



CONTINUOUS POSTURE ANOMALY MANAGEMENT

TECHNICAL INSIGHTS

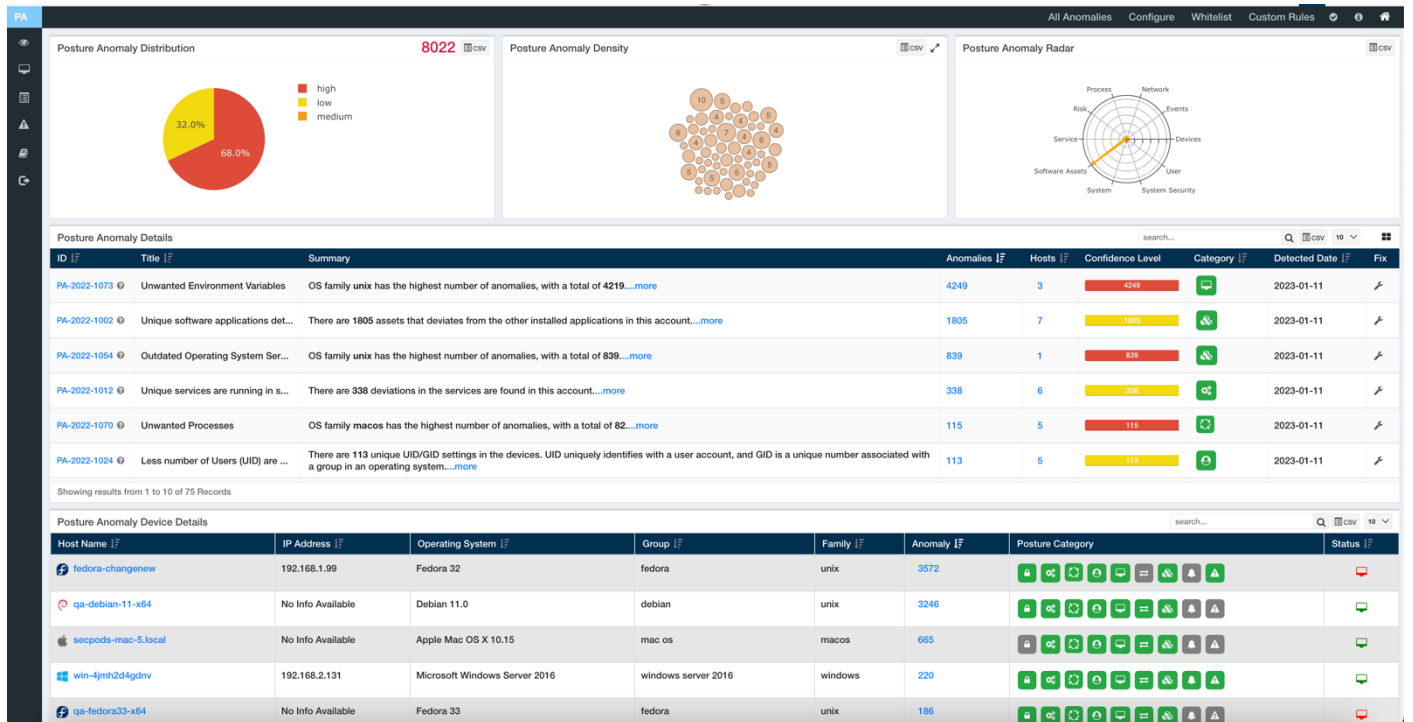
OVERVIEW

In every targeted attack, a weakness is exploited. These weaknesses are loopholes attackers exploit to gain unauthorized access to a target environment through authorized channels. A weakness can be a software vulnerability, hardware driver vulnerability, a misconfiguration, not having a critical patch, an asset exposure where unwanted applications are installed, deviations in security controls, or **Posture Anomaly**. These are equally important and must be dealt with in equal measures. Mitigating these will help organizations setup an impenetrable security posture.

Posture Anomalies (PA) are outliers and deviations present in devices against known-good. These anomalies are either statistically determined, machine learning computed, or deviations derived from security best practices. An unusual service or application installed on only a few systems that is analytically determined out of all device artifacts or weak Wi-Fi security strength, or an unapproved task scheduled to run are some of the examples.

Continuous Posture Anomaly Management (CPAM) assesses deviations based on statistical algorithms, rule-based outlier detection, and anomalies in data trends and monitors security control deviations. CPAM looks at 100s of device artifacts collectively across devices to uncover posture anomalies that are helpful to know and ensure hygiene is maintained across all devices.

A dashboard lists all anomalies in the devices, categorizes the anomalies based on confidence, and provides an instant fix to remove or white-list the rarities that are acceptable in the organization.



The dashboard of Continuous Posture Anomaly Management

PROBLEMS AND CHALLENGES

Continuous Posture Anomaly Management helps solve the pain points of CISOs, IT, and Security Administrators. Some of the issues are listed below,

- ▶ Lack of deep visibility. One must spend hours to build visibility in IT environment
- ▶ Technology clutter that is not streamlined
- ▶ Managing a diverse environment with ease that we cannot comprehend and visualize is a prerequisite for securing an organization.
- ▶ Too much data; security contextualizing and insights are not available.
- ▶ Unsure if device security controls are functioning
- ▶ Cyberattacks continue to exploit the most obvious attack vectors, often known as the low-hanging fruits.
- ▶ Unrealized investment in cyber security technology, high investment in low-yielding solutions.
- ▶ The post-attack analysis points to the most apparent attack entry point.

WHAT IS CONTINUOUS POSTURE ANOMALY MANAGEMENT?

When you have 100s or 1000s of systems in your environment, you are blindsided, not knowing if all the systems are configured certain way, and if all the systems are behaving certain way.

Every security tool whether prevention or detection based, they always look at security from an individual system point of view, they never look at the entire IT systems collectively as one entity and analyze the deviations. If you look at organization's computers, there will be commonalities across system, common security policies, common security controls, application policy, device control policy, common security products and protocols, common behavioral traits. Not having visibility to deviations against an acceptable commonality is a problem. These outliers will help us understand the IT infrastructure holistically and act against anomalies if they are exposure to a potential threat.

It is important to ensure only authorized or approved security controls and hygiene measures are implemented throughout the organization's IT systems. Across all the systems, getting visibility to what is running on them, how the security controls are configured, are they staying as they were configured, is a critical need for ensuring an accepted baseline. Any deviations to the approved measures must be marked as anomalies and dealt with. Appropriate actions must be applied to remove the anomaly for better cyber hygiene.

Cyberattacks occur because of so many foundational hygiene measures are not implemented and we do not understand our IT environment deeply enough. The starting of every attack is reconnaissance where attackers are studying the target environment and building attack vector map. The attackers will always look at the easiest form of attack tactic. Most often than not, they succeed using these tactics. The reason being, organizations today do not understand their environment deeply enough.

- ▶ Do you understand your environment deeply enough to know what is in it and what is not?
- ▶ Are there unnecessary IT? Unwanted installations and configurations?
- ▶ Are there outlier systems, and outlier configurations?
- ▶ Are basic security controls deployed? Are deployed security controls functioning well?
- ▶ How are these systems interacting with each other?

Attackers use the most obvious and simple techniques that give them maximum results. An attack occurred because,

- ▶ Anonymous logins, guest logins, default credentials
- ▶ Insecure network port widely open
- ▶ Unapproved software
- ▶ Unapproved VPN software is in use, gaming applications, cloud file sharing apps installed
- ▶ Insecure permissions
- ▶ Publicly discoverable data shares
- ▶ User access control is bypassed

The goal of Continuous Posture Anomaly Management (CPAM) is to discover risk exposures that are so fundamental to cyber-attack prevention journey which when implemented give maximum protection.

DATA SET FROM DEVICES

There are 100+ data collection points for Microsoft Windows, many Linux flavours and Mac machines with a total of 2000+ attributes for each category of probe. Here are some of the supported checks listed below,

ARP Cache	Access Token	Active Directory Entries	Alpine System Package Information	Antivirus Information	Authorization Database	AppArmor Status	Audit Event Policy	Audit Event Policy Subcategories
Auto Logon, Last logon, Last Reboot	Account Lockout Policy	BIOS Information	Bit Locker Information	Boot Priority	CCE Information	CPE Information	CVE Information	Computer Information
Connected MAC Address	Core Storage	Cron	DHCP Information	DNS Cache	DNS Information	DPKG Information	Device Information	Disk Encryption Information
Disk Utility	Environment Variables	Etc Host Information	Etc Protocol Information	Etc Protocols Information	Etc Service Information	Windows Events	Family of Operating Systems	File
File Extended Attributes	File Audit Permissions	File Effective Rights	Firewall Information	Foreign Addresses and Ports	GateKeeper	Group Information	Group SID	Grub Config
Health - CPU and RAM Usage	IP Forwarding Status	IP Table Rules	Interface Listener	Inet Listening Servers	Installed Application	Installed Patches	Network Interfaces	Junction
Kernel Information	Kernel Modules	Keychain	LaunchD Information	Local Ports	Lockout Policy	Logged-In Users	Logon Information	Missing Patches
Mount Points	NT User	NVRam Information	Network devices	Operating System Information	Package Information	Partitions	Password/ User Information	Password Policy
PE header	Ports/Network Information	Printer Effective Rights	Process	Pfctl Information	Property List (plist)	Registry	Registry Key Audit Permissions	Registry Key Effective Rights
RLimit Information	RPC Map Information	RPC Net Connection Information	RPM Information	RPM File verify	RPM Verify Package	Routing Table	Run Command History	Run Level Information
Running Process	Scheduled Programs	SELinux Boolean Information	SID	SID SID	Service	Service Information	Shadow file	Shared Resources
Shell History	Software License Information	Sudo Users	SUID Bin Binary	SUID bin file	Symlink	Sysctl	System ASLR Status	System Autorun Information
System Control	System DEP Policy	System DHCP	System DNS	System Exec Shield Status	System Metric	System Restore	System Route Information	System Profiler
System Setup	System Time	System UAC Policy	System Route Information	Systemd Property	Text File Content	Task Scheduler Information	Uname Information	User Access Control
User	User rights	Users SID	Vmstat Information	Volumes	XML File Content	WSUS and SCCM	Wireless Information	WMI
				WSUS SCCM Information	WUA Update Searcher			

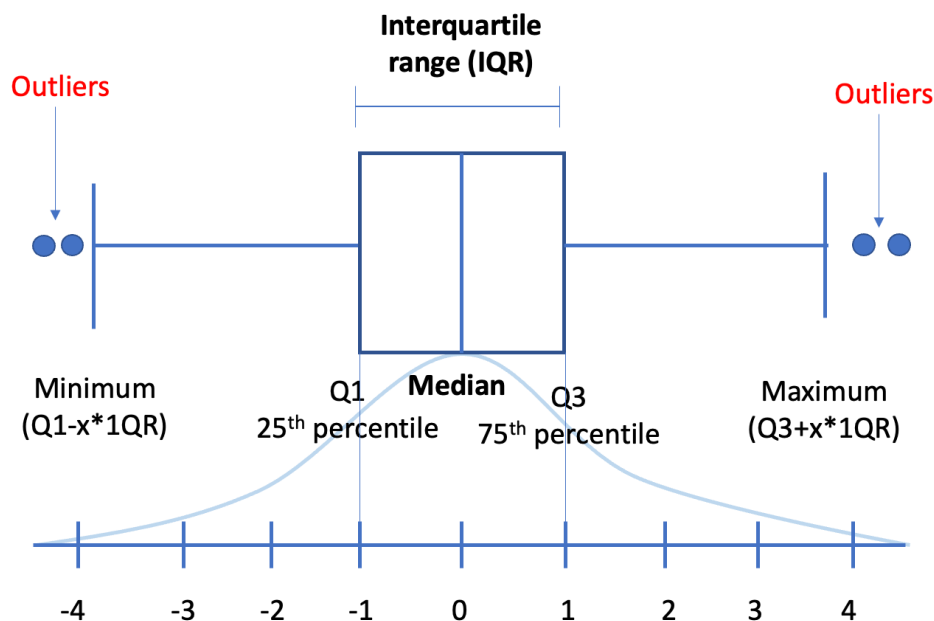
HOW IS POSTURE ANOMALY ANALYZED?

The process of finding anomalies or deviations in the device information collected through numerous probes in the operating system, in-built feeds, rules, and security detections through clustering and defining outliers by mathematically crafting an allowed threshold based on the number of devices in an account.

OUTLIER DETECTION USING INTERQUARTILE RANGE

We collect 1000+ objects from all the devices in the organization. Each of these objects is clustered from different devices and observed collectively.

A frequency distribution is computed on each finding. This distribution has median(Q2), Q1(25th percentile) and Q3(75th percentile). Interquartile range referred to as $IQR = Q3 - Q1$. Anything less than $Q1 - x * IQR$ or greater than $Q1 + x * IQR$ will be considered an outlier. The more the value of x , the more serious the outlier, the more that value **should not be in the device data**. In this model we are considering outliers as anomalies. A lower value of x will be low confidence anomalies, x with intermediate value will be medium confidence anomalies, x with a upper value will be high confidence anomalies. These values might be changed as and when needed.



RULE BASED ANOMALY DETECTION

Device artifacts such as current network connections, vulnerabilities and misconfigurations and other security settings are collected on a daily basis. The Sigmoid symbolized as $S(x)$ function is applied on the dataset that performs the role of an activation function in machine learning which is used to add non-linearity in a machine learning model. Essentially, the function determines which value to pass as output and what not to pass as output.

Rule based anomaly detection techniques are applied on several attributes from devices such as Network Ports, Processes, ARP entries, DNS Cache, etc., to compute anomalies. The following representation summarises the calculations,

$$x(1 + (S(g(y))))$$

where, x is frequency of attributes and y represents risk properties that the attribute carries in the organization.

Another computation involves analysis of frequency of occurrence in a data dictionary and deriving confidence using,

$$\frac{Range(S)}{Min(S)} = \frac{Max(S) - Min(S)}{Min(S)}$$

where, S is the sample data.

DATA TREND BASED ANOMALY DETECTION

We collect some parameters from devices over a period, and if there is a discrepancy in those parameters, we term that particular parameter's instance as an Anomaly, e.g.: Hostname, MAC Address, IP Address, Number of Vulnerabilities based on the severity, and CCEs. A simple standard deviation mechanism helps determine confidence of anomaly findings.

$$\sigma = \sqrt{\frac{\sum (x_i - \mu)^2}{N}}$$

Now statistically, these variations should be Normally distributed, and any Normal Random Variable stays within X * standard deviation of mean, with a probability of 99.7%. Hence here also, any value that is more than X * standard deviation away from mean, is an outlier.



CONTINUOUSLY SCAN

Day-on-day discover anomalies in the organization




CONFIGURE SCANS

Configure allowed services, processes, ports, start up applications, to discover unwanted elements in the organization



FIX OR WHITELIST ANOMALIES

Fix anomalies using pre-built response schemes or whitelist accepted deviations bearing unique requirements that need to be adapted in the organization



KEY COMPONENTS OF CPAM FRAMEWORK

Posture Anomaly Scanner

Downloads consolidated device reports on a daily schedule and discovers anomalies in an account's set of devices. The scanner is the core of our data analytics system. A scanner downloads the latest device information and calculates and identifies deviations in device objects. It considers allowed values in the configuration and a set of whitelist values provided by the user to eliminate those observations in the anomaly calculation. Alternatively, the scanner modestly recalculates anomalies without downloading the entire device reports.

Posture Anomaly Trends and Reports

The trends and reports server subscribes to Posture Anomaly Scanner to download results and restructure and compute trending data for anomalies conception. It supports visualization with a UI framework to view anomalies and take action. It also provides intuitive configure, whitelist, and fix actions to mitigate anomalies in devices.

Posture Anomaly Database

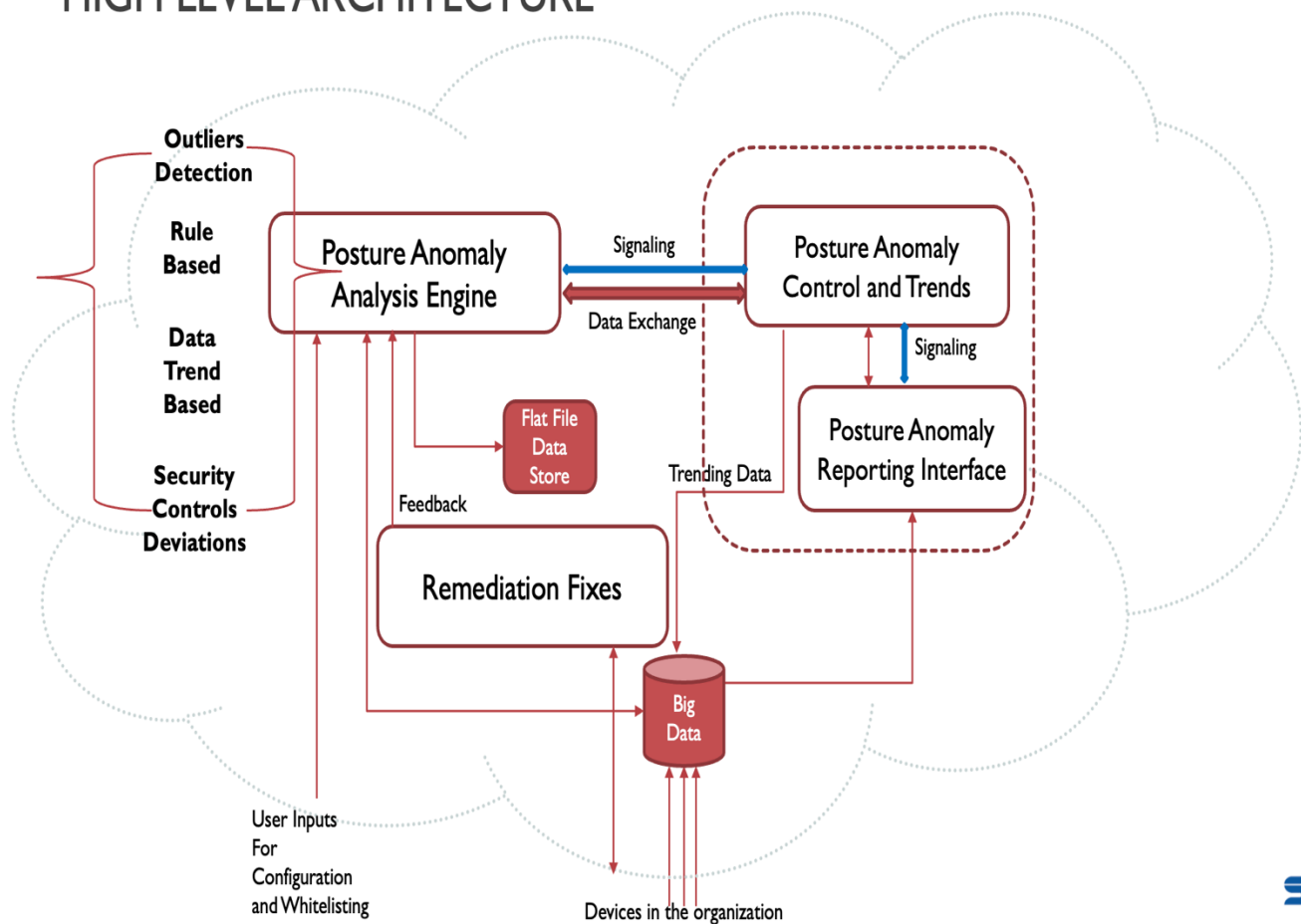
The database systems stores Posture Anomaly trends and anomaly data to report or show on user interface such as browsers.

Posture Anomaly File Data Store

Stores consolidated device reports for Posture Anomaly Scanner analytics.

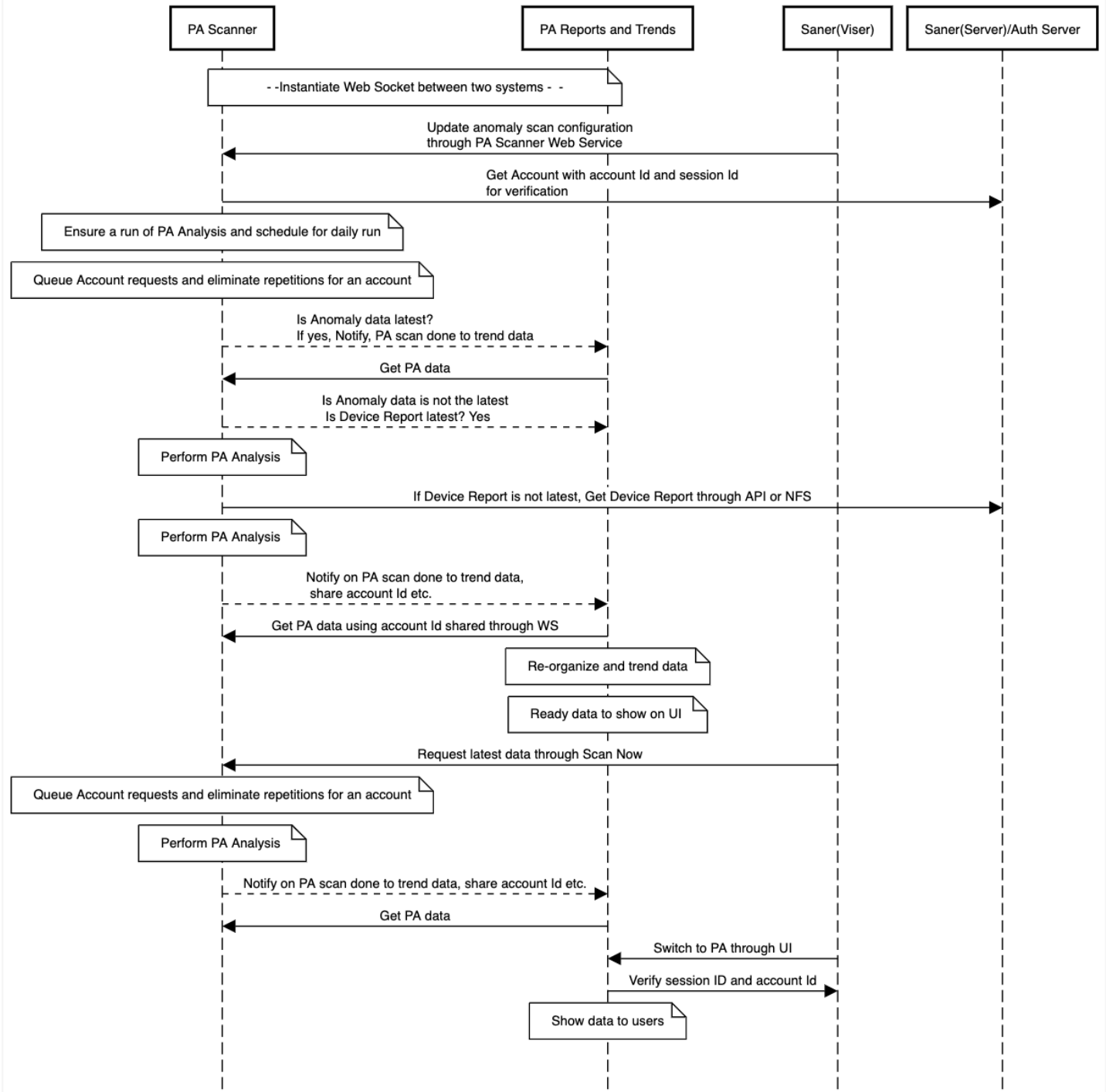
CONTINUOUS POSTURE ANOMALY MANAGEMENT ARCHITECTURE

HIGH LEVEL ARCHITECTURE



CONTROL AND DATA FLOW DIAGRAM

Posture Anomaly (PA) Instructions and Data Flow





PROMISED IMPACT

Users can get insightful data to understand anomalies in an organization, take action to mitigate them and create a security base line for an organization. In the business world, we rarely want things out of order, the faster we can detect anomalies and mitigate, the faster we are able to prevent cyberattacks.

Continuous Posture Anomaly helps remove uncertainty and get fresh perspective on your IT infrastructure CISOs, IT and Security administrators will be machine learn the IT environment by bringing order to your **diverse** IT environment, ensure security controls are configured and functioning well.

With a streamlined IT infrastructure, we can reduce your attack surface, work with a known-good assets in the IT environment by whitelisting and eliminating the unnecessary.

One can get a binocular view of their IT environment and be surprised.

Continuous Posture Anomaly Management
Email us at info@secpod.com