Coping with Permissive Rules

Permissive rules are a major firewall policy risk that may cause corporations to be open to cyber security threats. This is also one of the items in nearly all compliance checks like ISO27001 and PCI-DSS. Therefore, network security teams must deal with permissive rules to make them specific rules. However, this is not an easy process if done manually, since the premissive rules are first to be monitored for a period of time and an analysis be made afterwards. There must be a tool that make this done easily.

What is the mechanism to make permissive rules specific?

Opinnate solves this issue in an effective and optimum way.

By the aid of Opinnate collector module the rules that are permissive can easily be monitored for the duration period needed. After the specified duration period the IP addresses or services actually be used are found out. It becomes a rule creation process with the selected risk level afterwards.

Selectively collecting logs to optimize usage

Opinnate makes permissive rule monitoring in an optimum way. In its unique monitoring mechanism system will collect syslog messages from firewalls. In the meantime it selects just the needed syslog messages and starts storing them in the specified period. In this way, both system resource usages such as CPU and RAM and disk usage are lowered. NSPMs are not SIEM solutions to collect all syslog messages and with this mechanism Opinnate lower your IT spending.

Benefits

- No permissive rules
- Hardening firewall rules
- Being more secure
- Lower resource usage
- Lower disk usage