Einleitung

- Was ist überhaupt ein SOC
- Welche Produkte setzen wir in unserem FreeSOC ein
- Möglicher Datenaustausch im FreeSOC

Was ist überhaupt ein SOC

SOC ist die Abkürzung für Security Operation Center. Dies ist eine Zusammenfassung die aus mehreren Komponenten besteht:

- Mitarbeiter die Umgang mit IT Sicherheit geübt oder besser noch geschult sind
- Produkte für die IT Sicherheit
- Einen Raum (mindestns) der für diesen Zweck vorgesehen ist und entsprechend eingerichtet ist (z.B. mit mehreren Monitoren zur Überwachung

Die üblichen Aufgaben der Mitarbeiter umfassen:

- Überwachen der Infrastruktur
- Betreuen der Infrastruktur
- Updaten der Infrastruktur
- Schulen der Kolleginnen und Kollegen
- Überwachen und Betreuen der Clouddienste
- Überwachen und Betreuen der Internetanbindung

Welche Produkte setzen wir in unserem FreeSOC ein

Das von mir zusammengefügte SOC nenne ich FreeSOC, da es auf freie Open Source Produkten beruht - die Projektseite ist https://freesoc.de und derzeit noch im Aufbau.

Dies sind die folgenden:

- WAZUH
- MISP
- The Hive
- Cortex
- Shuffle

Die Zentrale Komponente ist dabei Wazuh - dies ist ein Open Source SIEM mit XDR Funktionalitäten. Alle Daten laufen erst in WAZUH zusammen, von dort werden diese ausgewertet und weiterverarbeitet. Angebunden werden, können dort:

- Windows Clients/Server
- MacOS Clients
- Linux/Unix Clients/Server
- Geräte wie Firewalls, Switches, Router, Telefonanlagen, VPN Gateway, Mailrelays und mehr mehr über Syslog

Weiterhin können auch folgende Zentrale Clouddienste überwacht werden, wie z.B.:

- Github
- Office/Microsoft 365 (und natürlich Azure)
- Google
- AWS

Die Agent überwacht folgendes:

- Vulnarability
- Compliance (PCI, GDPR usw.)
- Status mit Berichtserstellung
- Und noch vieles mehr

MISP ist eine zentrale Malware and Sharing Plattform, welche mehrere Feeds anbieten mit vielen interessanten Informationen wie z.B.:

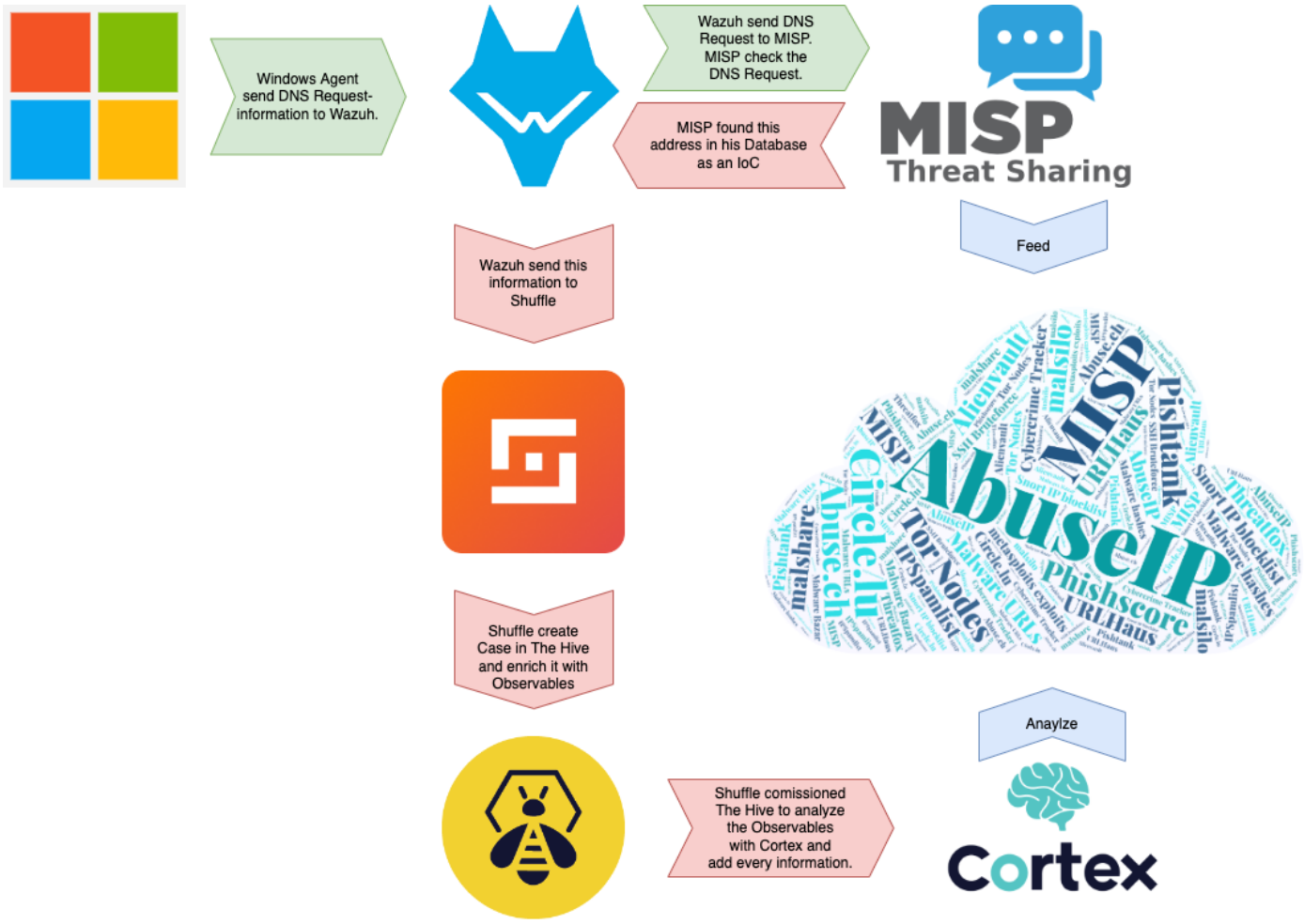
- Bad IP Adresses
- Spam Adressen
- Tor Exitnodes
- IoC wie URL, IP, Hashes, Dateinamen usw.
- Und vieles mehr

Hier werden die Datenbanken gepflegt, die uns unterstützen um z.B. IoC's zu finden.

The Hive ist ein SIRP, hier werden alle Informationen gemeldet und weiterverarbeitet. Mit Hilfe unserer automatisierungsplattform Shuffel sammeln wir alle IoCs ein und übergeben diese an Cortex, unserem Analyzer - der wieder rum nutzt mehrere Systeme wie MISP, Virustotal, AbuseIP usw. um dort Informationen zu sammeln und diese in dem Vorgang in The Hive anzureichern.

Nach der Bearbeitung können diese Vorgänge geschlossen und an MISP gegeben werden - um ggf. angebundenen Partnern zu Informieren.

Hier mal ein Beispiel vom gesamten Workflow:



Ein Beispiel wir unser SOC agiert seht ihr hier in dem Beispiel (leider erst mal nur in Englisch):

https://www.youtube.com/embed/hX5p9DQ3aBI?t=224s

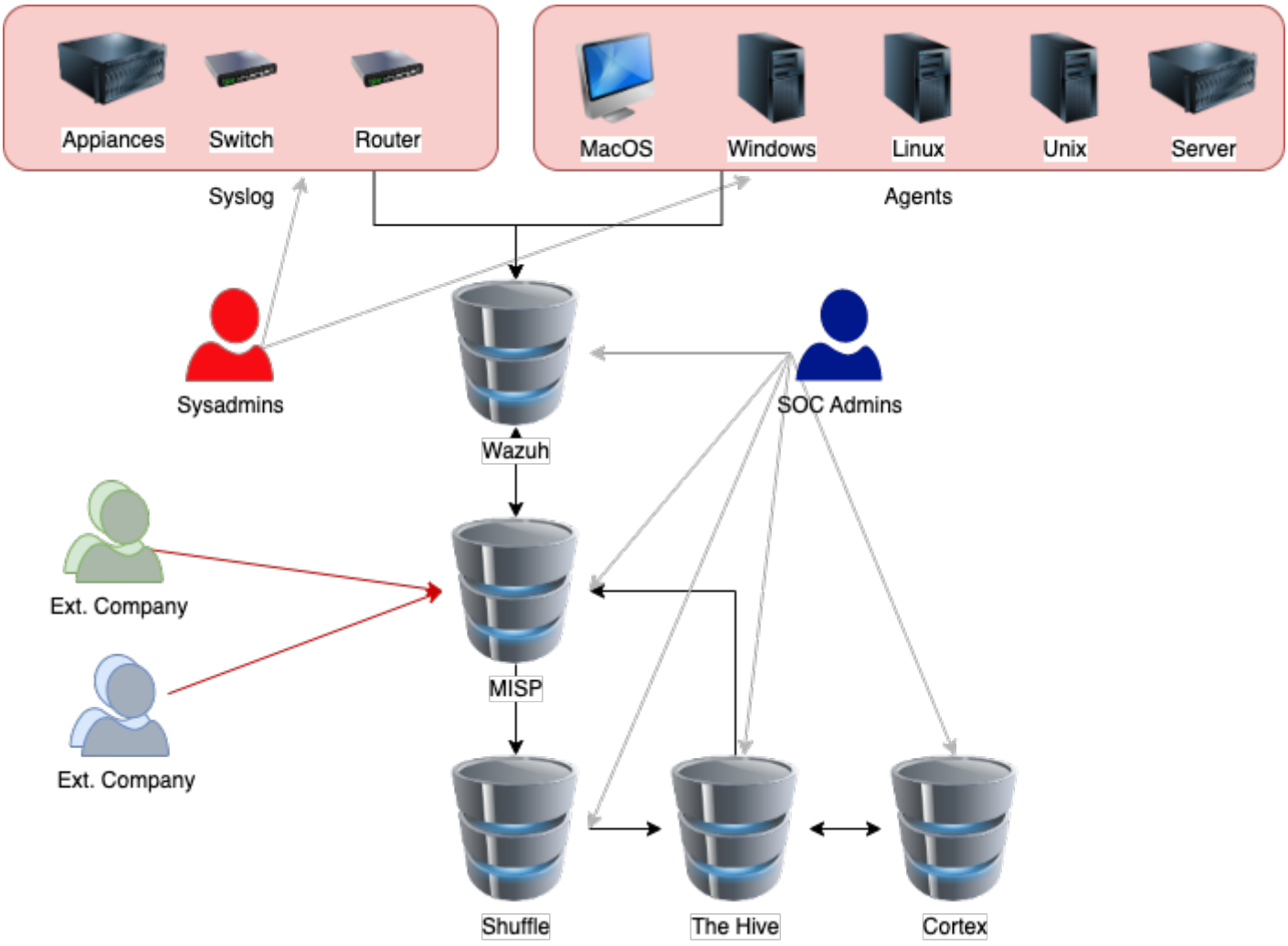
Möglicher Datenaustausch im FreeSOC

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.


Appiances
Switch
Router
MacOS
Windows
Linux
Unix
Server
Syslog
Agents
Sysadmins
SOC Admins
Wazuh
Ext. Company
MISP
Ext. Company
Shuffle
The Hive
Cortex