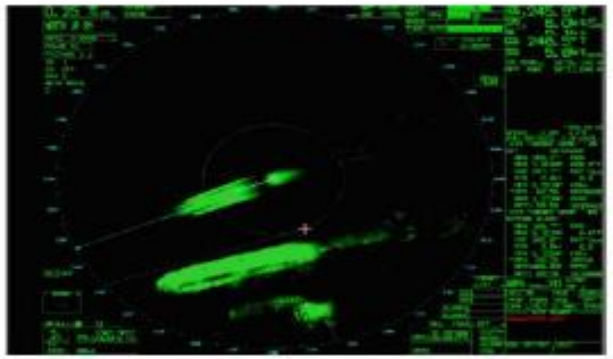

alpha strike
labs

Dezentrales Cyber-Aufklärungssystem

alpha strike labs

Radar



Satellit

Infrarot

konventionelle
Geländebeurteilung und Lagedarstellung

Wie führt man eine Lagedarstellung im Cyberspace durch?

Dezentrales Cyber-Aufklärungssystem (DCS)

- Zweistellige Anzahl von Suchknoten im Internet
- Scannt nach Diensten und Schwachstellen im Internet (2,8 Milliard geroutete IP-Adressen) innerhalb weniger Stunden
- Unterstützt über 40 offene und proprietäre Protokolle
- Spezialisiert auf Industrial Control Systems (ICS/SPS)

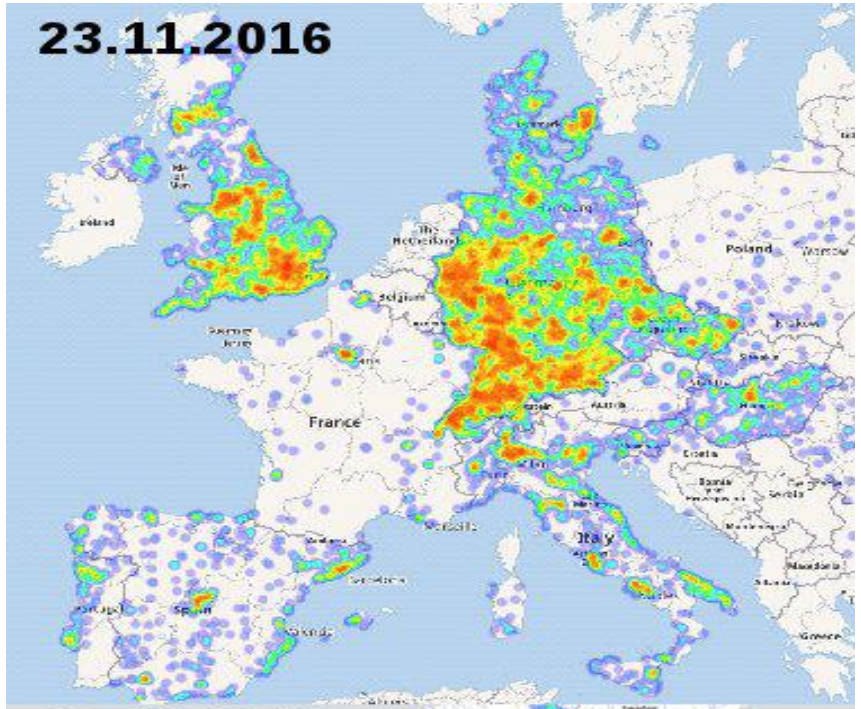
Dezentrales Cyber-Aufklärungssystem (DCS)

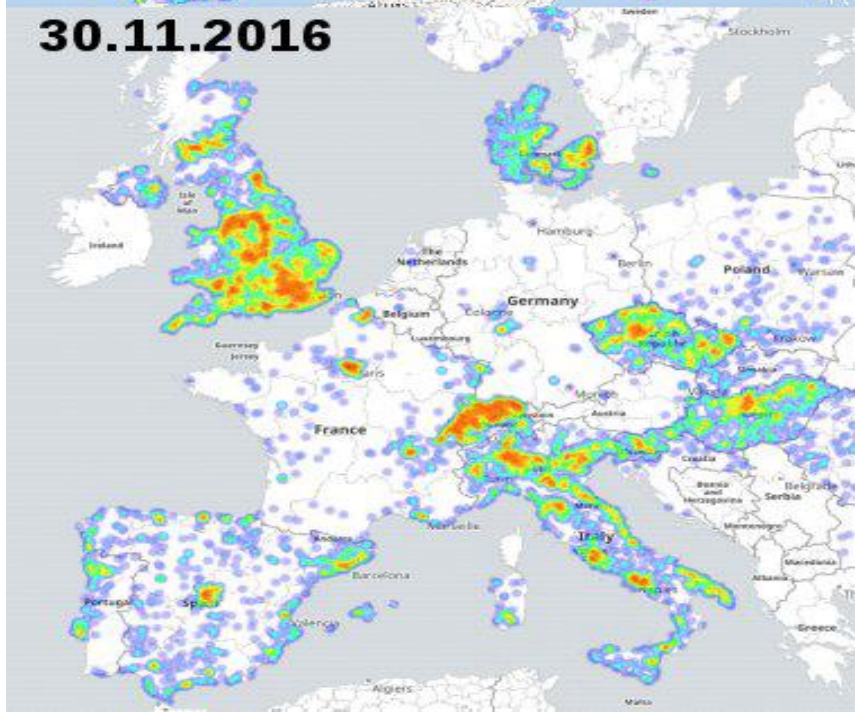
- Durch das DCS sind wir in der Lage eine globale Angriffsflächendetektierung für ein Unternehmen durchzuführen, **ohne,** dass uns vorab Informationen wie z.B. IP-Adressen zur Verfügung gestellt werden müssen.
- Oft finden wir Internet-Services, die schwachstellenbehaftet, weder bekannt oder noch dokumentiert waren (Schatten-IT).
- Das DCS kann Unternehmen von einer externen Hacker-Perspektive zu betrachten und alle eigenen externen Services zu identifizieren.

Dezentrales Cyber-Aufklärungssystem (DCS)

- Identifikation aller externen IP-Adressen, Webseiten und Schwachstellen die zu einem Unternehmen, einer kritischen Infrastruktur oder Behörde gehören können.
- Inter-Aktives Analyseframework:
  Mit automatischer Karten-, Chart- und Tabellenerzeugung

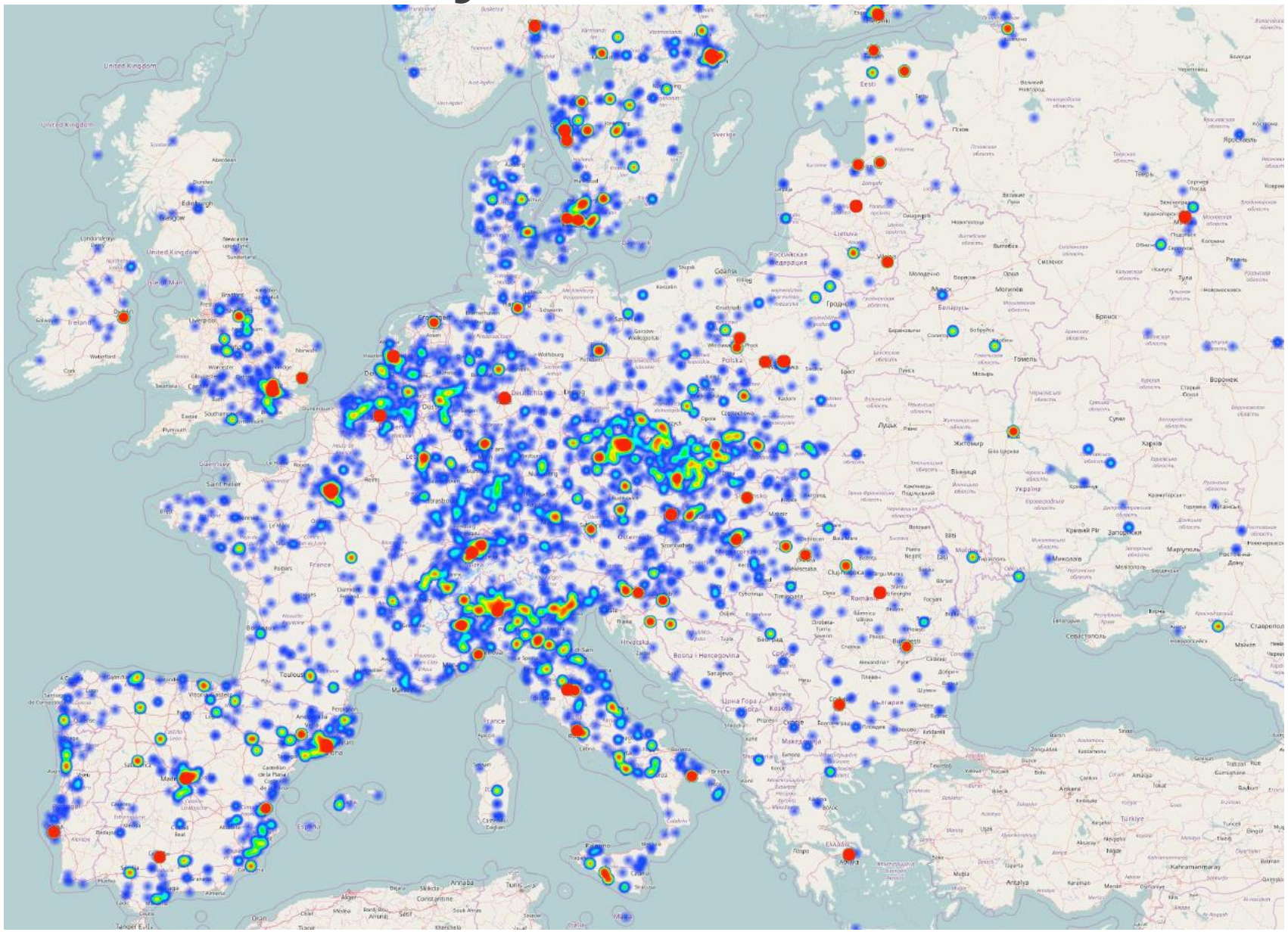
- Verteilungsanalysen:
  Wie sind schwachstellenbehaftete Netzwerkdienste auf der Welt verteilt?
- Vergleichsanalysen:
  Wie steht mein Unternehmen im Vergleich zu anderen dar?





- 24.11.2016: Ein Botnetz greift auch die Telekom via dem Protokoll TR-069 an: Viele DSL/Kabel-Router stürzen ab
- Unser CDAS kann durch Internetscans sofort ein Lagebild aller via TR-069 erreichbaren Systeme darstellen
- Die Telekom sperrte nach wenigen Tagen als Sofortmaßnahme TR-069-Zugriffe via extern
- Ein erneuter Scan / Lagedarstellung zeigt, dass Deutschland nun keine Angriffsfläche mehr bietet

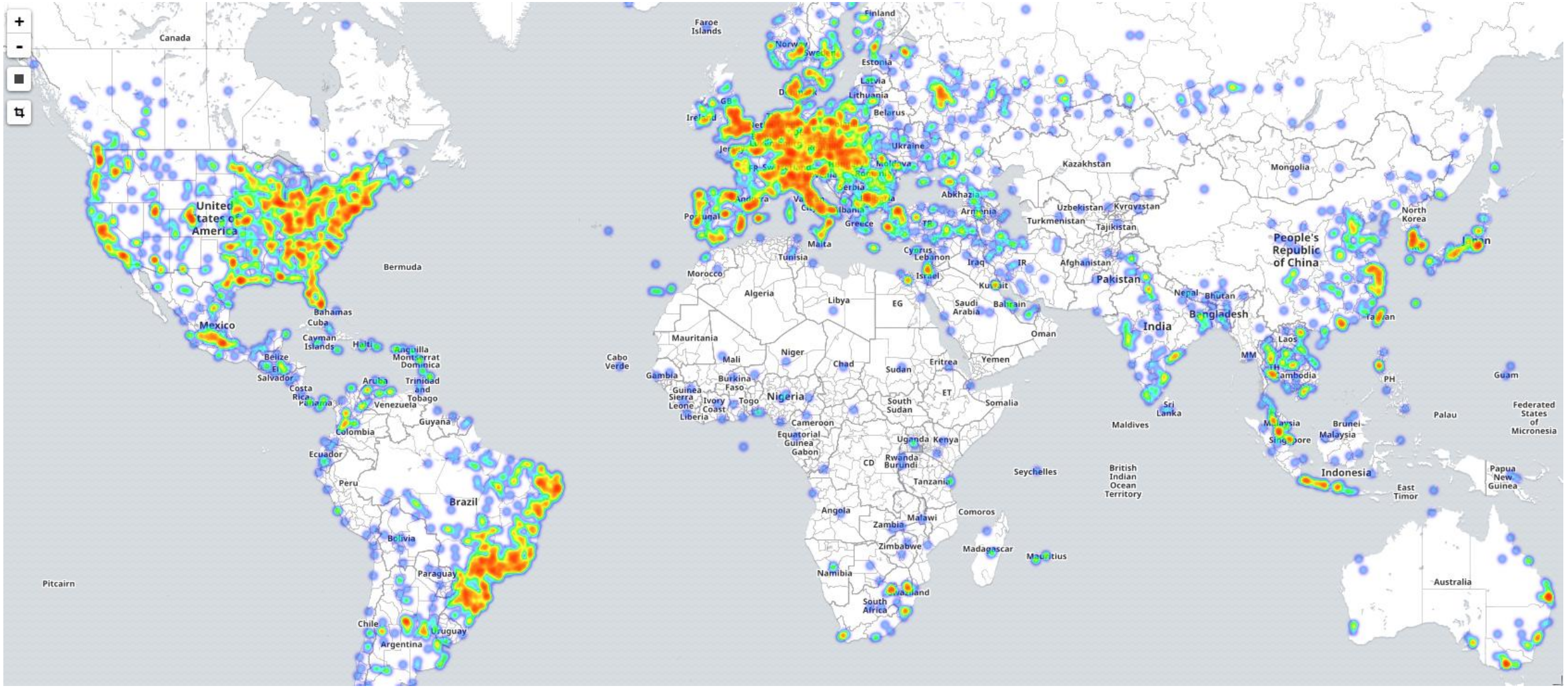
Industrielle Kontrollsysteme (SPS) im Internet



LIVE DEMO

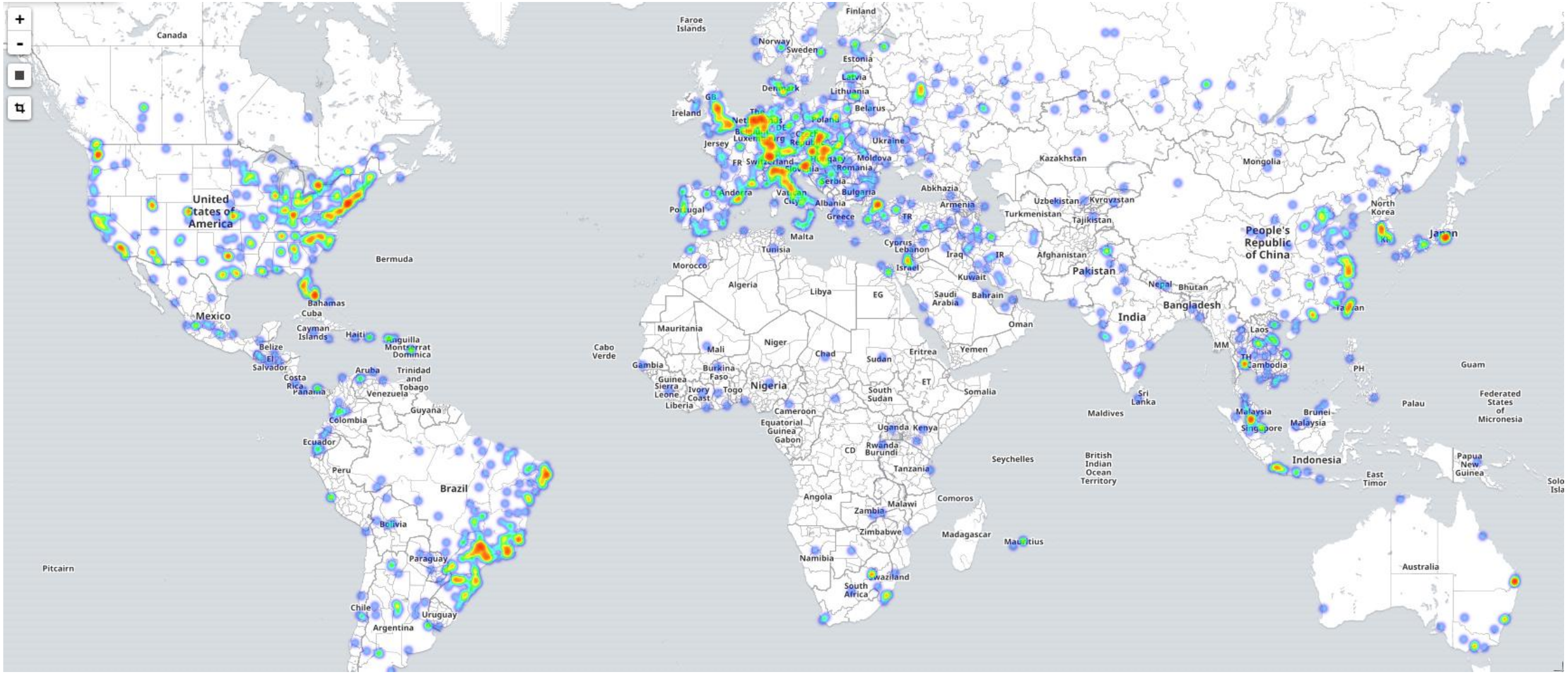
VM-Ware vCenter Administration Software

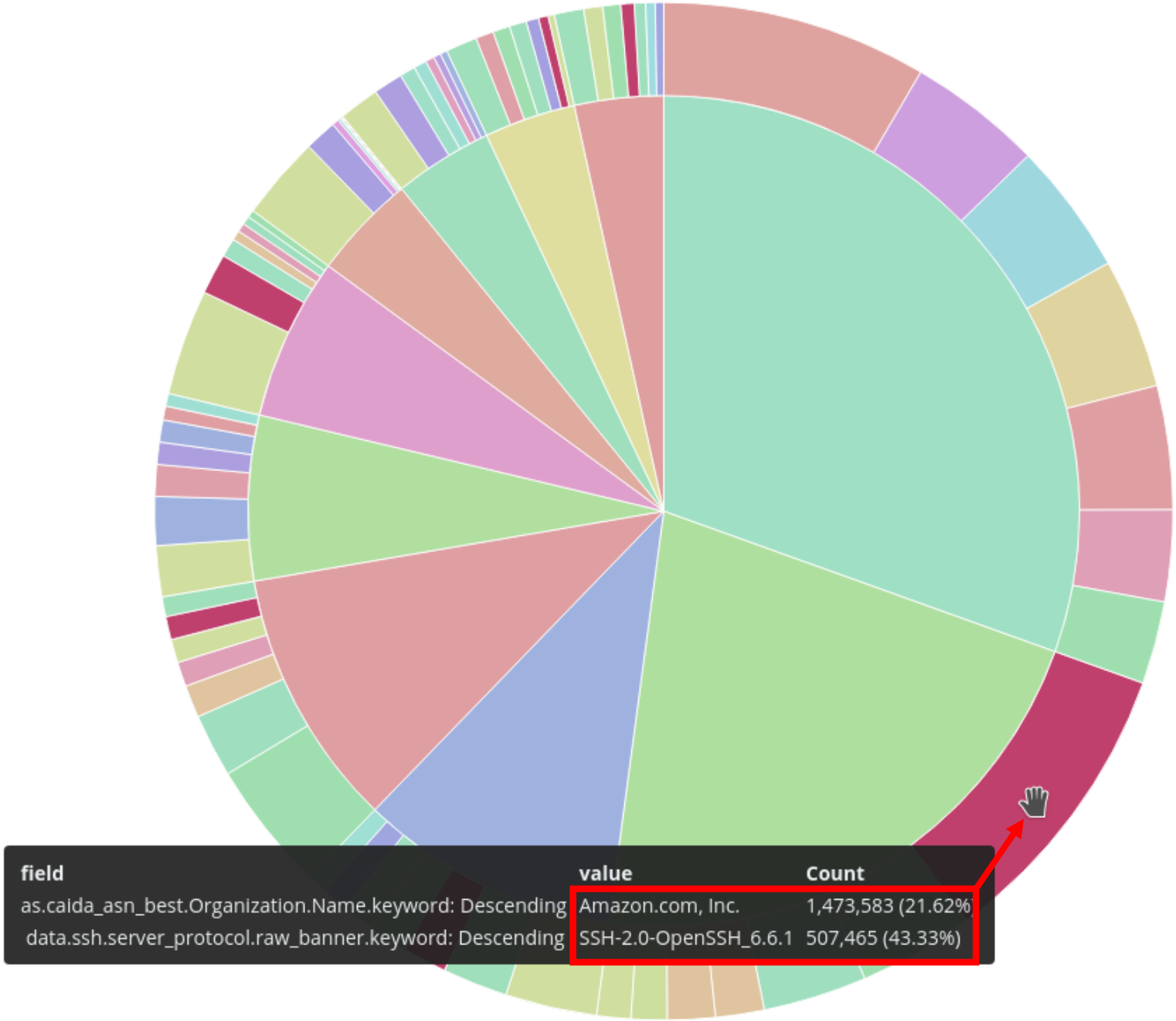
identifiziert via dem CommonName „Vmware Installer“ im HTTPS Zertifikat



VM-Ware vCenter Administration Software

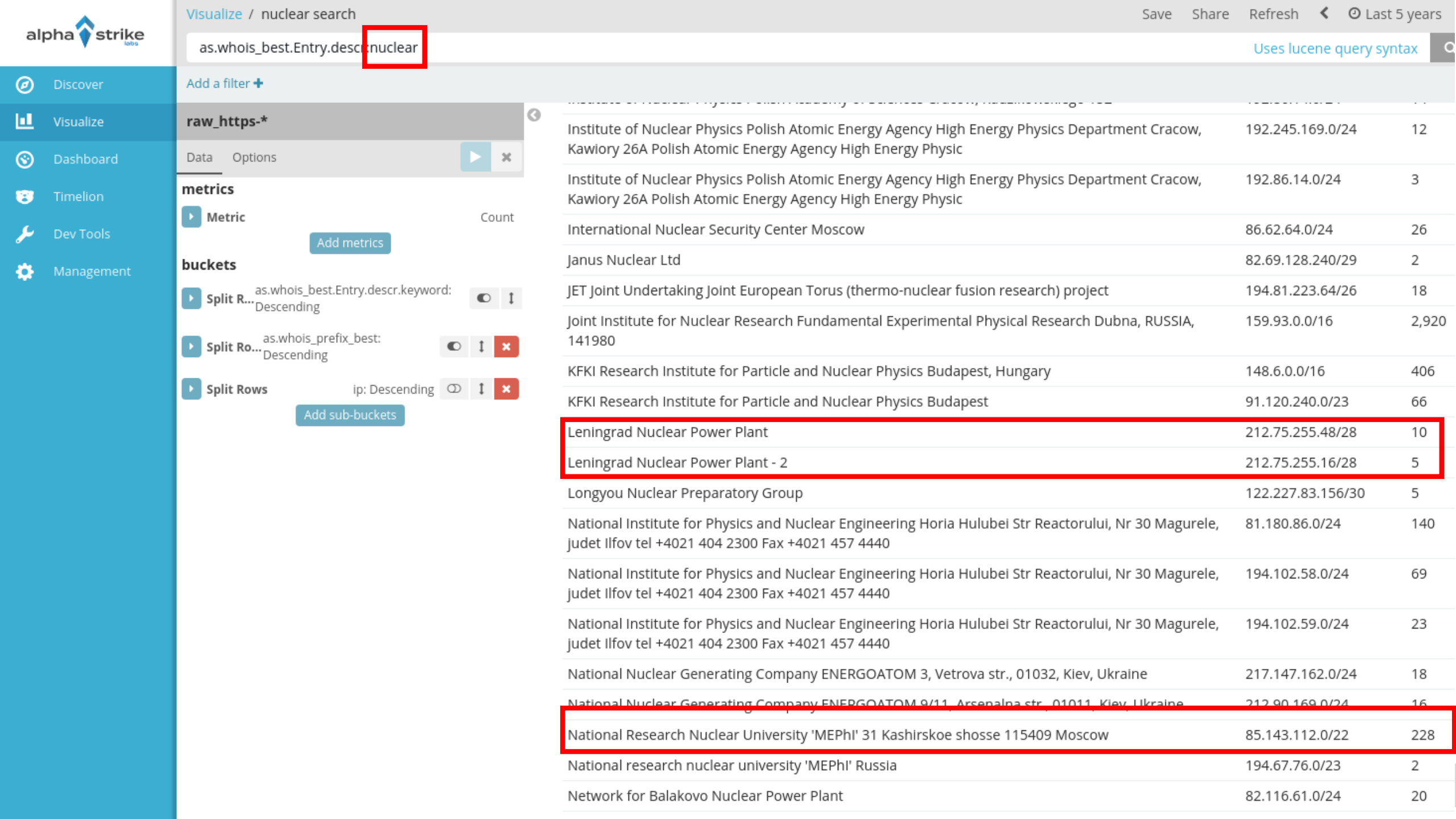
Eingrenzung auf alle vCenter mit Heartbleed-Vulnerability





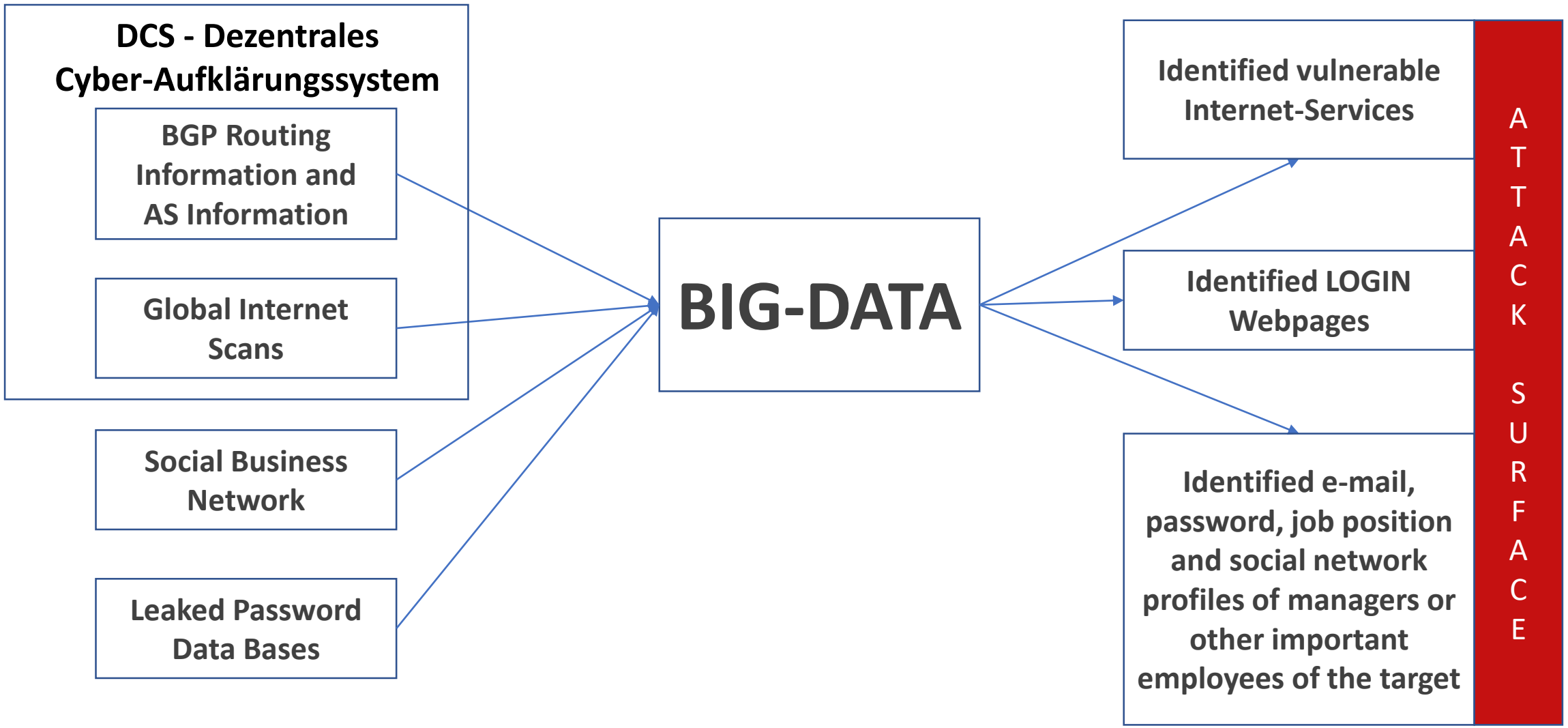
- Der innere Kreis zeigt die Verteilung von SSH-Diensten global auf die TOP 10 Netzwerke (AS) des Internets
- Der zweite Kreis zeigt die verwendeten TOP 10 SSH-Software-Versionen in dem jeweiligen Netzwerk

- Beispiel:
  - 1,4 Mio. SSH-Server werden bei Amazon gehostet (entspricht ~22% aller SSH-Server der TOP 10 Netzwerke)
  - ~43% aller SSH-Server bei Amazon verwenden OpenSSH_6.6.1



Institute of Nuclear Physics Polish Atomic Energy Agency High Energy Physics Department Cracow, Kawiory 26A Polish Atomic Energy Agency High Energy Physic	192.245.169.0/24	12
Institute of Nuclear Physics Polish Atomic Energy Agency High Energy Physics Department Cracow, Kawiory 26A Polish Atomic Energy Agency High Energy Physic	192.86.14.0/24	3
International Nuclear Security Center Moscow	86.62.64.0/24	26
Janus Nuclear Ltd	82.69.128.240/29	2
JET Joint Undertaking Joint European Torus (thermo-nuclear fusion research) project	194.81.223.64/26	18
Joint Institute for Nuclear Research Fundamental Experimental Physical Research Dubna, RUSSIA, 141980	159.93.0.0/16	2,920
KFKI Research Institute for Particle and Nuclear Physics Budapest, Hungary	148.6.0.0/16	406
KFKI Research Institute for Particle and Nuclear Physics Budapest	91.120.240.0/23	66
Leningrad Nuclear Power Plant	212.75.255.48/28	10
Leningrad Nuclear Power Plant - 2	212.75.255.16/28	5
Longyou Nuclear Preparatory Group	122.227.83.156/30	5
National Institute for Physics and Nuclear Engineering Horia Hulubei Str Reactorului, Nr 30 Magurele, judet Ilfov tel +4021 404 2300 Fax +4021 457 4440	81.180.86.0/24	140
National Institute for Physics and Nuclear Engineering Horia Hulubei Str Reactorului, Nr 30 Magurele, judet Ilfov tel +4021 404 2300 Fax +4021 457 4440	194.102.58.0/24	69
National Institute for Physics and Nuclear Engineering Horia Hulubei Str Reactorului, Nr 30 Magurele, judet Ilfov tel +4021 404 2300 Fax +4021 457 4440	194.102.59.0/24	23
National Nuclear Generating Company ENERGOATOM 3, Vetrova str., 01032, Kiev, Ukraine	217.147.162.0/24	18
National Nuclear Generating Company ENERGOATOM 9/11, Arsenalna str., 01011, Kiev, Ukraine	212.90.169.0/24	16
National Research Nuclear University 'MEPhI' 31 Kashirskoe shosse 115409 Moscow	85.143.112.0/22	228
National research nuclear university 'MEPhI' Russia	194.67.76.0/23	2
Network for Balakovo Nuclear Power Plant	82.116.61.0/24	20

OPEN SOURCE INTELLIGENCE (OSINT)



Herausforderungen

IPv6:

- Die Anzahl der IPv6-Adressen entspricht ungefähr der Anzahl von Molekülen auf der Welt. Das Scannen aller Adressen wird keine Option mehr sein.

Contact

Alpha Strike Labs GmbH

Mail: office@alphastrike.io

Web: www.alphastrike.io

Phone: +43 (0) 1 968 8905

Phone: +49 (0) 30 120 877 420

Mobile: +49 (0) 176 444 30475