correlation Engine

Benefits

Operational efficiency

- **Improved insight** – Assessment of multiple data sources to uncover detailed vulnerability data and business impact
- **Enhanced assignment** – more clarity around vulnerability ownership, and remediation priority
- **Asset Management** – Helps to discover unknown assets and can improve asset managment process

Enhanced remediation options

- **Virtual Patching** - Reduction of the attack surface through IPS signatures - integration with endpoint protection
- **Alternative patching** - Reduction of the attack surface through firewall rules and ACLs
- **Automated remediation** - Implementation of automated measures, configuration changes/restores

Enhanced compliance

- **Risk visibility** – Detailed reporting showcasing current vulnerability status and risk position to CISO
- **Compliance** – Regularory and compliance requirements easier to evidence and report
- **NIS2 regulation** – Addresses the NIS2 VM requirements that is applicable to all of Europe and some UK organisations.

Supports core zero-trust building blocks

- **Policy Decision Points** – Correlation engine provides critical risk and vulnerability context to inform access assessment decisions
- **Microsegmentation** - Microsegmentation integrated with vulnerability management platforms can visualize application workloads & their associated software vulnerabilities through a vulnerability map.

Thank you

© Computacenter 2024

Computacenter