ENGINSIGHT

FEATURE-ROADMAP 2023

Feature mit Kurzbeschreibung
Zero Day Service für Schwachstellen (CVE) Wir implementieren automatische Benachrichtigungen über neue CVEs, die bereits ausgenutzt werden und vor denen öffentlich gewarnt wird. Über das User Interface ist dann direkt ersichtlich, welche Hosts oder Webseiten davon betroffen sind.
Defence pdf-Reporting Zum Defence-Modul führen wir einen pdf-Report ein der alle wesentlichen Aktivitäten zusammenfasst.
Automatische Konfiguration von Systemen Wir schaffen weitere Möglichkeiten, automatisierte Konfigurationseinstellungen für Server/Clients in Enginsight zu hinterlegen. Aktuell gelingt das manuelle Hinterlegen von Listen inkl. Beschreibungstext für Konfigurationseinstellungen. Konfigurationen sollen zudem komplett automatisiert werden und Nutzer sollen vorlagenbasiert (Powershell/bash/Python) systemeigene Konfigscripte erstellen. Eigenen Plugins können dann in einer Konfigliste zusammengefasst werden.
Verbesserung der User Experience für Defence Größere Organisationen gewinnen eine bessere Bedienbarkeit, mehr Transparenz und Übersicht.
Umstellung der User Interfaces auf React + Quality-of-Life-Verbesserungen Wir werden eine Ansicht nach der anderen von Amber auf React umstellen. Mit der Umstellung erhalten vor allem umfassende Sortier- und Filterfunktionen Einzug.
Überwachung des Pulsar-Zustands durch einen Supervisor-Dienst Mit einem zusätzlichen Dienst soll die Funktionsweise des Pulsar-Agents überwacht werden.
Tray-Icon zur Anzeige vom Pulsar-Status Auf allen Endgeräten, auf denen ein Pulsar-Agent läuft, wird es möglich sein, ein Tray-Icon einzublenden, welches Auskunft über den aktuellen Status und die Aktivitäten des Pulsar gibt. Weiterhin können verschiedene Funktionen direkt über das Icon getriggert werden.
MacOS-Support durch den Pulsar-Agent Der Pulsar kann zukünftig auf MacOS installiert werden.
Erweiterung der Webanalysen und des Reportings für Webseiten Der Observer findet künftig alle Subdomains und Breach-Events in der Vergangenheit à la Shodan und stellt die Veränderungen aller Findings dar. Berichte werden überarbeitet inklusive Risk Scoring und gelingen automatisiert inkl. einer Beschreibung, wie die Analysen zustandekommen.
Syslog-Server-Anbindung Mit der Schaffung eines Syslog-Servers, der alle Logs innerhalb einer IT inkl. Cloudanwendungen erfassen und auswerten kann, wird Enginsight zum SIEM.
NIDS-Version des Pulsar-Agents auf dedizierter Hardware Neben unserem hostbasierten Ansatz für IDS unterstützen wir künftig auch den netzwerkbasierten Ansatz. Dafür wird es in der UI einen eigenen Bereich geben, über den die NIDS-Sensoren ausgerollt werden.
Backend-App zur Administration der Enginsight-Instanz Über die Backend-App mit separatem Login werden im ersten Schritt die Nutzer:innen einzelner Mandaten verwaltet werden können.
Redesign des User Interfaces und der Berichte für Hacktor Das UI zum Hacktor-Audit wird grundlegend überarbeitet und ausgebaut.
IDS/IPS SSL-Interception <> Apache/Nginx Ransomware und schadhafte Netzwerkkommunikation wird häufig über https verschlüsselt. Der Agent soll diese entschlüsseln, analysieren und weiterverschlüsseln können.
Netzwerk-Sniffing mit Hacktor (MITM) Hacktor soll als MITM (Man in the middle) Netzwerkverkehr mitschneiden, um etwa nach Credentials zu suchen, die dann für weitere Scans verwendet werden können.
Mikrosegmentierung in dynamischer Map Eine grafische Map wird Mikrosegmente visualisieren und die Möglichkeit bieten, daraus per Drag and Drop weitere Mikrosegmente anzulegen.
DNS-Blocking durch Pulsar Shield wird um Funktionen erweitert, um Schutz vor Crypto Mining, Scam, Tracking und Telemetrics Blocking zu bieten.