Continuous Posture Anomalies Management

Use-Cases

A detailed use-case guide for understanding various prevention mechanisms to detect anomaly forms

By Preeti Subramanian, SecPod, January 2023

Understanding the need

Anomaly detection mechanisms are often deployed to **detect** an attack, not **prevent** them. Identifying deviations in an organization's assets is essential as the first step towards gaining visibility and bringing order to business. Chaos and clutter of technologies are complicated to maintain.

Prevention mechanisms using Anomaly Detection start with questioning the rudimentary configurations of the systems. Do we need these inconsistent applications? Why are so many ports open, numerous processes running, or different firewalls configured across devices? A patch affects only one system in the organization; why is it so? Often we see that a unique operating system or application is running on that device, which also results in vulnerabilities and misconfigurations anomalies that are avoidable.

Visibility to 1000+ parameters in devices and detection of anomalies eases decision-making for IT and Security administrators to prevent surprise attacks. Simple and intuitive dashboards can help fix the deviations with a collection of relevant actions. Safe listing abnormal findings that are expected in the devices can bring a standard to be followed while computing anomalies.

Machine Learn your IT

We apply artificial intelligence to data collected from devices in our Saner account, analyze data based on predefined rules and trends, and successfully involve outlier mechanisms based on IQR. An **outlier** is a data point that deviates significantly from the rest of the objects assembled from regular scans of devices in the organization. A user interface provides visualization methods, such as Box-plot, Histogram, Scatter Plot, and Bar charts, to envisage the deviations and abnormalities.

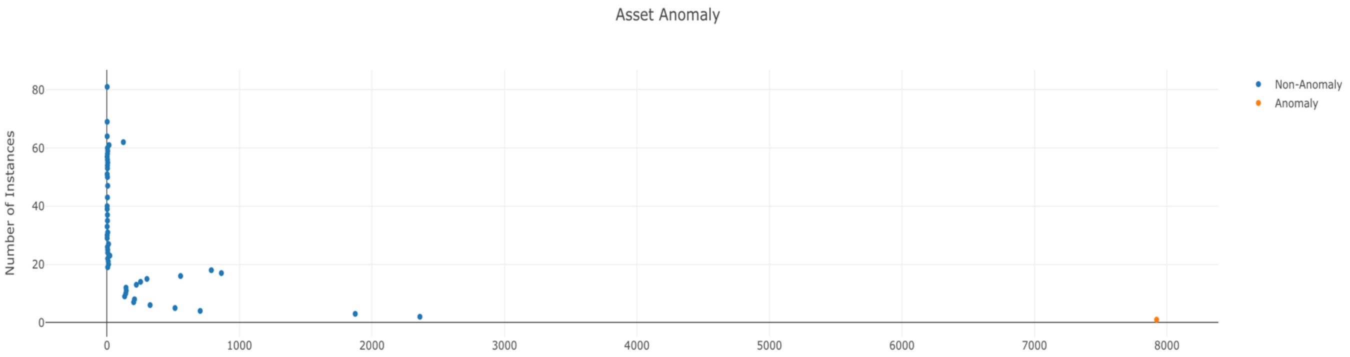
> *"A deviation or abnormality can be effectively recognized when data objects from devices are observed collectively and data analytics mechanisms are applied on these data objects."*

Machine learn your IT amid understanding outliers in applications, processes, services, ports, kernel version, ARP mapping, DNS cache, Windows events, Command history, Outbound connections made by devices, unusual start applications, environment variables, and task schedulers.

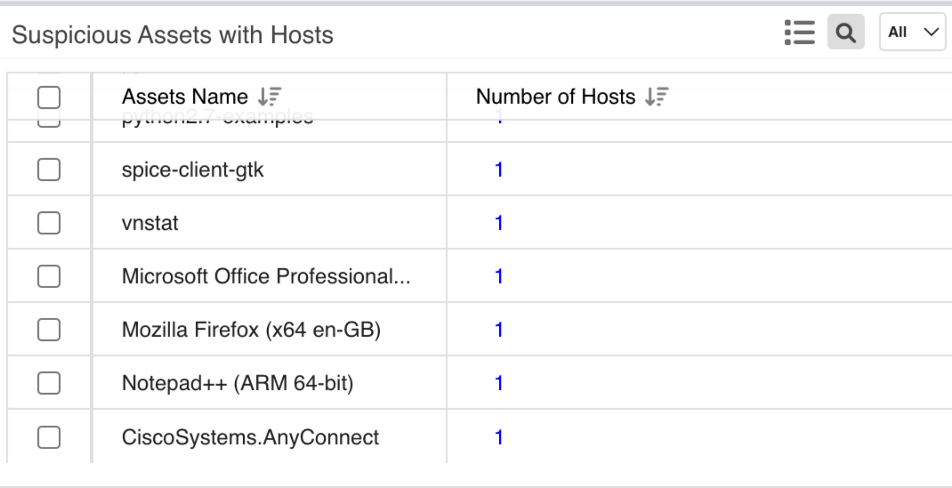
Unusual and unique applications are installed

A view of anomalies in applications installed helps make various decisions, whether to invest in such software assets because of a pressing business need or trade-off with better-streamlined solutions already available in the organization that caters to the same condition. The fewer unusual applications in the organization, the better the attack surface reduction when we uninstall such unnecessary software assets.

A scatter plot can help visualize many assets with a unique presence in only one device of the organization.



Such applications are listed in the table according to anomaly findings and devices. One can block and uninstall such applications or whitelist, confirming that the specific anomaly finding is not reported in the future.



Suspicious Assets with Hosts

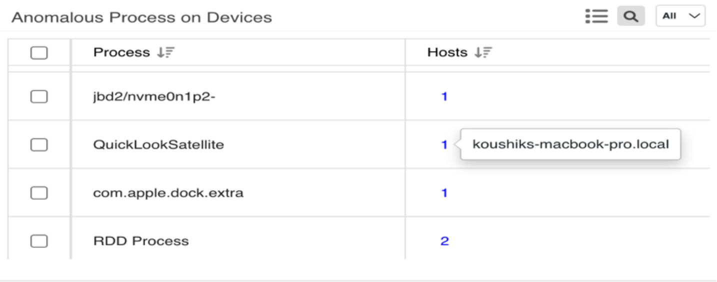
□	Assets Name	Number of Hosts
□	python2.7-examples	1
□	spice-client-gtk	1
□	vnstat	1
□	Microsoft Office Professional...	1
□	Mozilla Firefox (x64 en-GB)	1
□	Notepad++ (ARM 64-bit)	1
□	CiscoSystems.AnyConnect	1

Table: PA-2022-1002 identifies unique software applications determined in a select few systems

Unusual services and processes are running

Say goodbye to surprises and fix all sporadic services and processes running on a select few systems. Understand a little more about these processes using Custom Rules (Detection) available on the menu bar to determine if these running processes are pointless. These processes may add excessive burden on your CPU and RAM, reducing the machine’s responsiveness.

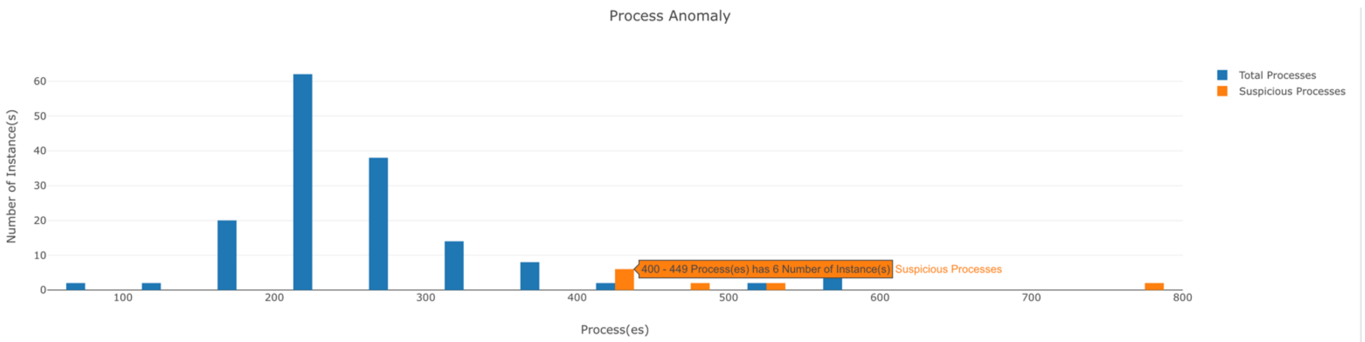
For example, QuickLookSatellite process on a Mac machine is at the top of the CPU usage list. The process quicklooksat is perhaps trying to make the preview of a file that is damaged.



Anomalous Process on Devices

□	Process	Hosts
□	jbd2/nvme0n1p2-	1
□	QuickLookSatellite	1 koushiks-macbook-pro.local
□	com.apple.dock.extra	1
□	RDD Process	2

The mechanism of detection involves identifying anomloulous processes running in the systems. Processes run in large numbers on a few systems when these systems are observed collectively.



Atypical Kernel Versions, Modules and Parameters determined

IT administrators are annihilated with issues such as audio or mouse not working with a particular kernel version**.** Setting the GSO parameter in Linux with a specific kernel version slows the transfer speed down compared to the same system but with a higher kernel version or unexpected memory usage while using a kernel version. Such issues can be thawed by streamlining kernel versions. CPAM gives visibility to these deviations. The fix may be tricky manually, but not with us. We help deploy a single script on many devices to install a specific kernel version and modify the entry through Native Internal Kernel Management grub configuration. Deploying this script through Software deployment can prevent such concerns.

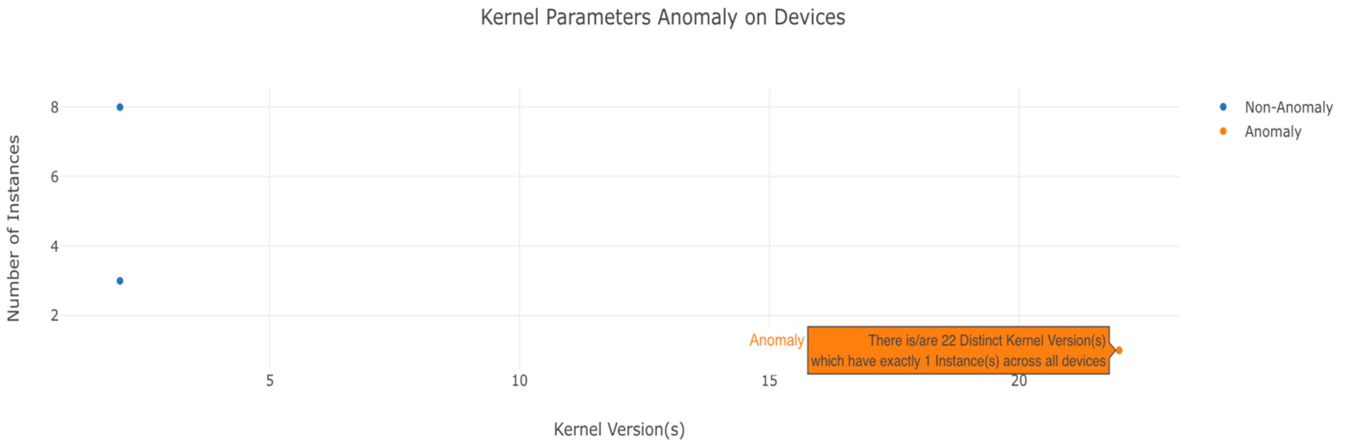
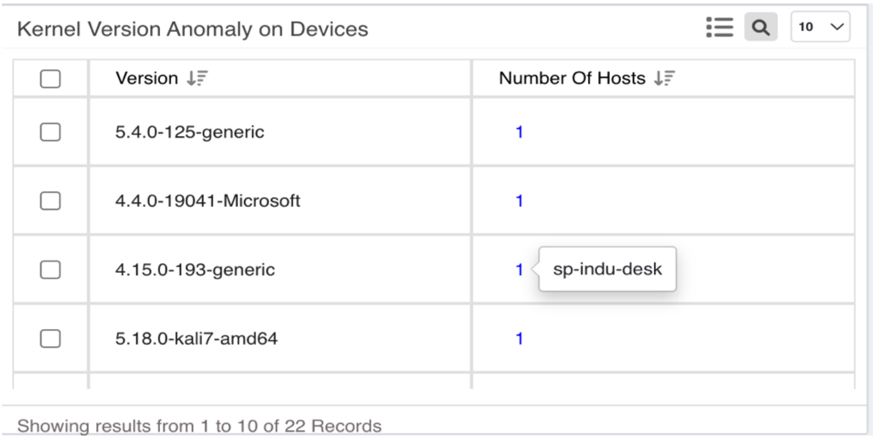


Table: A list of all anomalous kernel versions could be an eye-opener to comprehend the deviations in an organization.

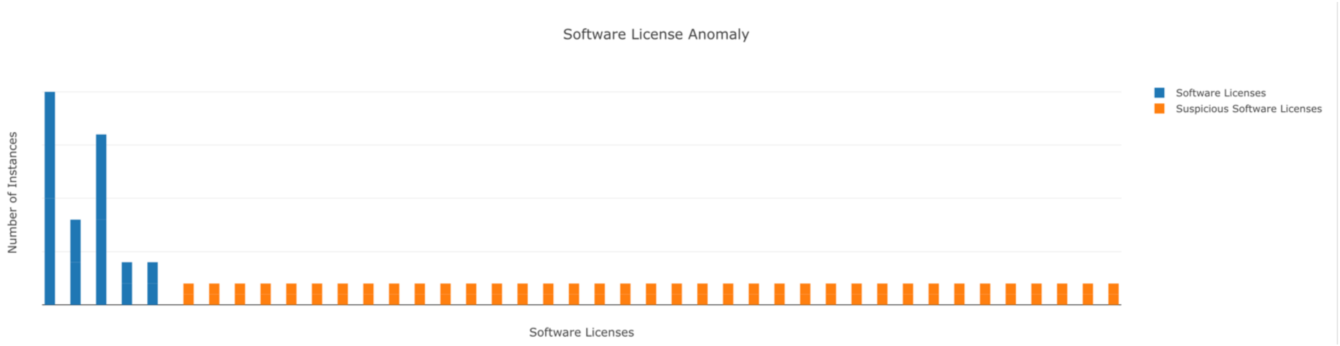

Kernel Version Anomaly on Devices

□	Version	Number Of Hosts
□	5.4.0-125-generic	1
□	4.4.0-19041-Microsoft	1
□	4.15.0-193-generic	1
□	5.18.0-kali7-amd64	1

Showing results from 1 to 10 of 22 Records

Unique software licenses

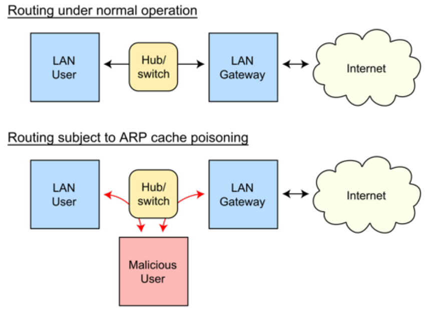
Determine unique software license keys in the organization with data analytics to collect, transform, cluster, tune and alert based on specific bound.



The plot shows that the organization has invested in bulk licenses as well as individual licenses of operating systems.

Irregular Mapping IP to MAC and DNS to IP

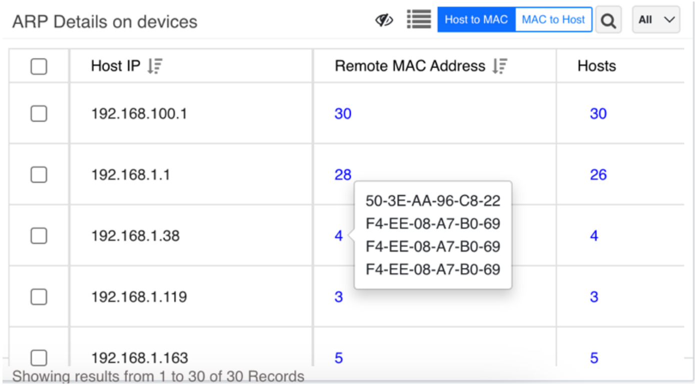
Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network. ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address and vice versa. Most commonly, devices use ARP to contact the router or gateway to connect to the Internet. Discrepancies in IP and MAC address mapping indicate ARP poisoning and Man in the Middle attacks. The attacker can sniff the packets and steal data if transferred not via HTTPs.



Source: Wiki

Similarly, DNS cache poisoning is the act of entering false information into a DNS cache so that DNS queries return an incorrect response and users are directed to the wrong websites.

We can visualize such issues using anomaly detection based on rule-based analytics and automatically designating confidence to each of anomaly finding using the IQR method.



ARP Details on devices

☐	Host IP	Remote MAC Address	Hosts
☐	192.168.100.1	30	30
☐	192.168.1.1	28	26
☐	192.168.1.38	4	4
☐	192.168.1.119	3	3
☐	192.168.1.163	5	5

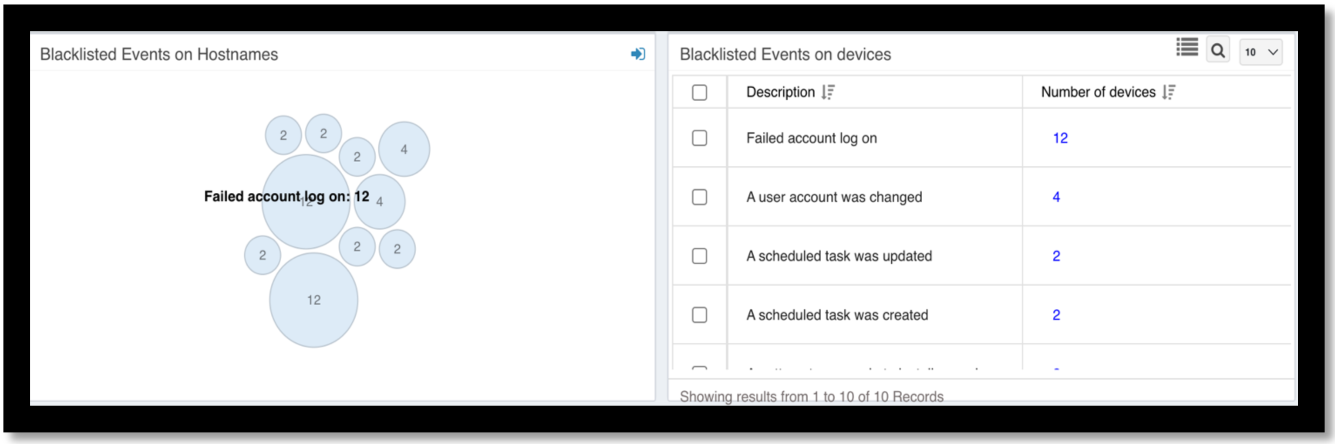
50-3E-AA-96-C8-22
F4-EE-08-A7-B0-69
F4-EE-08-A7-B0-69
F4-EE-08-A7-B0-69

Showing results from 1 to 30 of 30 Records

While three devices have the duplicate ARP entry for 192.168.1.38, one device deviates with MAC 50-3E-AA-96-C8-22, requiring investigation.

Anomalous Events in the Windows Events Log

Churning Windows events logs from devices for blacklisted and alarming events such as Event ID 4625 when a failed login is attempted on a machine, Event ID 4720 when a user account is created, Event ID 4738 when a user account is modified and many more. Administrators can scrutinize why such events are happening, whether they are genuine to be whitelisted or need to be addressed quickly to prevent attacks.



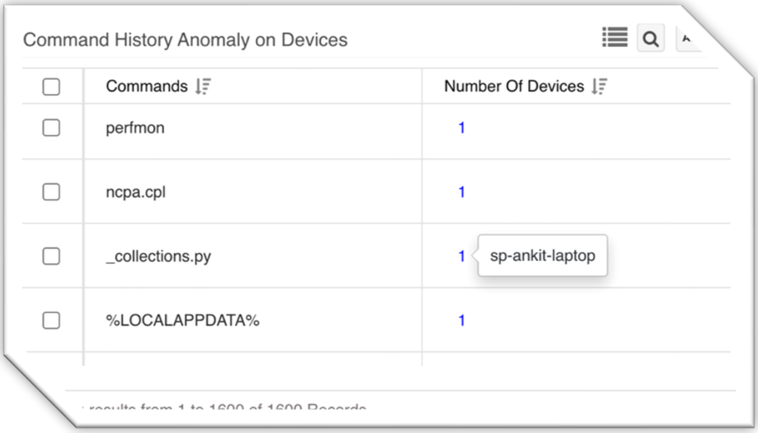
Blacklisted Events on devices

□	Description	Number of devices
□	Failed account log on	12
□	A user account was changed	4
□	A scheduled task was updated	2
□	A scheduled task was created	2

Showing results from 1 to 10 of 10 Records

Unusual commands are executed

Hundreds of commands can be analyzed and observed on a single click to understand what is being executed on the devices. If passwords are entered in clear text as arguments to scripts or clients connecting to the server, inputs such as password and tokens can be changed to pick from a file vault or encrypted files. A command uniquely runs on a specific device that serves as critical infrastructure to the organization, raises the alarm, and needs the administrator's focus.



Command History Anomaly on Devices

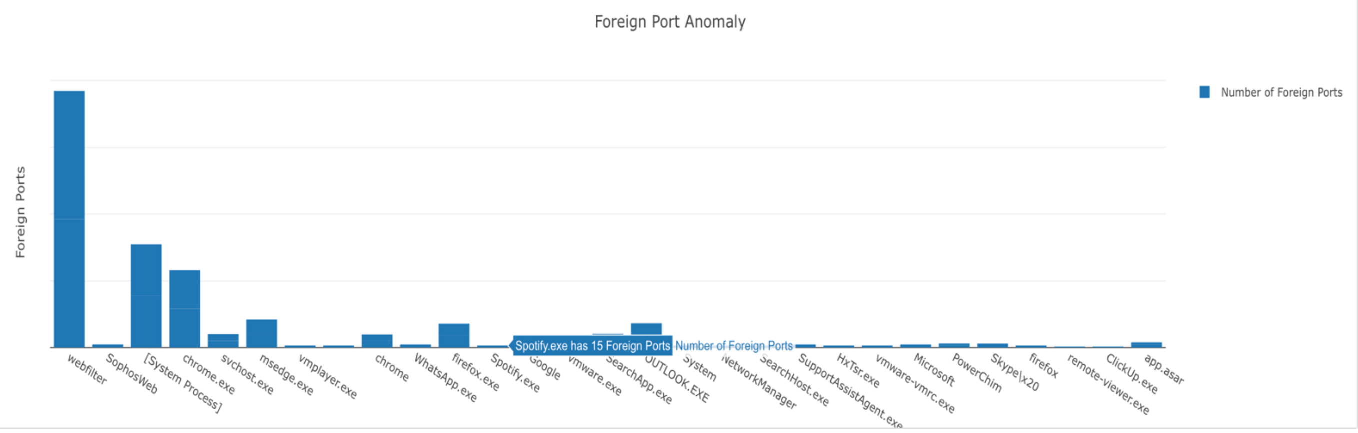
□	Commands	Number Of Devices
□	perfmon	1
□	ncpa.cpl	1
□	_collections.py	1
□	%LOCALAPPDATA%	1

results from 1 to 1600 of 1600 Records

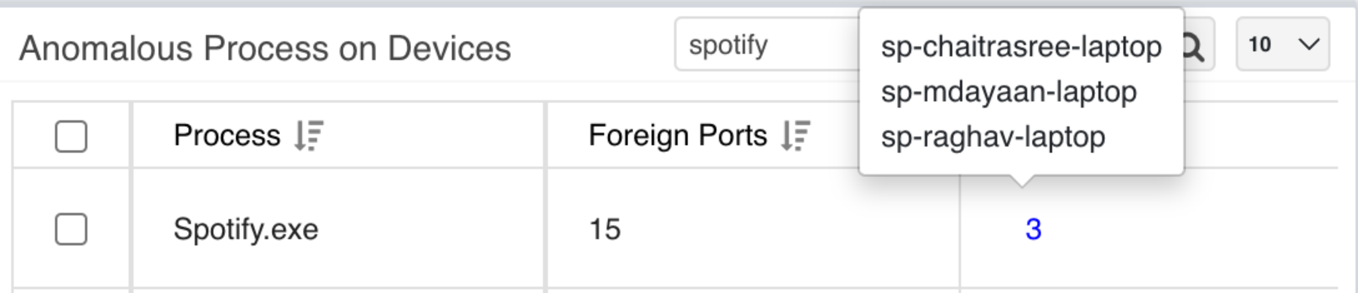
We are observing ncpa.cpl, a command that redirects the user to the network adaptors of the computer or a strange python file executed.

Outbound connections to unusual network ports are detected

Even though the best firewall configuration practices are in place, the users may be able to see standard outbound connections to a foreign address on different ports. Such connections often come as a revelation when we expect to connect to a server, say Google servers, on the standard ports but uncharacteristically see machines connected to a different port than expected.



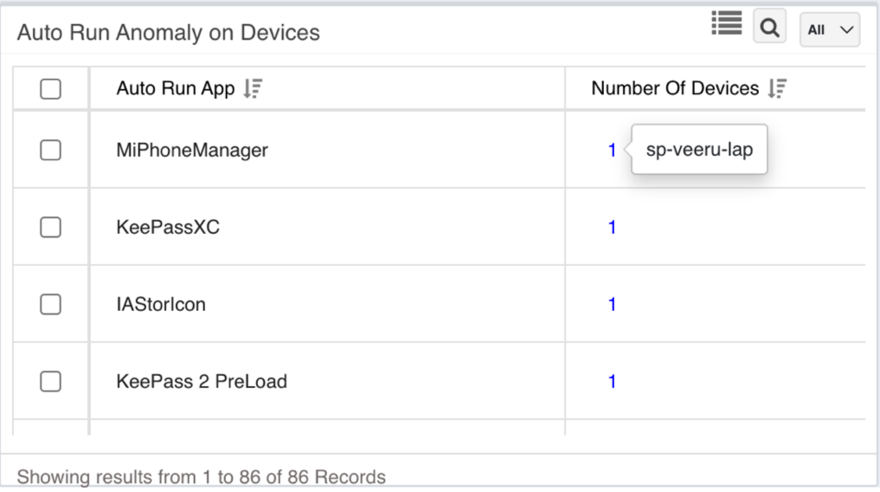
Identifying devices and foreign port instances of anomalous process spotify.exe


Anomalous Process on Devices

□	Process	Foreign Ports	
□	Spotify.exe	15	3

Unusual entries in the task scheduler, autorun and startup configuration, and environment variables

We expect typical applications to start when a machine boots up; deviations in startup applications are not sought. Unusual autorun applications could be dangerous as they bring vulnerabilities resulting in an impending malicious attack in the future. Strange entries in environment variables may point to an incorrect or unnecessary application. Also, task schedulers such as cron should run relevant tasks in hand. Cleaning up such deviations reduces the attack surface.


Auto Run Anomaly on Devices

□	Auto Run App	Number Of Devices
□	MiPhoneManager	1
□	KeePassXC	1
□	IAStorIcon	1
□	KeePass 2 PreLoad	1

Showing results from 1 to 86 of 86 Records

Users can remove unnecessary applications, such as personal phone managers, from the organization's laptop and reduce applications marked as auto-run.

Visualizing and fixing anomaly findings in your organization is valuable.

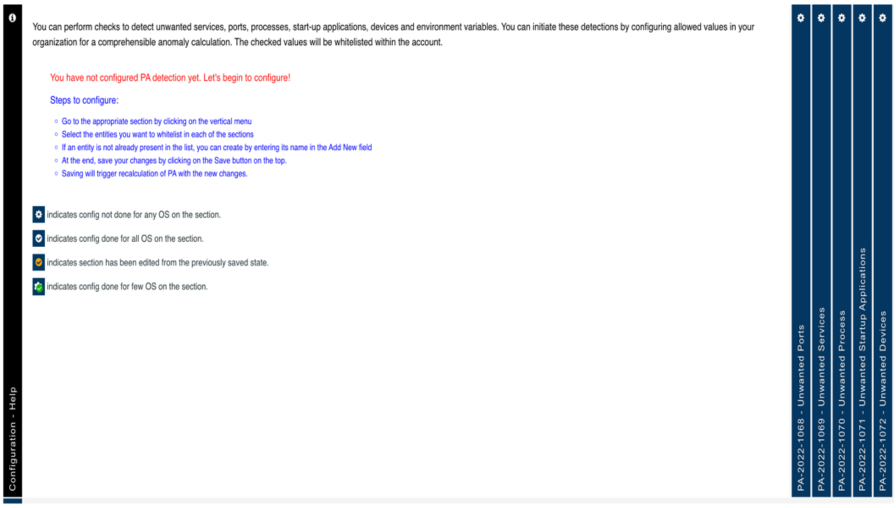
Known-Good Assets in your IT

We often encounter numerous software installed in a machine, whether in-use or not-in-use, personal devices connected to the organization's network, ports, or services running in computer systems, whether necessary or not. Employees and users have different software preferences accounting for their work requisites. Such anomalies often cause uncertainties and unnecessary surprises for our IT and Security Administrators, who constantly strive to keep the organization secure, keep track of inventories, help with software installation, and steadily keep them up to date. Finding anomalies in an organization and removing such deviations can help reduce the attack surface and prevent cyberattacks.

Unwanted applications, services, processes installed, Unwanted devices present, and Unwanted network ports are listening

Start configuring with what you distinguish as essential for your organization and whitelist services, processes, allowed network ports, environment variables, and startup applications. This configuration forms a baseline for the organization. On successful configuration, anomalies unfold when an unforeseen application is installed, opening a network port, starting a service, or an unexpected process. See such deviations miraculously appearing on the dashboards as soon as the scan finishes.

Declutter your IT infrastructure and eliminate the unnecessary. Control your SBOM.



You can perform checks to detect unwanted services, ports, processes, start-up applications, devices and environment variables. You can initiate these detections by configuring allowed values in your organization for a comprehensible anomaly calculation. The checked values will be whitelisted within the account.

You have not configured PA detection yet. Let's begin to configure!

Steps to configure:

- Go to the appropriate section by clicking on the vertical menu
- Select the entities you want to whitelist in each of the sections
- If an entity is not already present in the list, you can create by entering its name in the Add New field
- At the end, save your changes by clicking on the Save button on the top.
- Saving will trigger recalculation of PA with the new changes.

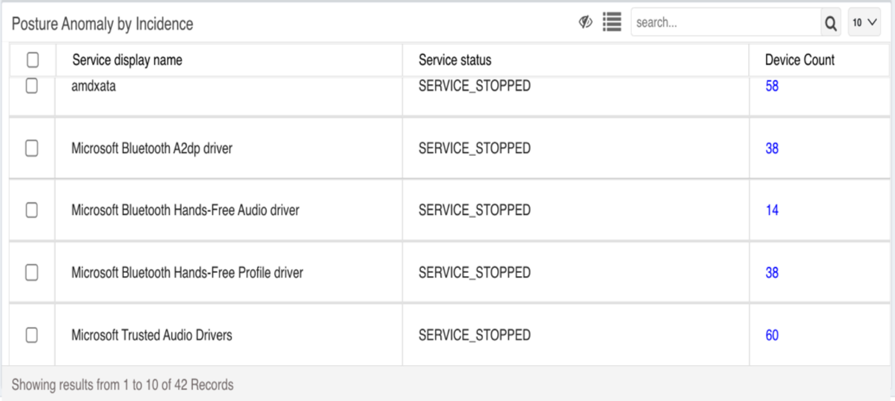
⚙ indicates config not done for any OS on the section.

✓ indicates config done for all OS on the section.

✓ indicates section has been edited from the previously saved state.

✓ indicates config done for few OS on the section.

Configuration - Help
PA-2022-1068 - Unwanted Ports
PA-2022-1069 - Unwanted Services
PA-2022-1070 - Unwanted Process
PA-2022-1071 - Unwanted Startup Applications
PA-2022-1072 - Unwanted Devices



Posture Anomaly by Incidence

□	Service display name	Service status	Device Count
□	amdxata	SERVICE_STOPPED	58
□	Microsoft Bluetooth A2dp driver	SERVICE_STOPPED	38
□	Microsoft Bluetooth Hands-Free Audio driver	SERVICE_STOPPED	14
□	Microsoft Bluetooth Hands-Free Profile driver	SERVICE_STOPPED	38
□	Microsoft Trusted Audio Drivers	SERVICE_STOPPED	60

Showing results from 1 to 10 of 42 Records

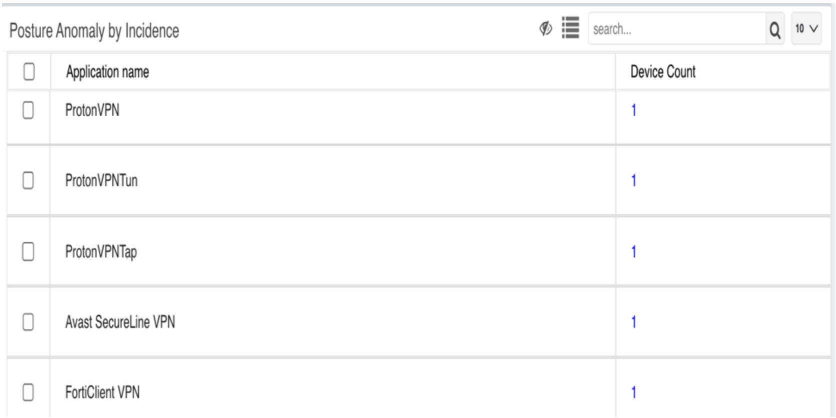
Inspect scheduled tasks, run level programs, and environmental variables deeply

Anomalies can be present in scheduler tasks such as run-level of applications, tasks set in crontab, Windows schedule, and various environment variables that need an in-depth countenance.

- Runlevels determine which programs can execute after the OS boots up and can be used by attackers to run malicious software that goes unnoticed
- Environment variables can be poisoned to point to the malicious software versions
- Strange tasks can come up at night hours or holidays, when IT and Security administrators are preoccupied, to perform malicious attacks on the systems during off hours and steal confidential information. These may go completely unheeded, and activities appear normal during work hours.

Do you know how many VPN tools are used in your environment?

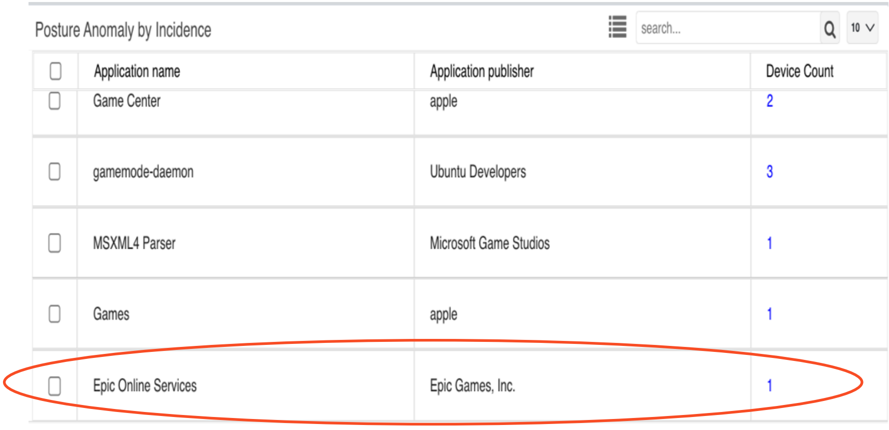
There could be so many unique VPN software installed on only one machine. This could be streamlined.



Posture Anomaly by Incidence

☐	Application name	Device Count
☐	ProtonVPN	1
☐	ProtonVPNTun	1
☐	ProtonVPNTap	1
☐	Avast SecureLine VPN	1
☐	FortiClient VPN	1

What are these Cloud applications or Gaming Apps in use?



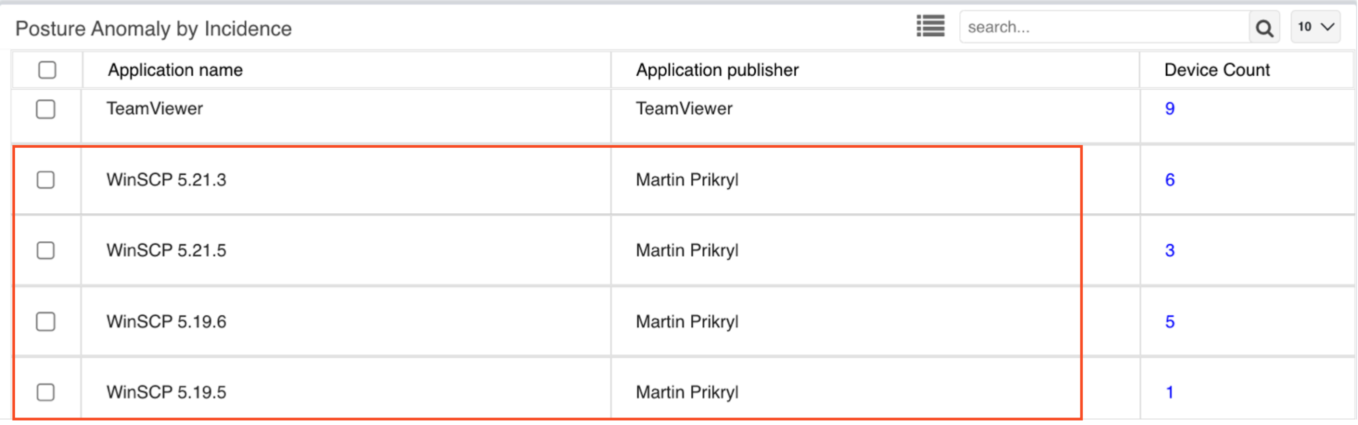
Posture Anomaly by Incidence

☐	Application name	Application publisher	Device Count
☐	Game Center	apple	2
☐	gamemode-daemon	Ubuntu Developers	3
☐	MSXML4 Parser	Microsoft Game Studios	1
☐	Games	apple	1
☐	Epic Online Services	Epic Games, Inc.	1

Continous Posture Anomaly Management aims to discover risk exposures that are fundamental to the cyber-attack prevention journey.

Are these File transfer apps indispensable to our organization?

Users can spot many file transfer applications in the organization. There could be instances where the same file transfer application with different versions may cause chaos while maintaining and patching these versions. Streamlining such applications is worthwhile.

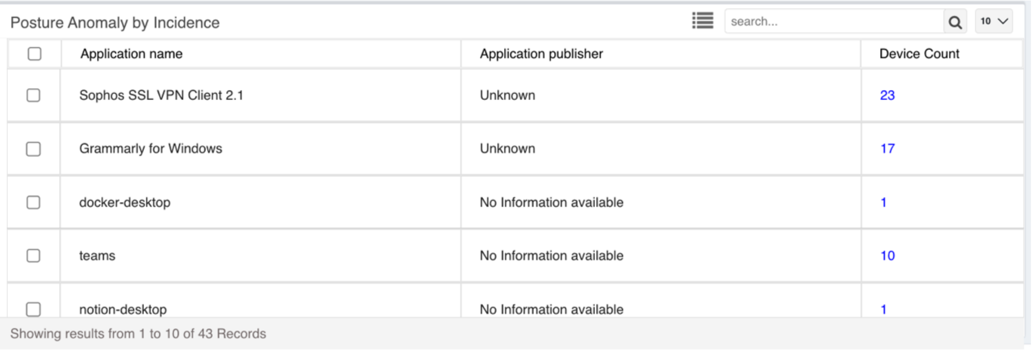


Posture Anomaly by Incidence

□	Application name	Application publisher	Device Count
□	TeamViewer	TeamViewer	9
□	WinSCP 5.21.3	Martin Prikryl	6
□	WinSCP 5.21.5	Martin Prikryl	3
□	WinSCP 5.19.6	Martin Prikryl	5
□	WinSCP 5.19.5	Martin Prikryl	1

Do we have Applications from unknown publishers or unverified?

Applications that are downloaded from different sources cannot promise genuinity. Applications with broken signatures and unknown publishers may have been tampered with. Uninstalling such applications and replacing them with authentic software can bring uniformity and security, or whitelisting them will avoid the display of anomaly findings for all or present-day devices.



Posture Anomaly by Incidence

□	Application name	Application publisher	Device Count
□	Sophos SSL VPN Client 2.1	Unknown	23
□	Grammarly for Windows	Unknown	17
□	docker-desktop	No Information available	1
□	teams	No Information available	10
□	notion-desktop	No Information available	1

Showing results from 1 to 10 of 43 Records

Binocular View of your IT

Explore and learn about your environment in a way you hadn't seen before and be surprised with what you find. Some anomalies appear only when we observe trending data over several days.

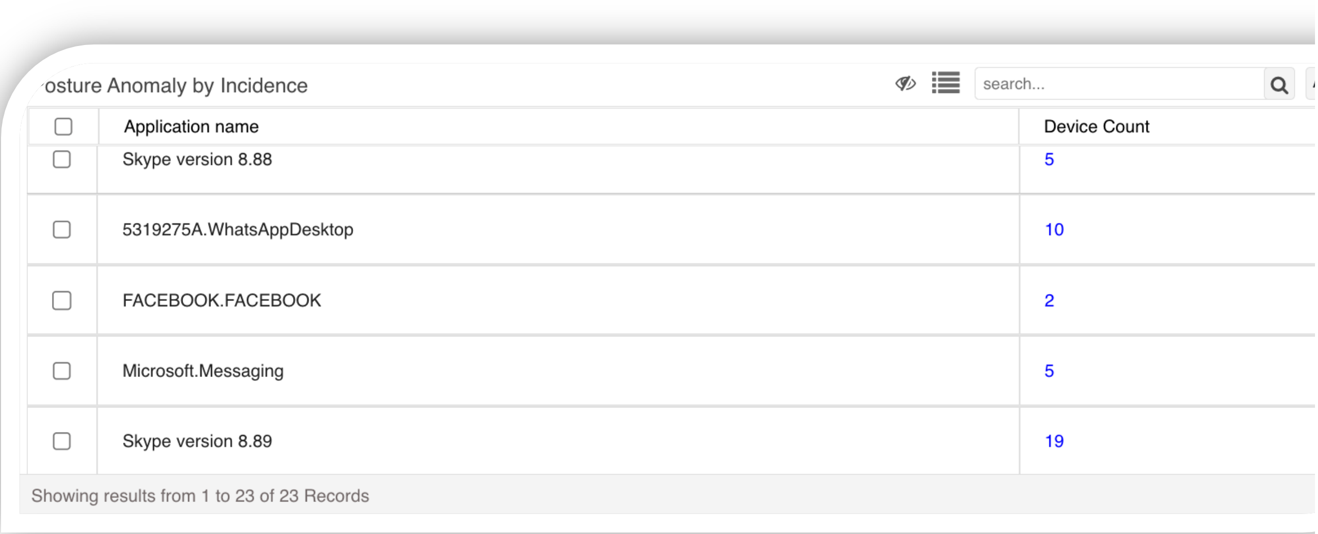
Track changes in IP addresses, Hostnames, and MAC addresses for accountability. Identify inactive users or the presence of different user privileges. Distinct Firewall configurations in a select few systems can be a point of trepidation.

Track your IP, Host, and MAC address change for accountability

A frequent change in the IP address of a device, even though lease duration and a comprehensive IP range are configured in the DHCP server, may indicate a shortage of more IP addresses. MAC address change implies a change in the network adapter, and host names seldom change frequently in an organization. Keeping such factors in mind, the anomalies are computed over trending data of 30 days.

Why is someone using so many collaboration client applications?

Too many collaboration and meeting applications are in use because of users' diverse inclinations toward what works best for them, especially in work-from-home scenarios. These applications are tedious to maintain, and simplifying the usage of such applications to a few would make it easier to manage.



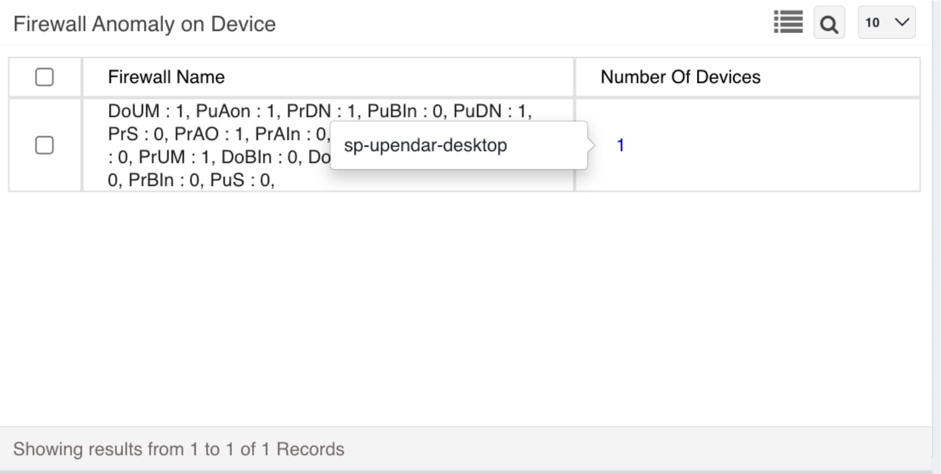
osture Anomaly by Incidence

□	Application name	Device Count
□	Skype version 8.88	5
□	5319275A.WhatsAppDesktop	10
□	FACEBOOK.FACEBOOK	2
□	Microsoft.Messaging	5
□	Skype version 8.89	19

Showing results from 1 to 23 of 23 Records

Why does someone have a unique firewall configuration that is so different from others?

Unexpected revelations of different firewalls configured in a group of systems completely deviating from the organization's standard can be concerning. A firewall plays a vital role in network security and must be properly configured to protect organizations from data leakage and cyberattacks.



Firewall Anomaly on Device

□	Firewall Name	Number Of Devices
□	DoUM : 1, PuAon : 1, PrDN : 1, PuBIn : 0, PuDN : 1, PrS : 0, PrAO : 1, PrAIn : 0, : 0, PrUM : 1, DoBIn : 0, Do 0, PrBIn : 0, PuS : 0,	1

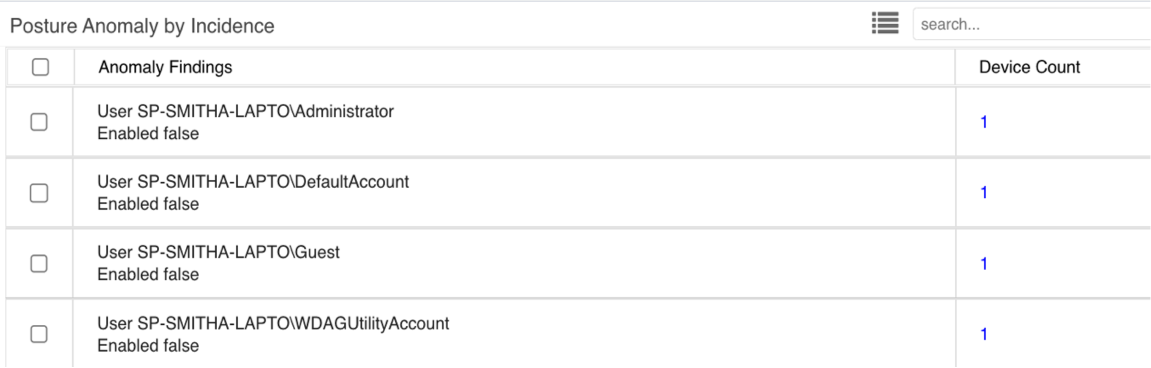
sp-upendar-desktop

Showing results from 1 to 1 of 1 Records

Inactive users or the presence of different user privileges

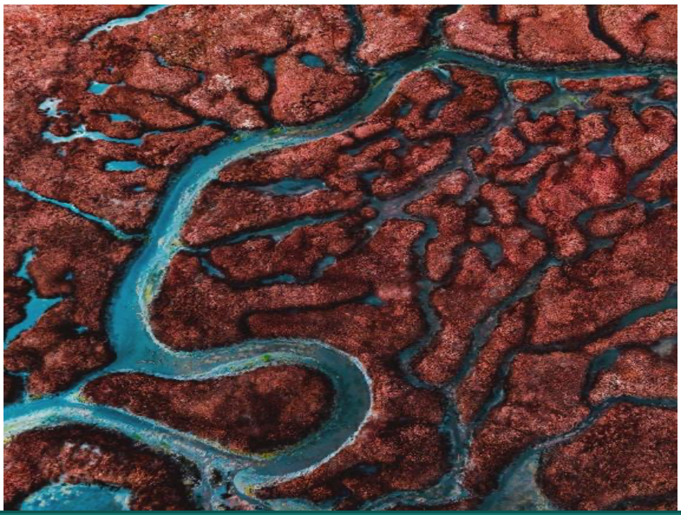
Expired login usernames expired exist with outdated permissions. Employees who have left the organization may still have access to systems. Excessive users with elevated privileges are present in the system. Users with no password, anonymous/default users, or guest logons are present in the system. All these scenarios can lead to unauthorized access and privilege escalation attacks.

This below table shows users that are disabled and can be removed if no longer in use.



Posture Anomaly by Incidence

□	Anomaly Findings	Device Count
□	User SP-SMITHA-LAPTO\Administrator Enabled false	1
□	User SP-SMITHA-LAPTO\DefaultAccount Enabled false	1
□	User SP-SMITHA-LAPTO\Guest Enabled false	1
□	User SP-SMITHA-LAPTO\WDAGUtilityAccount Enabled false	1



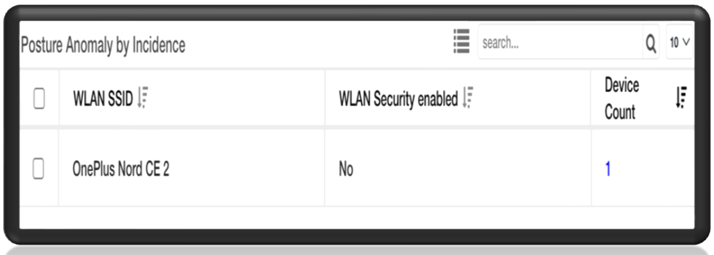
PA looks at 100s of device artifacts collectively across devices to uncover posture anomalies that are helpful to know and ensure particular hygiene is maintained across all devices.

Monitor Security Controls Deviations

Discover if the configuration has changed on several devices or if settings deviate from the standard format. Typical security settings include a secure Wi-Fi configuration, user and group settings, login configuration, Bit locker settings, System DEP Policies, ASLR settings, SE Linux flag, Gatekeeper settings, UEFI Boot option, Time Synchronization with NTP server, Device Shares, etc.

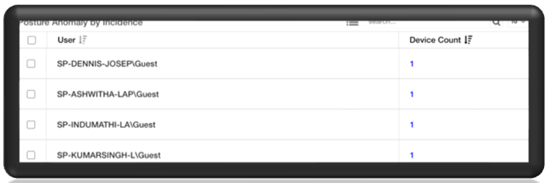
Is Endpoint protection software functioning?

- Is Wi-Fi security configuration analyzed and strengthened?
- Is Wi-Fi security disabled?
- Is Wi-Fi Encryption disabled?
- Is he Authentication algorithm not set?
- Is SSID discoverable?



Posture Anomaly by Incidence

□	WLAN SSID	WLAN Security enabled	Device Count
□	OnePlus Nord CE 2	No	1



Posture Anomaly by Incidence

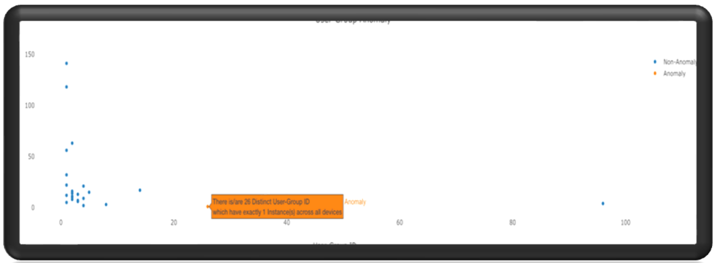
□	User	Device Count
□	SP-DENNIS-JOSEP\Guest	1
□	SP-ASHWITHA-LAP\Guest	1
□	SP-INDUMATHI-LA\Guest	1
□	SP-KUMARSINGH-L\Guest	1

Verify User identity is configured appropriately

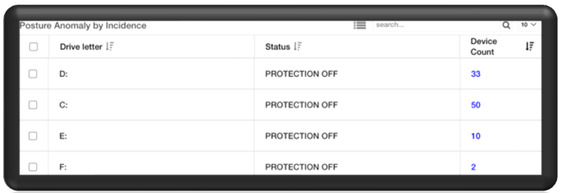
- Users with empty passwords?
- Are Guest logins enabled?
- Is UAC disabled?
- Anonymous login enabled?
- Are Inactive users present?

Conflicting UID/GID

We are identifying anomalous UID GID setting in the devices. UID is a number associated with a user account and GID is a number associated with a group in an operating system. This process involves data collection, transformation, clustering, tuning, and alerting based on the lower bound.



There is/are 26 Distinct User-Group ID which have exactly 1 Instance(s) across all devices



Posture Anomaly by Incidence

□	Drive letter	Status	Device Count
□	D:	PROTECTION OFF	33
□	C:	PROTECTION OFF	50
□	E:	PROTECTION OFF	10
□	F:	PROTECTION OFF	2

Is BitLocker/ KeyChain disabled?

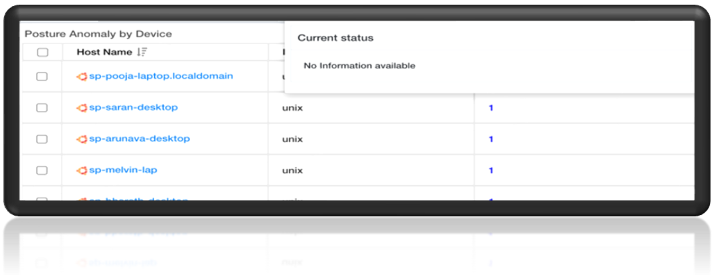
- Discovering Bit Locker status in the system. BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.
- Detecting Keychain configured in the system. Keychain access is a macOS app that stores your passwords and accounts information and reduces the number of passwords you must remember and manage.

DEP/ ASLR/ SELinux enabled for threat protection?

- Identifying System DEP policies in the system. Data Execution Prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help protect against malicious code exploits.

- Detecting ASLR configuration in the system. Address space layout randomization (ASLR) is a technique that is used to increase the difficulty of performing a buffer overflow attack that requires the attacker to know the location of an executable in memory.

- SELinux defines access controls for system applications, processes, and files. It uses security policies, which are a set of rules that tell SELinux what can or can't be accessed, to enforce the access allowed by a policy.



Posture Anomaly by Device

Current status

No Information available

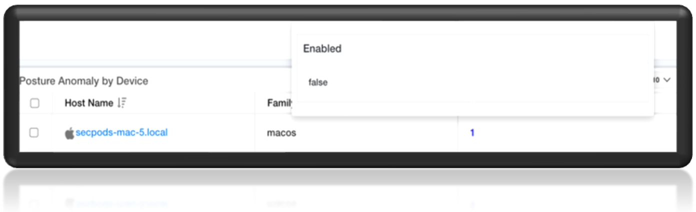
□	Host Name		
□	sp-pooja-laptop.localdomain		
□	sp-saran-desktop	unix	1
□	sp-arunava-desktop	unix	1
□	sp-melvin-lap	unix	1

Summary

- OS family **unix** has the highest number of anomalies, with a total of **18**.
- The group **ubuntu** has the highest number of anomalies, with a total of **16**.

Gatekeeper enabled

Detecting Gatekeeper configured in the system. macOS includes a security technology called Gatekeeper, which is designed to help ensure that only trusted software runs on a user's Mac.

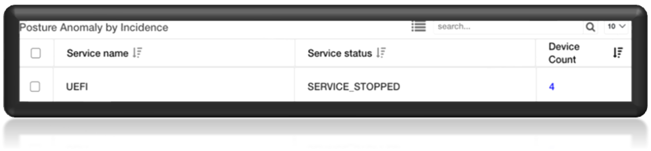


Posture Anomaly by Device

Enabled

false

□	Host Name	Famil	
□	secpods-mac-5.local	macos	1



Posture Anomaly by Incidence

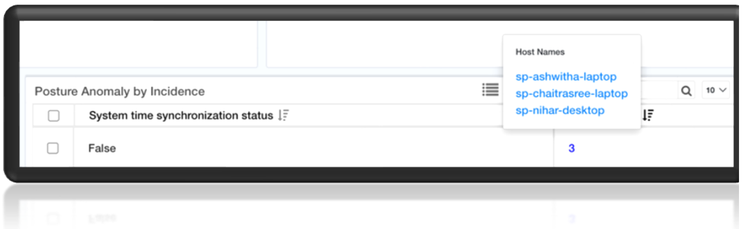
□	Service name	Service status	Device Count
□	UEFI	SERVICE_STOPPED	4

UEFI boot enabled

Checks whether BIOS is not running in UEFI mode. BIOS settings should be in UEFI mode, and Secure boot enabled

Time synchronization issue is detected

We detect if the system time is not synchronized with the server using Network Time Protocol(NTP). Time synchronization is critical because managing, securing, planning, and debugging a network involves determining when events happen. Time also provides the only frame of reference between all devices on the web.



Posture Anomaly by Incidence

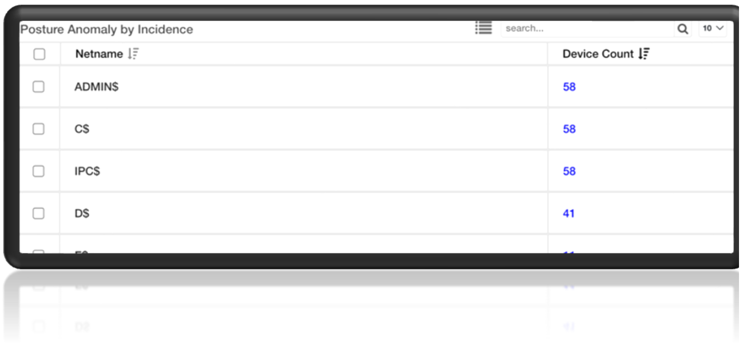
Host Names

sp-ashwitha-laptop
sp-chaitrasree-laptop
sp-nihar-desktop

□	System time synchronization status	
□	False	3

Device shares are determined

We detect if devices have resources on a local network that others can access. A network share is a folder on a PC, Mac, or server. Insider threats are responsible for almost two-thirds of all data breaches. By sharing a device with other people, identifying the insider threat that caused the cybersecurity problem becomes infinitely harder.



Posture Anomaly by Incidence

□	Netname	Device Count
□	ADMIN$	58
□	C$	58
□	IPC$	58
□	D$	41

The Value of Implementing Continuous Posture Anomaly Management

In the business world, we rarely want things out of order; the faster we can detect anomalies and mitigate them, the quicker we can prevent cyberattacks. We provide insightful data and the means to fix the deviations to speed up your security administration.

This process will remove uncertainty and get fresh perspective on your IT infrastructure. Users can be ensured that the security controls are configured and functioning well. With a streamlined IT and Security Management with CPAM, reduce your attack surface, work well with a known-good IT environment by whitelisting and eliminating the unnecessary. Get a binocular view and be surprised!

The Pain Points of IT and Security Management

There needs to be deeper visibility, and administrators spend hours building visibility in the IT environment. Technology clutter due to numerous user preferences is inevitable. Managing a diverse environment is challenging to comprehend with too much data and no security insight to contextualize it. Cyberattacks continue to occur, exploiting the most obvious attack vectors; low-hanging fruits. High investment in low-yielding solutions is of no value to the organization.

With Continuous Posture Anomaly Management, gain quick security mileage by implementing the most prominent security hygiene measures, improve operational efficiency with comprehensive and insightful intelligence, remove uncertainty and gain confidence in your IT security measures.

Continuous Posture Anomaly Management

Email us at info@secpod.com