sycope

Under control now and tomorrow

www.sycope.com

sycope

Sycope jest zaawansowanym rozwiązaniem, które rejestruje, przetwarza i analizuje wszystkie parametry zawarte w NetFlow i powiązanych z nim protokołach, wzbogaca je o dane SNMP, geolokalizację i edytowalne listy adresów IP.

System bezpieczeństwa został stworzony w oparciu o metodykę ATT&CK MITRE, a autorskie reguły i mechanizmy detekcji incydentów bezpieczeństwa umożliwiają wykrycie ataków i niepożądanych aktywności w sieci.

Rozkład ruchu sieciowego w oparciu o różne kryteria.

Jedno rozwiązanie do monitorowania wielu obszarów infrastruktury IT

Visibility

Moduł zapewnia pełny wgląd w działanie sieci IT, dzięki czemu menedżerowie IT mogą szybko podejmować decyzje dotyczące alokacji zasobów i działań zabezpieczających przed nieplanowanymi przestojami związanymi z awariami infrastruktury IT.

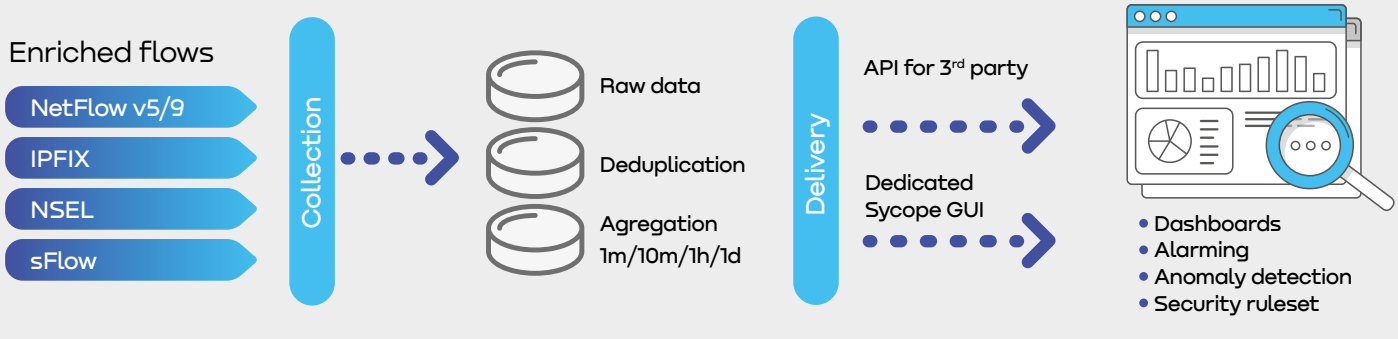
Performance

Moduł Performance posiada wbudowane mechanizmy do analizy warstw 4 - 7 sieci obejmujących restransmisje TCP, czas odpowiedzi klienta, czas odpowiedzi serwera, opóźnienia aplikacji, co pozwala diagnozować i eliminować problemy wydajnościowe.

Security

Moduł służący do wykrywania i analizy anomalii oraz zagrożeń bezpieczeństwa w kontekście całej organizacji. Zapewnia wsparcie w takich procesach jak Network Forensics, wykrywanie i obsługa incydentów i cyberzagrożeń, czy Threat Hunting. Zwiększa widoczność zagrożeń dla bezpieczeństwa na poziomie całej organizacji. Zbudowany na bazie metodyki ATT&CK MITRE, umożliwiając zespołom bezpieczeństwa łatwe zrozumienie wykrytych zagrożeń.

System dający odpowiedzi na Twoje pytania



“System gotowy do pracy w jeden dzień – nie jest standardem. Byliśmy mile zaskoczeni łatwością instalacji i integracji Sycope z naszymi innymi systemami”

Artur Wójcik
Narodowy Instytut Onkologii w Gliwicach

Co robimy inaczej

Operacje out-of-the-box

Funkcje dostępne „z pudełka” obejmują:

- szereg dashboardów zapewniających widoczność, wydajność i bezpieczeństwo,
- aktualne feedy bezpieczeństwa i zestawy reguł,
- funkcje alarmowania i raportowania,
- obsługę wielu protokołów netflow, w tym niestandardowych pól (tryb wykrywania),

natomiast rozwiązanie można w bardzo szerokim zakresie dostosować do własnych potrzeb

Przeszukiwanie i analiza danych z wykorzystaniem mechanizmów big data

Możliwosc szybkiego filtrowania dowolnych danych, z dowolnego źródła, według dowolnego pola, przy użyciu dowolnej wartości i dla dowolnego pulpitu nawigacyjnego

Niestandardowe dashboardy

Korzystając z trybu prostego lub zaawansowanego, możesz stworzyć dowolny pulpit nawigacyjny:

- możliwość tworzenia własnych widgetów lub dashboardów,
- możliwość ustawiania elastycznych zakresów czasowych dla widgetów,
- widoki prywatne i współdzielone,
- intuicyjne menu kontekstowe.

Prezentacja najważniejszych pararametrów w module performance.

Dashboardy ze wskaźnikami KPI ułatwiają proces codziennego monitorowania trendów zagrożeń bezpieczeństwa.

Deduplikacja danych

Sycope, w przypadku pozyskania duplikatu flowów z kilku źródeł, deduplikuje dane, zachowując jedynie unikalny wpis. Mechanizm deduplikacji pozwala m.in. na:

- prezentację rzeczywistych wartości o wielkości ruchu niezależnie od zastosowanych filtrów,
- wyświetlanie ścieżki w oparciu o pola NetFlow otrzymane dla tej samej transmisji z wielu routerów.

Wygodne przejście od ogółu do szczegółu – jednym kliknięciem

Funkcja drill down pozwala jednym kliknięciem zaprezentować dane dotyczące pojedynczego portu, interfejsu lub numeru IP.

Wykrywanie, analiza i mitygacja zagrożeń

Sycope w sposób ciągły analizuje dane, aby wykrywać zagrożenia w Twojej sieci i pomagać w rozwiązywaniu problemów związanych z bezpieczeństwem.

MITRE ATT&CK

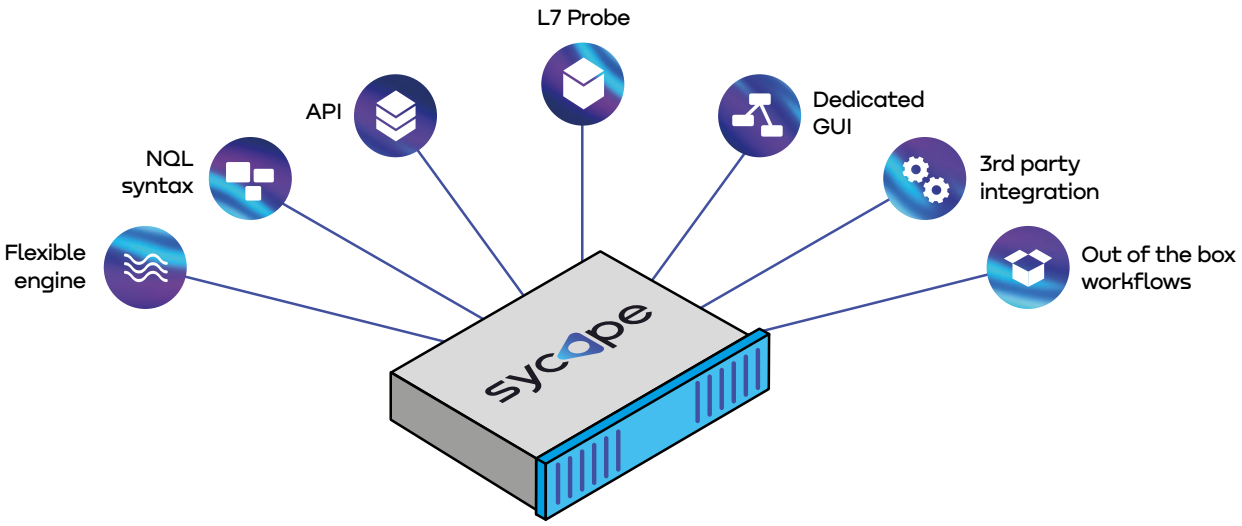
Zastosowanie metodyki MITRE ATT&CK umożliwia:

- analizę sekwencji zdarzeń,
- ocenę wpływu ataku na infrastrukturę IT.

Scenariusze dedykowane dla Network i Security Operating Center

Wszystkie ważne informacje dostępne są w ramach jednego widoku, aby łatwiej i szybciej zidentyfikować problemy i zagrożenia.

Sycope – w skrócie



Elastyczny silnik

Funkcje takie jak wysokowydajna baza danych, obsługa różnych wersji protokołu netflow, wbudowana deduplikacja 2.0, tryb wykrywania niestandardowych danych, umożliwiają łatwe tworzenie i wsparcie dla źródeł danych innych niż przepływy sieciowe.

NQL

Własny język zapytań dostosowany do sposobu wykorzystania systemu monitorowania, zapewnia wysoką wydajność pozyskiwania dokładnych danych, pozwala na tworzenie i obliczanie dowolnych nowych metryk (również przez użytkownika).

API

Umożliwia integrację systemu Sycope z własnymi rozwiązaniami (np. systemem Servicedesk), a także tworzenie dodatkowych lub niestandardowych dashboardów.

Integracja z rozwiązaniami firm trzecich

Możliwość wykorzystania API, powiadomień wieloprotokołowych i wbudowanej integracji z NAC

Out-of-the-box workflows

Wybór gotowych przepływów pracy dla wielu przypadków użycia, dedykowanych dla zespołów NOC/SOC, analiz śledczych (forensic) i raportowania biznesowego.

Sonda L7

Żadna aplikacja się nie ukryje. Detekcja aplikacji w warstwie 7 wraz z pomiarem czasu odpowiedzi.

sycope

Sycope specjalizuje się w projektowaniu i wdrażaniu wysoko specjalizowanych rozwiązań informatycznych z zakresu monitorowania i poprawy wydajności sieci i aplikacji oraz bezpieczeństwa IT. Nasze rozwiązania zostały stworzone i opracowane przez inżynierów, z ponad 20 letnim doświadczeniem w pracy z zagadnieniami wydajności sieci, wydajności aplikacji i bezpieczeństwa IT. Korzystając z rozwiązań światowych dostawców APM/NPM i SIEM zrealizowali ponad 400 projektów.

www.sycope.com
contact@sycope.com

Warsaw, Poland
Goraszewska 19
02-910 Warsaw

Prague, Czech Republic
Freyova 12/1
190 00 Praha