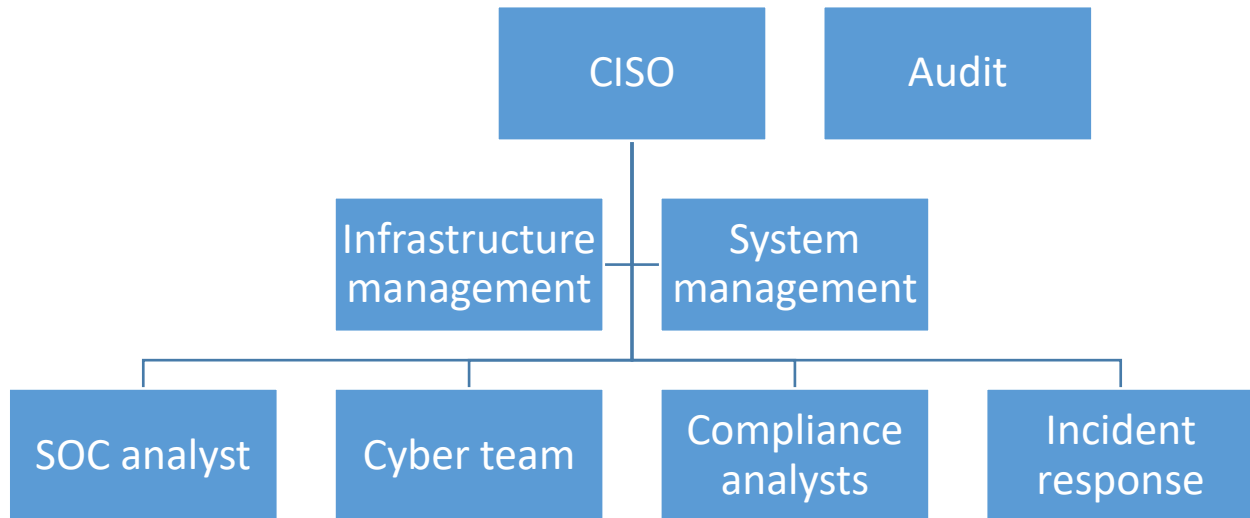


Use Cases

First page – overview of many PEM uses and the possible use cases for each kind of worker in the org, have a graphic showing the hierarchy, you can click on each of the section to jump to that worker and the use cases/challenge that PEM solves for them. Have each relevant section highlighted on the correct page.

Tasks –

- Create hierarchy tree – check with Ori
- Identify correct screen for each use case, bring screenshot



CISO 1

System Management Team

Infrastructure Architects

Cyber Team

Compliance Analysts

Incident Response

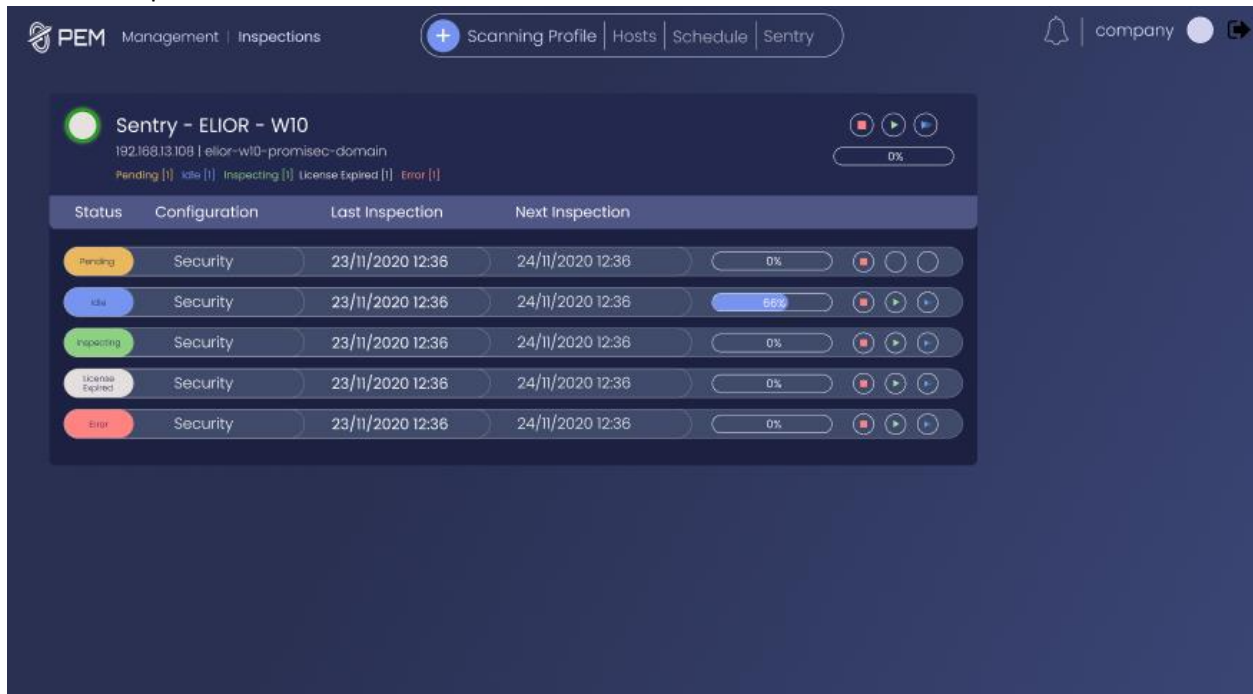
SOC Analysts

Audits

[T1] Use Cases

Promisec Endpoint Manager contains within it a multitude of tools, and has applicable capabilities for employees at every level of the organization. Whether for the strategic and administrative challenges of the CISO, the monitoring challenges of the SOC team, or the security challenges of the system management, PEM has a solution. The various use cases which PEM is capable of include full organizational visibility, automated reporting, and analysis capabilities which can be used to identify and deal with security issues at the lowest levels.

Screen – Inspections



Status	Configuration	Last Inspection	Next Inspection	Progress	Actions
Pending	Security	23/11/2020 12:36	24/11/2020 12:36	0%	Stop, Play, Refresh
Idle	Security	23/11/2020 12:36	24/11/2020 12:36	56%	Stop, Play, Refresh
Inspecting	Security	23/11/2020 12:36	24/11/2020 12:36	0%	Stop, Play, Refresh
License Expired	Security	23/11/2020 12:36	24/11/2020 12:36	0%	Stop, Play, Refresh
Error	Security	23/11/2020 12:36	24/11/2020 12:36	0%	Stop, Play, Refresh

Explore your use case.

[T2] CISO –

Dashboard



[T3] Challenge – ensure that the IT is functioning smoothly, that the organization is secure and compliant, and that critical events are dealt with.

[T3] PEM solution –

- Monitor overall organization status with dashboard
- See and respond to organizational trends over time
- Receive automated reporting regarding status and critical gaps
- Produce high-level reports for presentation to executives

[T2] System management team

Users and permissions



The interface shows a table of User Groups with the following columns: Group Name and Permissions. The permissions are represented by buttons for various actions.

Group Name	Permissions
EE Admins	Inspection Write, Inspection Run, Management, Dashboard View, Updates, Users and Permissions, Inspection View
EE Users	Inspection Write, Inspection Run, Management, Dashboard View, Updates, Users and Permissions, Inspection View
EE Viewers	Inspection Write, Inspection Run, Management, Dashboard View, Updates, Users and Permissions, Inspection View
BHART	Inspection Write, Inspection Run, Management, Dashboard View, Updates, Users and Permissions, Inspection View
Inspection Run	Inspection Write, Inspection Run, Management, Dashboard View, Updates, Users and Permissions, Inspection View
Inspection Write	Inspection Write, Inspection Run, Management, Dashboard View, Updates, Users and Permissions, Inspection View
Management	Inspection Write, Inspection Run, Management, Dashboard View, Updates, Users and Permissions, Inspection View
Users & Permissio...	Inspection Write, Inspection Run, Management, Dashboard View, Updates, Users and Permissions, Inspection View
Updates	Inspection Write, Inspection Run, Management, Dashboard View, Updates, Users and Permissions, Inspection View
Dash View	Inspection Write, Inspection Run, Management, Dashboard View, Updates, Users and Permissions, Inspection View

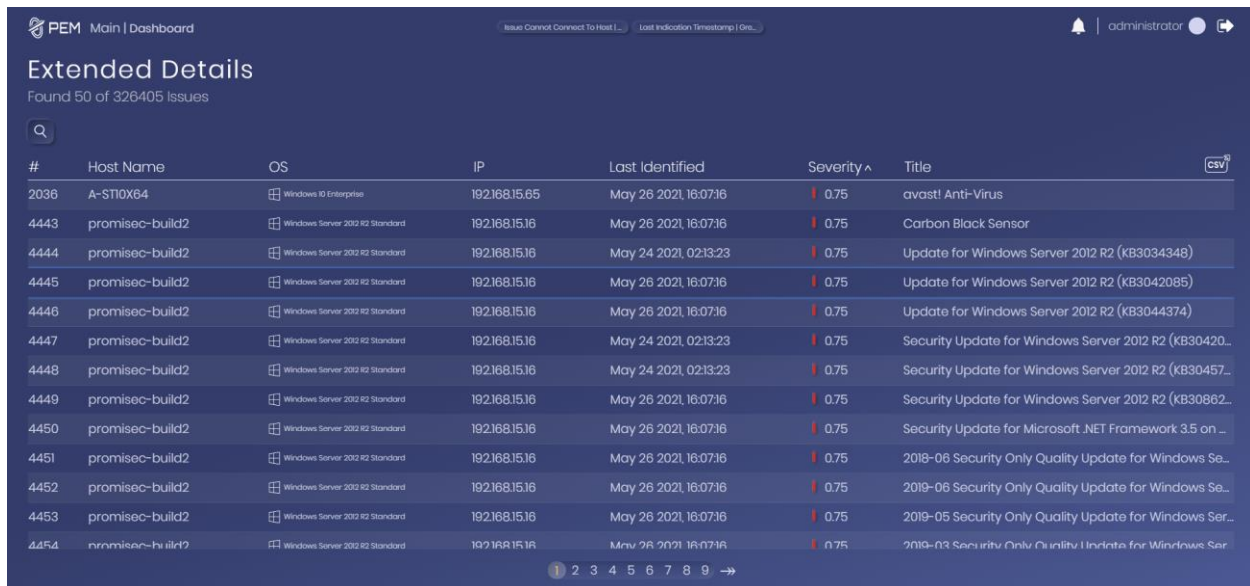
[T3] Challenge – Administrate organizational networks and systems, ensuring maximum efficiency and overall security.

[T3] PEM solution –

- Monitor hardware and software inventory
- Manage storage and system capacity, ensuring efficient use of resources
- Ensure deployment, activation and updating of security tools to all endpoints
- Manage system users and their permissions with predefined and custom groups

[T2] Infrastructure architects

Extended details



#	Host Name	OS	IP	Last Identified	Severity ^	Title
2036	A-ST0X64	Windows 10 Enterprise	192.168.15.65	May 26 2021, 16:07:16	0.75	avast! Anti-Virus
4443	promisec-build2	Windows Server 2012 R2 Standard	192.168.15.16	May 26 2021, 16:07:16	0.75	Carbon Black Sensor
4444	promisec-build2	Windows Server 2012 R2 Standard	192.168.15.16	May 24 2021, 02:13:23	0.75	Update for Windows Server 2012 R2 (KB3034348)
4445	promisec-build2	Windows Server 2012 R2 Standard	192.168.15.16	May 26 2021, 16:07:16	0.75	Update for Windows Server 2012 R2 (KB3042085)
4446	promisec-build2	Windows Server 2012 R2 Standard	192.168.15.16	May 26 2021, 16:07:16	0.75	Update for Windows Server 2012 R2 (KB3044374)
4447	promisec-build2	Windows Server 2012 R2 Standard	192.168.15.16	May 24 2021, 02:13:23	0.75	Security Update for Windows Server 2012 R2 (KB30420...
4448	promisec-build2	Windows Server 2012 R2 Standard	192.168.15.16	May 24 2021, 02:13:23	0.75	Security Update for Windows Server 2012 R2 (KB30457...
4449	promisec-build2	Windows Server 2012 R2 Standard	192.168.15.16	May 26 2021, 16:07:16	0.75	Security Update for Windows Server 2012 R2 (KB30862...
4450	promisec-build2	Windows Server 2012 R2 Standard	192.168.15.16	May 26 2021, 16:07:16	0.75	Security Update for Microsoft .NET Framework 3.5 on ...
4451	promisec-build2	Windows Server 2012 R2 Standard	192.168.15.16	May 26 2021, 16:07:16	0.75	2019-06 Security Only Quality Update for Windows Se...
4452	promisec-build2	Windows Server 2012 R2 Standard	192.168.15.16	May 26 2021, 16:07:16	0.75	2019-06 Security Only Quality Update for Windows Se...
4453	promisec-build2	Windows Server 2012 R2 Standard	192.168.15.16	May 26 2021, 16:07:16	0.75	2019-05 Security Only Quality Update for Windows Ser...
4454	promisec-build2	Windows Server 2012 R2 Standard	192.168.15.16	May 26 2021, 16:07:16	0.75	2019-03 Security Only Quality Update for Windows Ser...

[T3] Challenge – Construct, configure and maintain organizational infrastructure, ensuring optimized and secure information systems.

[T3] PEM solution –

- Integrate new endpoints seamlessly into the existing security paradigm
- Use automatic GPO and golden image implementation to keep all endpoints at optimal security status
- Monitor overall network security, use custom groups to monitor specific logical/network endpoint groups

[T2] Cyber team

MITRE ATT&CK

PEM Main | Cyber Issue: Cannot Connect To Host... Last Indication Timestamp: Gre... administrator

File Integrity

Found 50 of 470 Results

Scanned 23
 Unscanned 43

Search: All

#	Host Name	OS	IP	Last Identified	E. Severity ^	File Path
1333	A-ST10X32	Windows 10 Enterprise	192.168.15.50	May 24 2021, 22:09:00	418	c:\windows\system32\searchindexer.exe
1334	A-ST10X32	Windows 10 Enterprise	192.168.15.50	May 24 2021, 22:09:00	418	c:\windows\system32\winlogon.exe
1335	A-ST10X32	Windows 10 Enterprise	192.168.15.50	May 24 2021, 22:09:00	418	c:\windows\system32\dwm.exe
1336	A-ST10X32	Windows 10 Enterprise	192.168.15.50	May 24 2021, 22:09:00	418	c:\program files\remp\sedsvc.exe
1337	A-ST10X32	Windows 10 Enterprise	192.168.15.50	May 24 2021, 22:09:00	418	c:\windows\system32\lsass.exe
1338	A-ST10X32	Windows 10 Enterprise	192.168.15.50	May 24 2021, 22:09:00	418	c:\windows\system32\logonui.exe
1339	A-ST10X32	Windows 10 Enterprise	192.168.15.50	May 24 2021, 22:09:00	418	c:\windows\system32\svchost.exe
1340	A-ST10X32	Windows 10 Enterprise	192.168.15.50	May 24 2021, 22:09:00	418	c:\windows\system32\spoolsv.exe
1341	A-ST10X32	Windows 10 Enterprise	192.168.15.50	May 24 2021, 22:09:00	418	c:\windows\system32\wbem\wmiprvse.exe
1342	A-ST10X32	Windows 10 Enterprise	192.168.15.50	May 24 2021, 22:09:00	418	c:\windows\system32\vssvc.exe
1839	A-ST10X32	Windows 10 Enterprise	192.168.15.50	May 24 2021, 22:25:18	418	c:\cybertestfile\exe.exe
1849	A-ST10X32	Windows 10 Enterprise	192.168.15.50	May 24 2021, 22:25:18	418	c:\exe.exe
1855	A-ST10X32	Windows 10 Enterprise	192.168.15.50	May 24 2021, 22:09:00	418	c:\windows\system32\ahant.exe

1 2 3 4 5 6 7 8 9 →

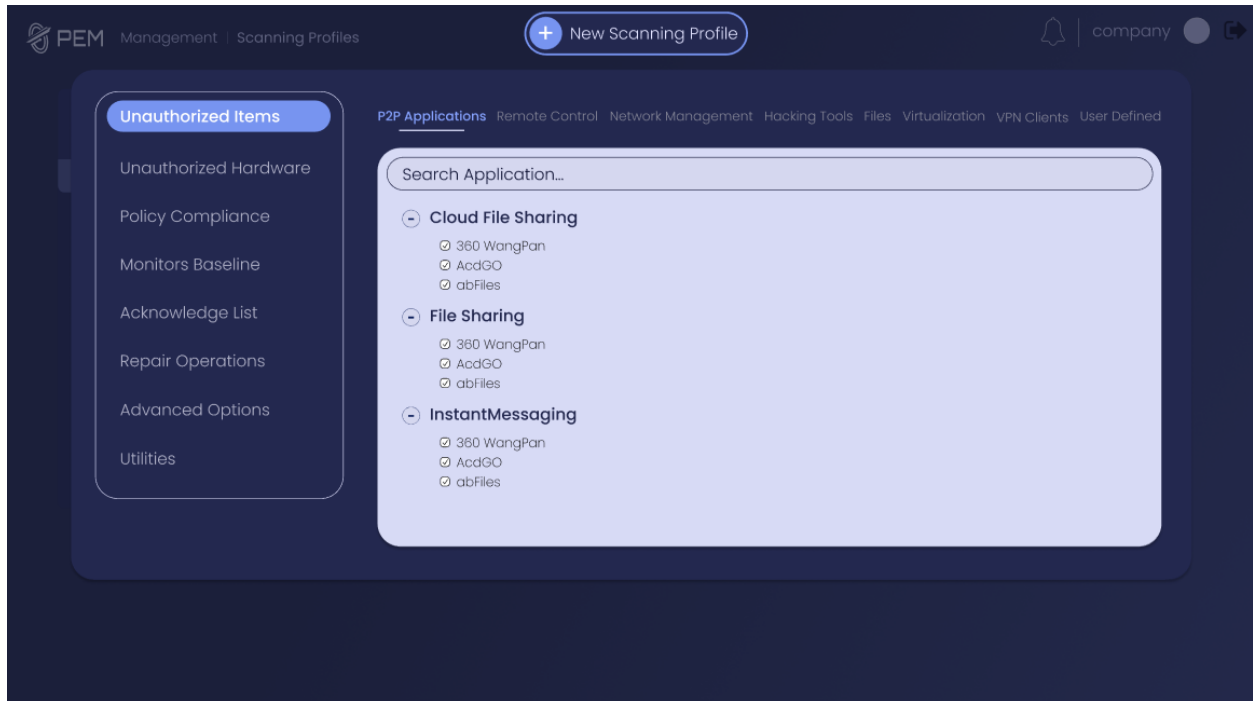
[T3] Challenge – Identify, analyze and remediate security gaps. Challenge company security with external testing.

[T3] PEM solution –

- Monitor hash changes and identify suspicious hashes
- Identify active CVEs
- Use integrated MITRE ATT&CK matrix to perform strategic analysis and identify weak points

[T2] Compliance analysts

Scanning profile screen



[T3] Challenge – Ensure organizational compliance to defined policies and accepted standards.

[T3] PEM solution –

- Define organizational policy, either custom or according to accepted compliance standards such as CIS or NIST
- Identify exceptions or deviations from defined organizational policies, including applications whitelists/blacklists
- Either escalate or remediate identified instances to ensure organization-wide compliance

[T2] Incident response team

Notification/trend/?



[T3] Challenge – Create and maintain incident response methodology and strategy, respond decisively and rapidly to cybersecurity events to mitigate damage to organizational assets, reputation, and business continuity.

[T3] PEM solution –

- Become aware of signs of ongoing incidents with alerting system
- Forensic analysis following incidents
- Track positive or negative trends of specified attributes or endpoints according to remediation recommendations to ensure prevention of future incidents

[T2] SOC analysts

Reports (CSV)

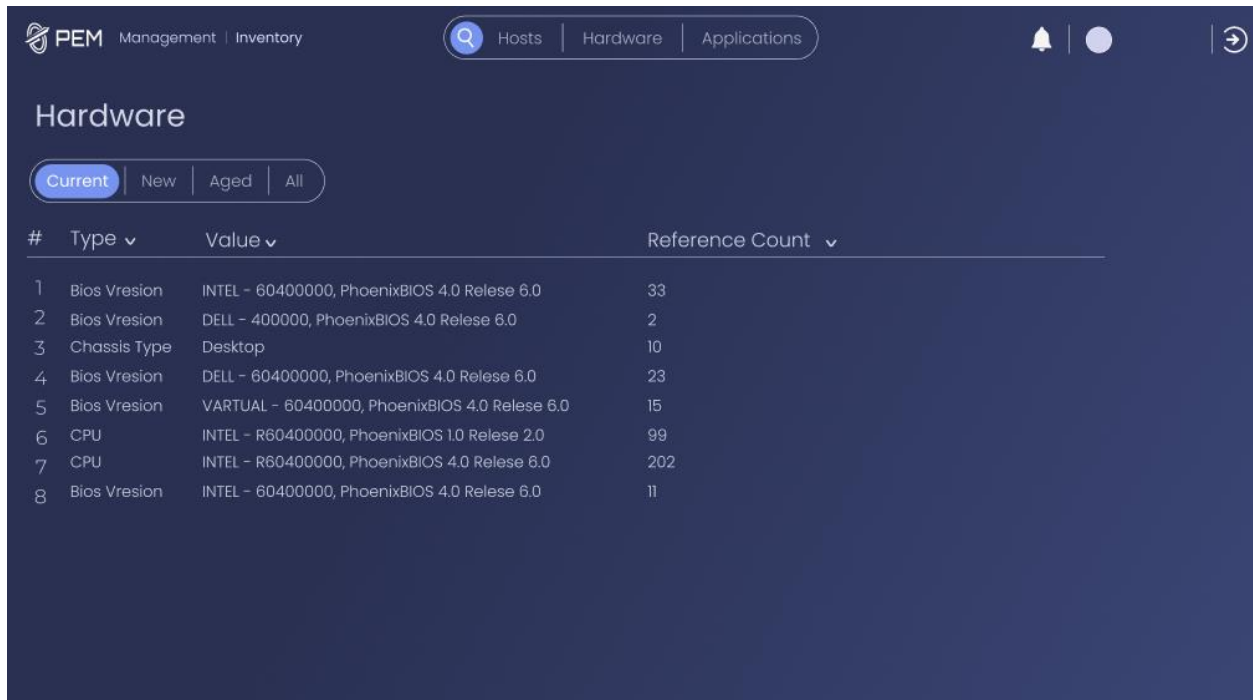
[T3] Challenge – Monitor for security events, respond or escalate identified instances of security gaps, incidents, or suspicious activity. Remain aware of and report trends.

[T3] PEM solution –

- Integrate PEM findings into third-party security solutions or organizational SIEM
- Identify security events
- Identify suspicious activity
- Isolate security issues to the level of specific endpoints to enable remediation

[T2] Audit team

Inventory



The screenshot shows the 'Hardware' section of the PROMISEC management interface. It features a navigation bar with 'Hosts', 'Hardware', and 'Applications' tabs. Below the navigation, there are filter buttons for 'Current', 'New', 'Aged', and 'All'. The main content is a table with the following data:

#	Type	Value	Reference Count
1	Bios Vresion	INTEL - 60400000, PhoenixBIOS 4.0 Release 6.0	33
2	Bios Vresion	DELL - 400000, PhoenixBIOS 4.0 Release 6.0	2
3	Chassis Type	Desktop	10
4	Bios Vresion	DELL - 60400000, PhoenixBIOS 4.0 Release 6.0	23
5	Bios Vresion	VARTUAL - 60400000, PhoenixBIOS 4.0 Release 6.0	15
6	CPU	INTEL - R60400000, PhoenixBIOS 1.0 Release 2.0	99
7	CPU	INTEL - R60400000, PhoenixBIOS 4.0 Release 6.0	202
8	Bios Vresion	INTEL - 60400000, PhoenixBIOS 4.0 Release 6.0	11

[T3] Challenge – Oversee organizational assets, ensure adherence to accepted policies and reduce waste.

[T3] PEM solution –

- Use hardware and software inventory to assess organizational assets
- Software license management to prevent wasted resources