Beschreibung der Anwendungsmöglichkeiten zur Überwachung der IT-Infrastruktur auf Grundlage des Netzwerkflusses - Sycope FlowControl

Kunde	Das Nationale Institut für Onkologie "Maria Skłodowska-Curie" Staatliches Forschungsinstitut in Gliwice, Polen
Vorbagen:	Implementierung eines Tools zur Analyse des Netzwerkverkehrs und zur Erkennung von Bedrohungen unter Verwendung des NetFlow-Protokolls. Das Tool sollte eine umfassende Analyse der Netzwerkinfrastruktur sowohl auf allgemeiner als auch auf detaillierter Ebene ermöglichen, dabei skalierbar sein und eine einfache Integration mit Produkten von Drittanbietern ermöglichen.
Lösung:	Sycope FlowControl
Umsetzung:	Passus S.A

Sachlage

Das Nationale Institut für Onkologie „Maria Skłodowska-Curie" in Gliwice, gehört zu den führenden hochspezialisierten Klinik- und Forschungszentren in Polen. Es verfügt über eine moderne Ausstattung, ein erfahrenes Forschungsteam und arbeitet mit vielen Forschungseinrichtungen in Polen und dem Ausland zusammen. Gleichzeitig ist das Institut eines der größten onkologischen Zentren , das eine große Zahl von Patienten mit Krebserkrankungen behandelt und auch an der Durchführung von Master- und Doktorarbeiten mehrerer Universitäten beteiligt ist.

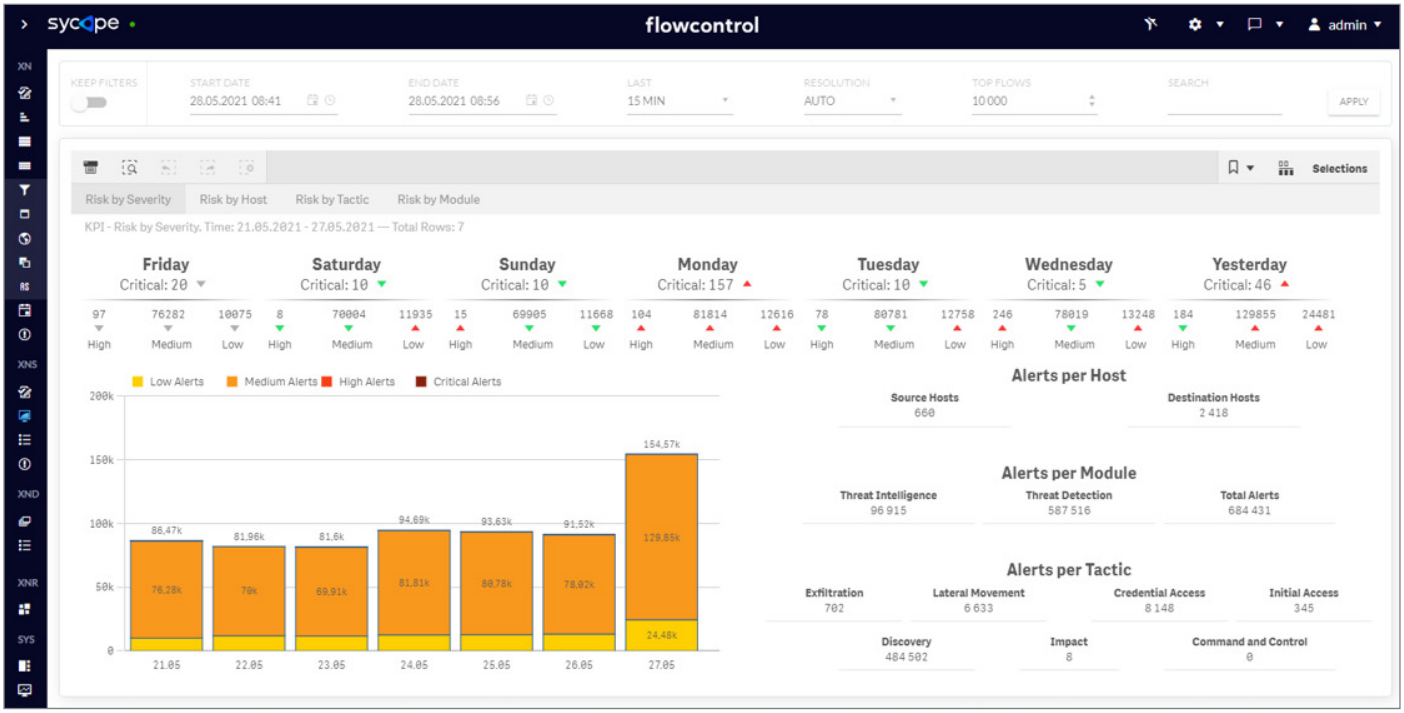
Die Abteilung des Instituts in Gliwice beschäftigt derzeit über 120 Mitarbeiter im Bereich Forschung und Entwicklung, darunter mehr als 30 Professoren und Habilitierte sowie mehr als 80 Mitarbeiter mit Doktortitel. Das hochqualifizierte wissenschaftliche Personal ist ein interdisziplinäres Team, das verschiedene wissenschaftliche Bereiche vertritt, u.a. Medizin wie klinische Onkologie, Chirurgie, Nuklearmedizin, Strahlentherapie, onkologische Endokrinologie sowie medizinische Biologie, Biotechnologie, medizinische Physik, Chemie, Bioinformatik und Epidemiologie.

Die IT-Infrastruktur des Nationalen Instituts für Onkologie besteht aus einem umfangreichen LAN-Netzwerk. Diese Infrastruktur unterstützt Anwendungen einer Multi-Layer-Architektur, die für den Betrieb des Instituts von zentraler Bedeutung sind, und gewährleistet den Datentransfer von medizinischen und diagnostischen Geräten wie Tomographen, Magnetresonanztomographen und PET-Geräten, deren Zahl jedes Jahr größer wird.. Dies bedeutet, dass zusätzlich zu dem für große Organisationen typischen Datenverkehr zusätzlich ein großer Datentransfer im Netz des Nationalen Instituts für Onkologie im Zusammenhang mit dem Austausch von radiologischen Bildern, einschließlich CT, MR, PET und Ultraschall stattfindet. Das Institut plant den kontinuierlichen Ausbau bestehender medizinischer Systeme, die die Übertragung von Bildern und multimedialen Inhalten über IP-Netze voraussetzen. Das Nationale Institut für Onkologie in Gliwice nutzt eine Reihe von IT-Lösungen, um seine Effizienz zu optimieren und den Betrieb der einzelnen Geräte und Anwendungen zu überwachen. Angesichts der Art der verarbeiteten Daten sind auch die Sicherheit und die Gewährleistung der Vertraulichkeit des gesamten Datenmaterials von grundlegender Bedeutung.

Die Situation des Kunden

Bisher verwendete das Nationale Institut für Onkologie Systeme zur Netzwerküberwachung, die Pakete, Protokolle und aktive Geräte analysiert. Die gewaltige Menge an Daten, die aus verschiedenen Systemen stammten, hatte zur Folge, dass jede Analyse zeitaufwändig und komplex war. Unter anderem war es schwierig vorherzusagen, wie sich die geplante Entwicklung der medizinischen Infrastruktur auf die Effizienz der IT-Infrastruktur und damit auf den Service sowohl für die Patienten als auch für das Forschungspersonal des Onkologischen DInstituts auswirken würde.

Für das Nationale Institut für Onkologie, in Gliwice, war es von entscheidender Bedeutung, die Quellen der Netzwerkauslastung zu ermitteln und herauszufinden, woher der erhöhte Datenverkehr stammte und wohin dieser ging. Insbesondere, weil einige Nutzer über Probleme mit der Verfügbarkeit und Leistung einiger Dienste berichteten. Ein weiteres Kriterium bestand in der Fähigkeit, Leistungsprobleme, Sicherheitsvorfälle und Anomalien schnell zu identifizieren. Die Mitarbeiter des Instituts erwarteten außerdem, dass die neue Lösung unbefugte Kommunikation, Malware-Bedrohungen und Brute-Force-Angriffe aufspüren würde. Die Herausforderung bestand also darin, ein effizientes,



Unternehmen sehen den schnellen Zugriff auf kritische Informationen, die den Schutz der Organisation ermöglichen, als entscheidend an. Das interaktive Dashboard wird täglich aktualisiert und zeigt Sicherheitsalarme, unterteilt nach kritischen Informationen, Hosts, Taktiken und Modulen an.

kostengünstiges Überwachungsinstrument zu etablieren, mit dem es möglich würde, den gesamten Netzwerkverkehr sowohl auf Leistung als auch auf Sicherheit zu analysieren. Weitere wesentliche Kriterien waren die Intuitivität der Lösung und die einfache Implementierung. - Die Mitarbeiter des Instituts konnten - aufgrund ihrer vielfältigen Aufgaben - nicht allzu viel Zeit für die Parametrisierung und das Erlernen des neuen Systems aufwenden.

Verlauf der Arbeiten

Nachdem die Auswahlkriterien klar definiert waren, wurde ein System zur Analyse des Netzwerkverkehrs und zur Erkennung von Bedrohungen unter Verwendung des NetFlow-Protokolls einschließlich der Installation zur Ausschreibung gebracht. Unter den an der Ausschreibung teilnehmenden Unternehmen legte die Passus S.A. mit ihrem Produkt FlowControl unter Berücksichtigung der funktionalen Kriterien das günstigste Angebot vor und erhielt damit den Zuschlag für die besagte Ausschreibung.

Die Implementierung und Einführung von Sycope FlowControl dauerte nur einen Arbeitstag und fand im Dezember 2019 statt. Das IT-Team des Instituts schätzte die schnelle und effiziente Installation von FlowControl, das bereits am nächsten Tag nach der Implementierung genutzt werden konnte. Positiv wurde auch die intuitive Benutzeroberfläche aufgenommen, weil diese eine wochenlange Einarbeitung in den vollen Funktionsumfang ersparte. Für die Implementierung des FlowControl-Systems musste das Nationale Institut für Onkologie nicht extra eine Infrastruktur aufbauen, was die Implementierungs-kosten erheblich senkte. Mit dieser Lösung kann fast der gesamte mögliche Datenverkehr analysiert werden.

Lösungsmöglichkeiten und Vorteile

FlowControl ermöglichte es dem Kunden, den Netzwerkverkehr mithilfe des NetFlow-Protokolls zu analysieren. Das Nationale Institut für Onkologie hat damit begonnen, Daten aus dem Netzwerkverkehr zu sammeln und zu analysieren, um die Ursachen von Netzwerkverbindungs-problemen zu diagnostizieren und Engpässe zu identifizieren. Diese Lösung lieferte detaillierte Informationen über den von den Benutzern erzeugten Datenverkehr, die Kommunikation zwischen den Servern und die im Unternehmen verwendeten Anwendungen.

> *„Vor der Einführung der Sycope-Lösung verwendeten wir Systeme, die zwar gut funktionierten, aber viel teurer waren und nur eine begrenzte Leistung aufwiesen", sagt Artur Wójcik der IT-Spezialist, der die FlowControl-Lösung im Nationalen Institut für Onkologie in Gliwice implementierte. „Vor allem fehlte uns ein Tool, mit dem wir schnell auf Daten zugreifen und diese bis zu mehreren Monaten speichern können, ohne eine zusätzliche Netzwerkinfrastruktur aufbauen zu müssen. Wir wussten auch, dass wir zu diesem Zeitpunkt nach einer erschwinglichen Lösung suchen mussten."*

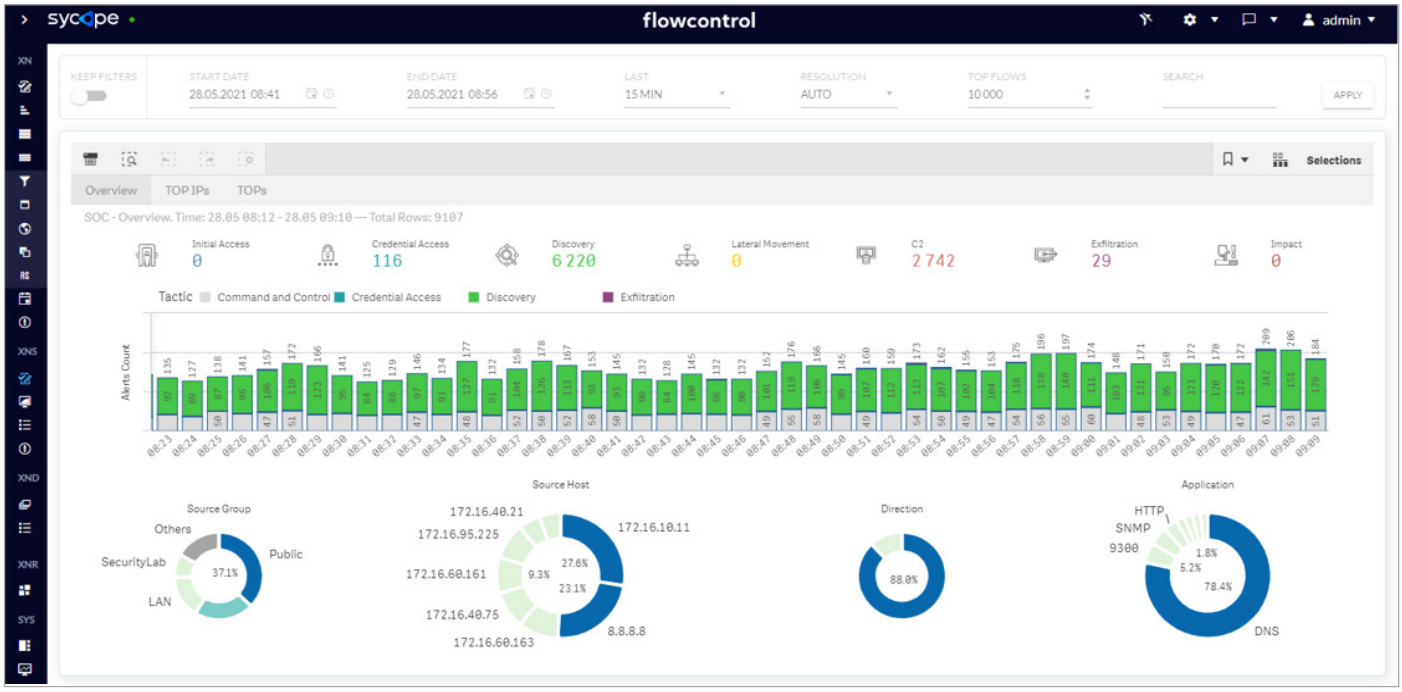
Vordefinierte Dashboards mit Statistiken über Schnittstellennutzung, Netzwerkbandbreite und Netzwerkressourcen erleichtern das Verständnis und die Verwaltung des Netzwerkverkehrs. Anhand der in den Network Flows enthaltenen Informationen konnten die Quellen und Ziele des Datenverkehrs sowie die Dienstklasse ermittelt werden, so dass die für Verzögerungen und Leistungseinbußen verantwortlichen Anwendungen schnell identifiziert werden konnten. Die Identifizierung ungenutzter Ressourcen ermöglichte es, die Effizienz der Infrastruktur zu steigern und geeignete Entscheidungen über Investitionen in Kapazitätserweiterungen zu treffen, was zu einer Kostenoptimierung beitrug. Mit FlowControl wurden auch die Auswirkungen der neu implementierten Anwendungen auf die Leistung überprüft.

Heute spielt das FlowControl-System die Rolle eines Arztes in einer begehbaren Klinik, da es die Bereiche aufzeigt, die einer weiteren Analyse bedürfen. Klare Verbindungsdiagramme und entsprechend ausgewählte Ansichten ermöglichen es, die Bereiche der Infrastruktur zu lokalisieren, die Aufmerksamkeit erfordern. Erweiterte Suchwerkzeuge, darunter die intuitive Google-Suche, stellen eine große Hilfe in der täglichen Arbeit dar. Eine tiefergehende Analyse wird durch die Drill-Down-Tools erleichtert, die es dem Benutzer ermöglichen, mit einem einzigen Klick von allgemeinen Indikatoren zu einer detaillierten Analyse von Statistiken und Indikatoren für einen bestimmten Port, eine Schnittstelle oder eine IP-Adresse übergehen zu können.

> *„Ein System, das an einem Tag einsatzbereit ist, geht über die standardmäßigen Vorgaben hinaus. Wir waren angenehm überrascht, wie einfach die Installation und die Integration von FlowControl in unsere anderen Systeme war", betont Artur Wojcik.*

Die IT-Abteilung des Nationalen Instituts für Onkologie setzt das System FlowControl auch verstärkt im Bereich der Sicherheit ein. Sehr beliebt ist die MITRE-Methode im XNS-Modul, die es ermöglicht, die von einem Vorfall ausgehenden Risiken in einem breiteren Kontext zu bewerten und sich auf die Angriffe zu konzentrieren, die eine echte Bedrohung für wichtige Daten und Anwendungen darstellen.

In den kommenden Monaten plant das Team, die Einstellungen und Warnmeldungen auf der Grundlage ihrer Anforderungen anzupassen, was letztlich die Effizienz und Effektivität der Nutzung des Systems steigern wird.



Für den Kunden war es äußerst hilfreich, Diagramme, Indikatoren und Tabellen zu verwenden, die an die Besonderheiten der Arbeit des SOC-Teams angepasst sind und auf der Analyse des NetFlow-Protokolls basieren: Dadurch konnte der Kunde die Veränderungsdynamik und die Art der verdächtigen Ereignisse im Minutentakt analysieren.

Sycope konzentriert sich auf die Konzeption und Entwicklung hochspezialisierter IT-Lösungen zur Überwachung und Verbesserung der Netzwerk- und Anwendungsleistung sowie der IT-Sicherheit sowohl in On-Premise-Architekturen als auch in hybriden, privaten und öffentlichen Cloud-Umgebungen. Unsere Lösungen wurden von Ingenieuren geschaffen und entwickelt, die sich seit rund 20 Jahren mit den Themen Netzwerkperformance, Anwendungseffizienz und IT-Sicherheit beschäftigen. Mit den Lösungen globaler APM/NPM- und SIEM-Anbieter haben sie mehr als 400 Projekte für Kunden wie Franklin Templeton Investment, das Verteidigungsministerium, die NATO, die Polnische Nationalbank, T-Mobile, Ikea, die ING Group, Orange und die Alior Bank durchgeführt. Neben vielen erfolgreichen Implementierungen wird die Kompetenz des Teams durch viele Einzelzertifikate bestätigt, u.a.: persönliche Sicherheitsfreigabe bis zur Klausel „Confidential" und „NATO Secret", CISA, CISSP, ISO 27001 Lead Auditor, IBM Certified Deployment Professional Security QRadar SIEM, ArcSight Zertifikat AS Data Platform Technical, Certified Ethical Hacker, Offensive Security Certified Professional.