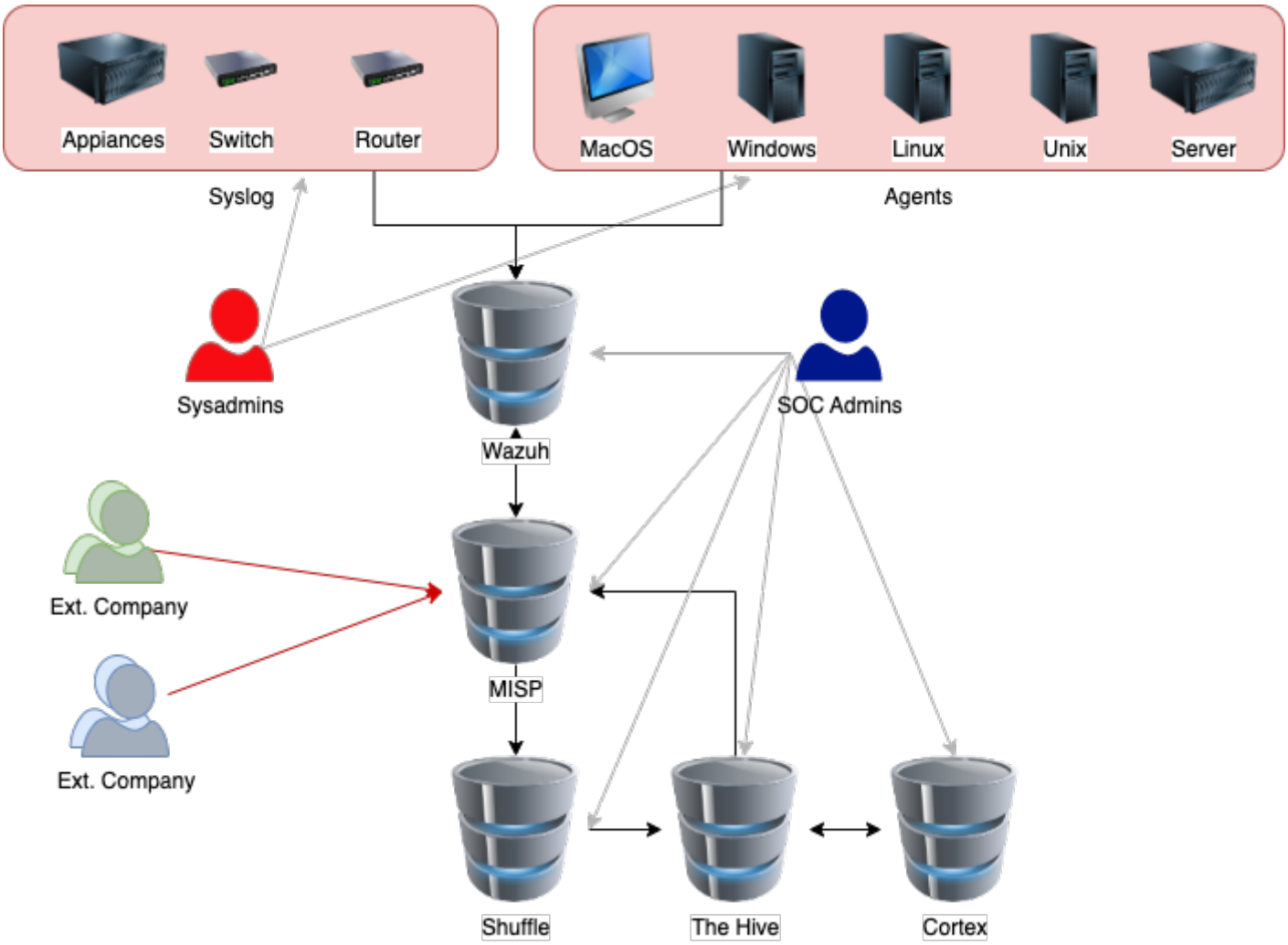
Möglicher Datenaustausch im FreeSOC

Der zentrale Datenbestand liegt im Wazuh - hier werden alle Daten hin geliefert. Hier benötigen Systemadministratoren und SOC Mitarbeiter Zugriffsrechte um ggf. Systeme hinzuzufügen oder zu entfernen.

Die Daten werden überwacht und zur weiteren Auswertung an MISP weitergegeben. MISP greift auf mehrere Datenquellen zu und kontrolliert ob diese bekannt sind. Wenn ja, dann wird ein IoC in Wazuh erstellt. Auf MISP benötigen Sicherheitsadministatoren und SOC Mitarbeiter Zugriff, damit diese MISP pflegen (Feeds/Quellen hinzufügen und ändern usw.).

Sollte ein IoC erstellt werden, wird Shuffle getriggert und ein Case in The Hive erstellt, Daten aus Wazuh geholt und mit in dem Case angereichert - mit diesen Daten werden diverse Analyzer in Cortex gestartet und alle Ergebnisse mit in den Case eingetragen. Auf The Hive und Cortex benötigen die SOC Mitarbeiter Zugriff.

Wurde das Ticket bearbeitet und abgeschlossen, kann dieses in MISP archiviert werden und ggf. mit anderen angebundenen Unternehmen geteilt werden.



Revision #4
Created 2022-12-27 20:16:33 UTC by Peter Leibling
Updated 2022-12-27 21:06:59 UTC by Peter Leibling