SECURONIX™ | windchill®

SOLUTION BRIEF

Securonix for PTC Windchill: Monitor Intellectual Property Theft and Misuse

The cyber security landscape continues to increase in complexity. Hackers continue to innovate, business technologies generate increasing amounts of data, and legacy perimeter defenses struggle with modern insider and cyberthreats.

Securonix Security Analytics Platform enables you to detect, investigate, and respond to cybersecurity threats in real time. Windchill is a product lifecycle management application used by companies for design and documentation collaboration. Securonix for Windchill allows you to perform security monitoring in order to detect and stop intellectual property theft and accidental data leakage.

The Securonix Security Analytics Platform combines log management, threat detection, and incident response into an end-to-end platform that can be deployed on-premises or in the cloud. It collects massive volumes of data in real time, applies entity context to it, uses patented machine learning algorithms to detect advanced threats, and provides actionable security intelligence for quick response.

Windchill is a product lifecycle management platform used by manufacturing and engineering companies to store and share information about assemblies, parts, and designs. It contains your sensitive intellectual property, and needs to be protected. However, it is also used for collaboration, so it must be accessible to many stakeholders including engineers, supply chain managers, suppliers, accountants, contractors, and more.

Out-of-the-box, Windchill offers role-based access capabilities, but security monitoring is largely a manual process. Legacy security information and event management (SIEM) and user and entity behavior analytics (UEBA) solutions cannot handle application-specific security monitoring

Integration Benefits

- Prevent intellectual property theft
- Detect accidental data leakage
- Provide effective security monitoring

Fully Integrated Security

Securonix Security Monitoring

- Using behavioral analytics, Securonix can detect a sudden spike in objects accessed by a user or when a user is accessing objects that are not normally accessed by others in the same peer group. These anomalies can potentially point to malicious users or users with compromised credentials.
- Changes to Windchill security labels can be innocent. However, if a user lowers to criticality of a security label, then starts sharing it with new users, it can be a potential data exfiltration situation.
- Access permissions to objects within Windchill may not align with the user's business role. Securonix analyzes access permissions, compares against their peers, and determines if users have the appropriate level of access.

Example Security Use Cases

- Monitor data exfiltration attempts and detect attempts at downloading or inappropriately sharing large amount of data.
- Monitor suspicious object sharing events. Discover instances where a user shares objects with a high-risk security label with somebody who doesn't need access to the object. Or, find instances when a high-risk object has been added to a low-risk project and was shared.
- Monitor suspicious copy and rename events. Discover instances where a user has renamed high-risk files to make them sound more innocuous or generic in an attempt to bypass controls.
- Monitor for anomalous permissions, such as an employee who has access to an excessive number of files.
- Cross-correlate Windchill data with HR and other data to identify employees who are a flight risk. Employees looking to leave can be at a higher risk for exfiltrating data.

How it Works

- Using API integration, Securonix is able to pull information directly from Windchill.
- Securonix uses machine learning and advanced behavioral analytics to detect anomalies in your data.
- Securonix applies contextual data about the user and object to prioritize threats.

About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000

14665 Midway Rd. Suite #100, Addison, TX 75001 | ©2018 Securonix