nixu
cybersecurity.

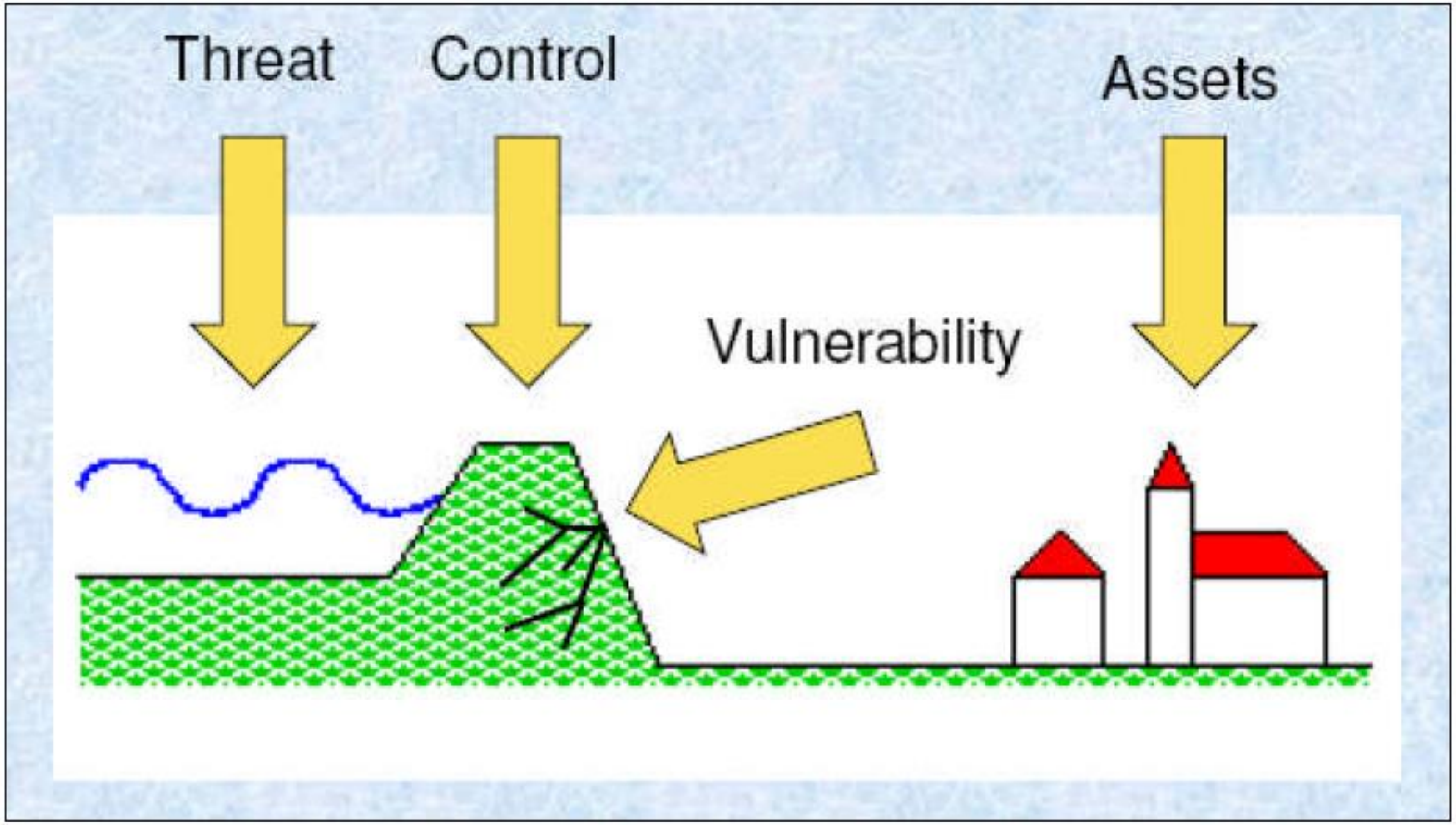
No vulnerability, No cry

Alles van waarde is weerloos

Chris van den Hooven
Security Consultant Nixu

PvIB 14 mei 2019

Het poldermodel



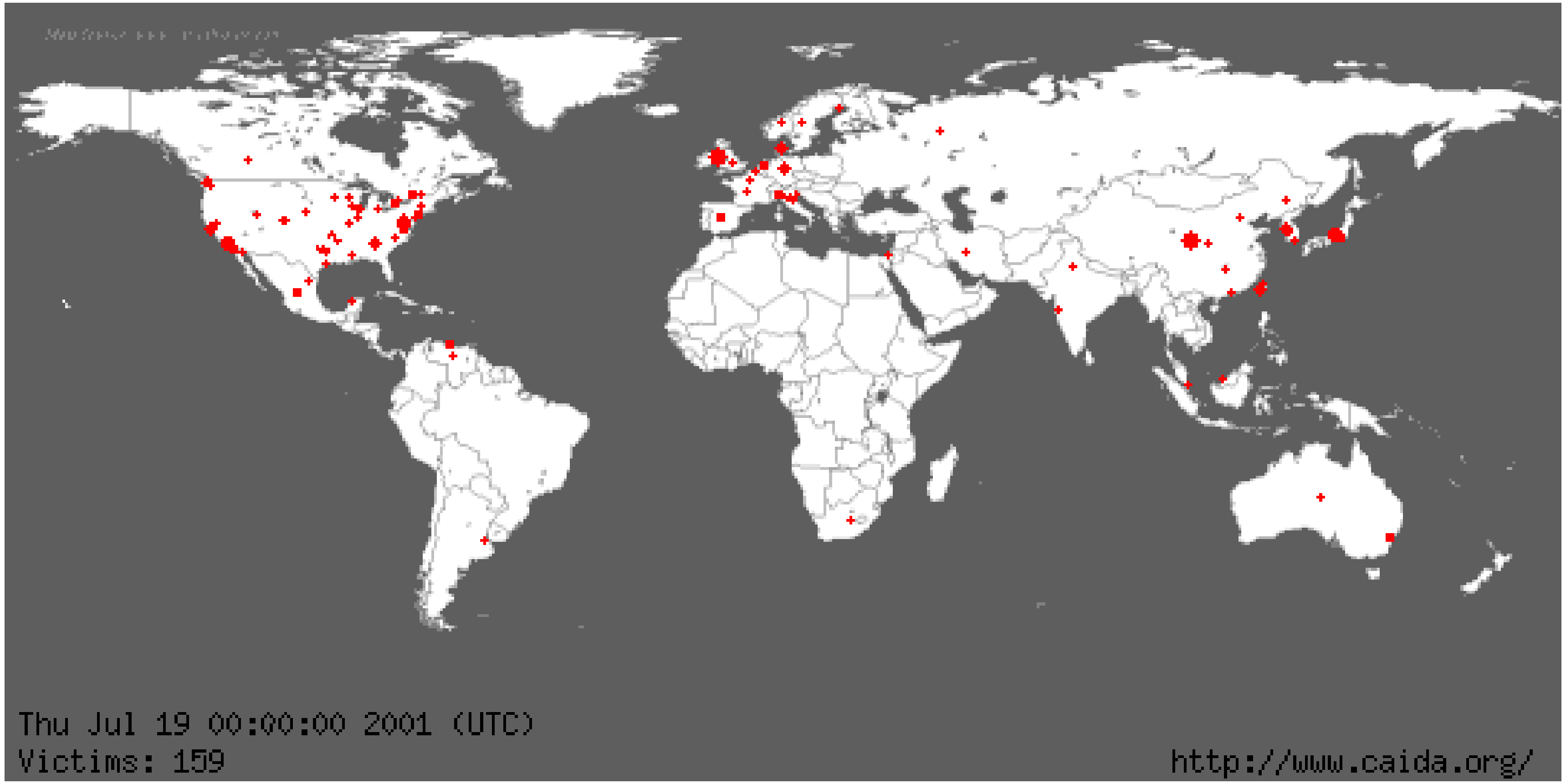
Vulnerabilities in informatiesystemen

- Software fout
- Configuratiefout
- Gebruiker?

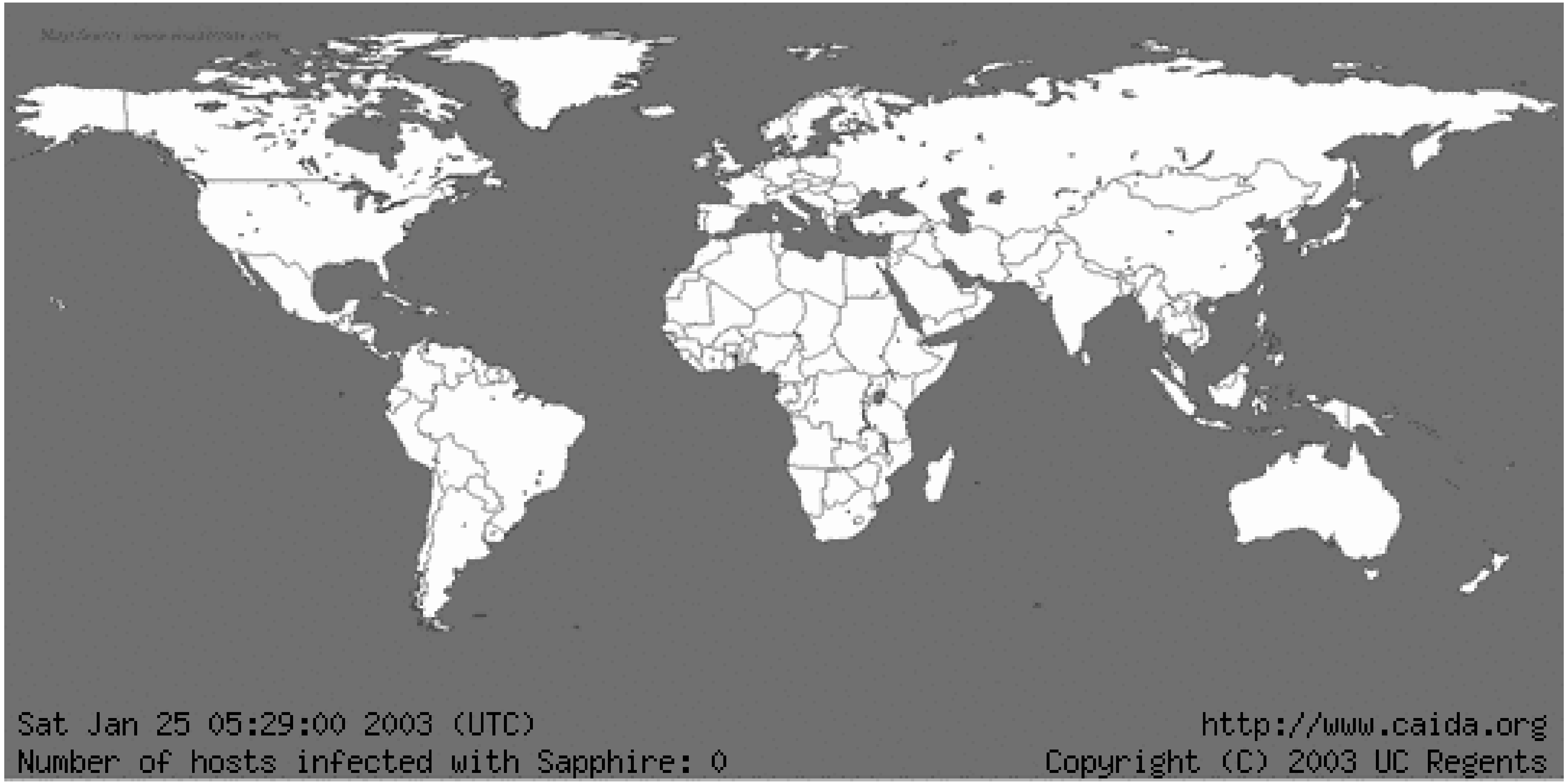
Exploit

```
GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u685
8%ucbd3%u7801 %u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3
%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0
```

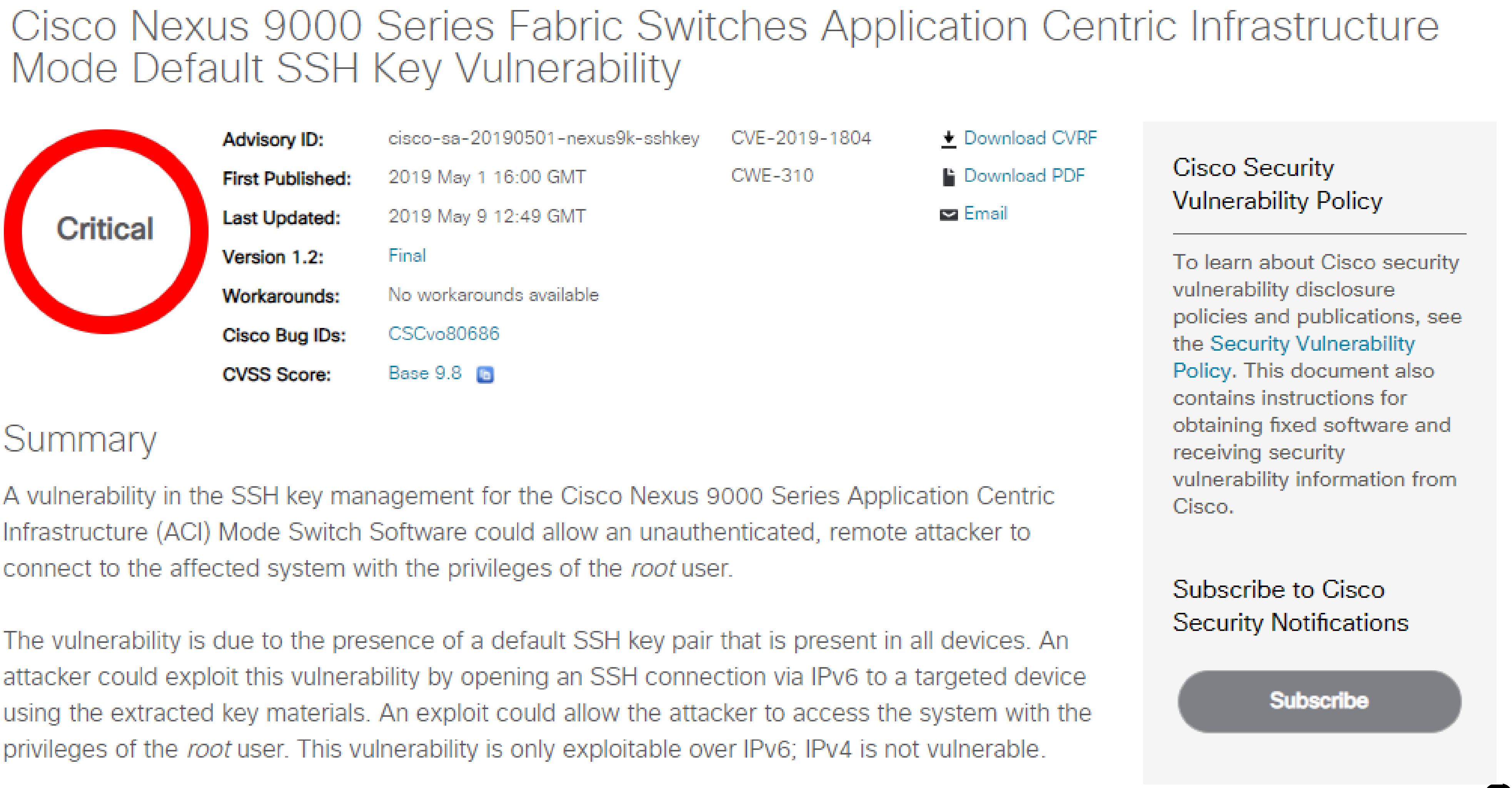
Where did this all started (Code Red, 2001)



Where did this all started (Slammer/ Saphire, 2003)


Sat Jan 25 05:29:00 2003 (UTC)
Number of hosts infected with Sapphire: 0
http://www.caida.org
Copyright (C) 2003 UC Regents

Recente publicatie



Cisco Nexus 9000 Series Fabric Switches Application Centric Infrastructure Mode Default SSH Key Vulnerability

Critical

Advisory ID:	cisco-sa-20190501-nexus9k-sshkey
First Published:	2019 May 1 16:00 GMT
Last Updated:	2019 May 9 12:49 GMT
Version 1.2:	Final
Workarounds:	No workarounds available
Cisco Bug IDs:	CSCvo80686
CVSS Score:	Base 9.8

CVE-2019-1804
CWE-310

Download CVRF
Download PDF
Email

Summary

A vulnerability in the SSH key management for the Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an unauthenticated, remote attacker to connect to the affected system with the privileges of the *root* user.

The vulnerability is due to the presence of a default SSH key pair that is present in all devices. An attacker could exploit this vulnerability by opening an SSH connection via IPv6 to a targeted device using the extracted key materials. An exploit could allow the attacker to access the system with the privileges of the *root* user. This vulnerability is only exploitable over IPv6; IPv4 is not vulnerable.

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

Theorie

High-level process steps:

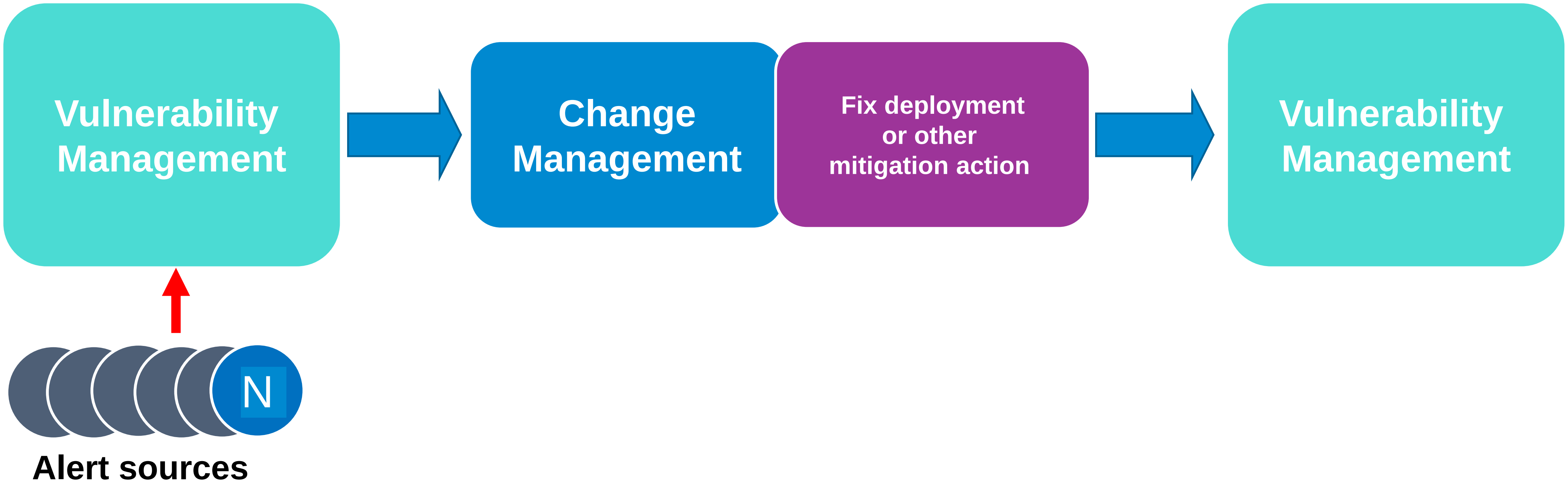
Vulnerability Notification through becoming aware of disclosed vulnerabilities and performing security assessments.

Vulnerability Identification through manual or automated scanning of technologies throughout the organization.

Vulnerability Remediation & Mitigation through application of patches, adjustment of configurations, modification of systems, or acceptance of risk.

CIS® Center for Internet Security®

Vulnerabilty Management process



Vulnerability Management

Change Management

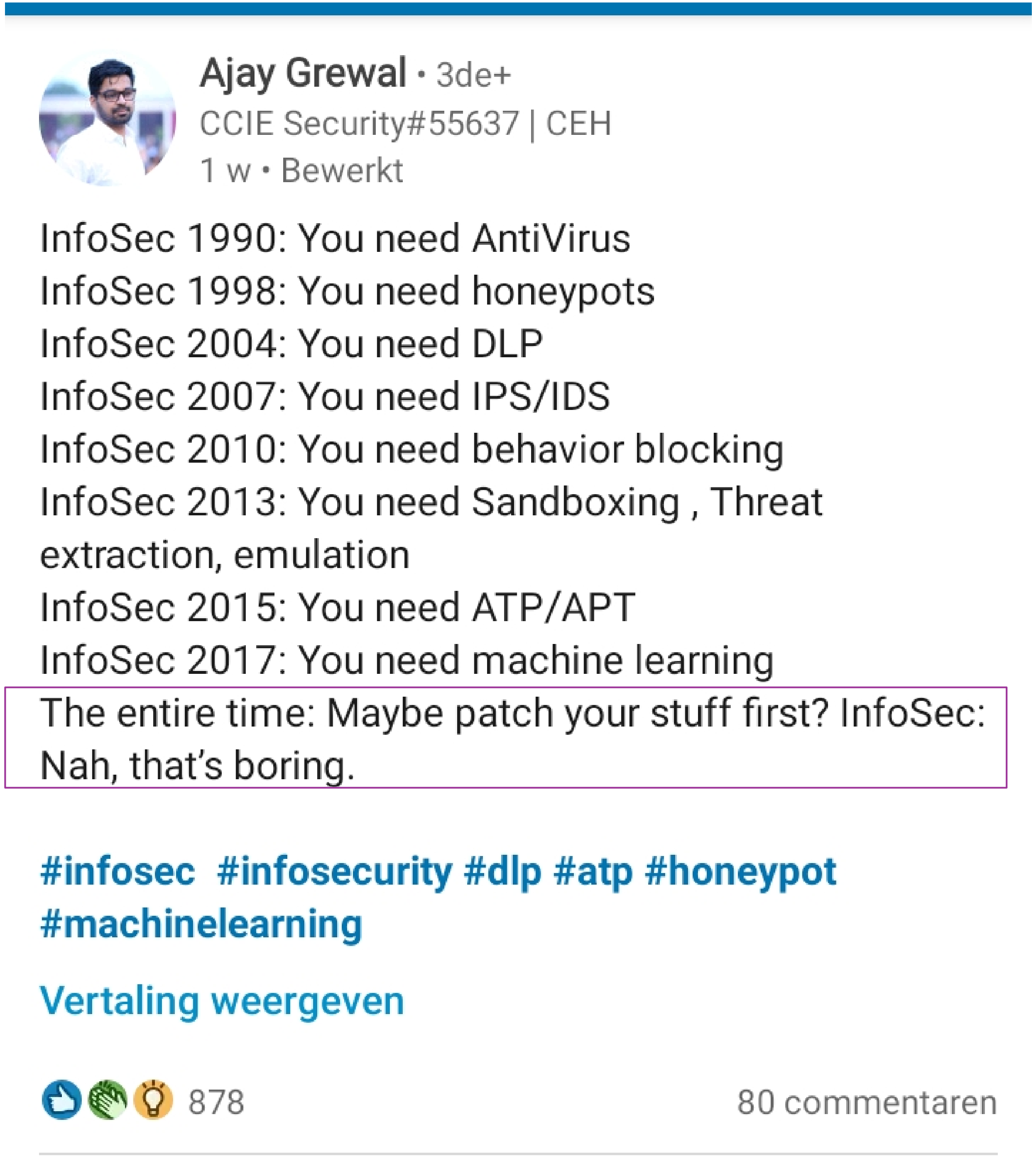
Fix deployment or other mitigation action

Vulnerability Management

Alert sources

Praktijk

Boring?



Ajay Grewal • 3de+
CCIE Security#55637 | CEH
1 w • Bewerkt

InfoSec 1990: You need AntiVirus
InfoSec 1998: You need honeypots
InfoSec 2004: You need DLP
InfoSec 2007: You need IPS/IDS
InfoSec 2010: You need behavior blocking
InfoSec 2013: You need Sandboxing , Threat extraction, emulation
InfoSec 2015: You need ATP/APT
InfoSec 2017: You need machine learning
The entire time: Maybe patch your stuff first? InfoSec: Nah, that's boring.

#infosec #infosecurity #dlp #atp #honeypot #machinelearning

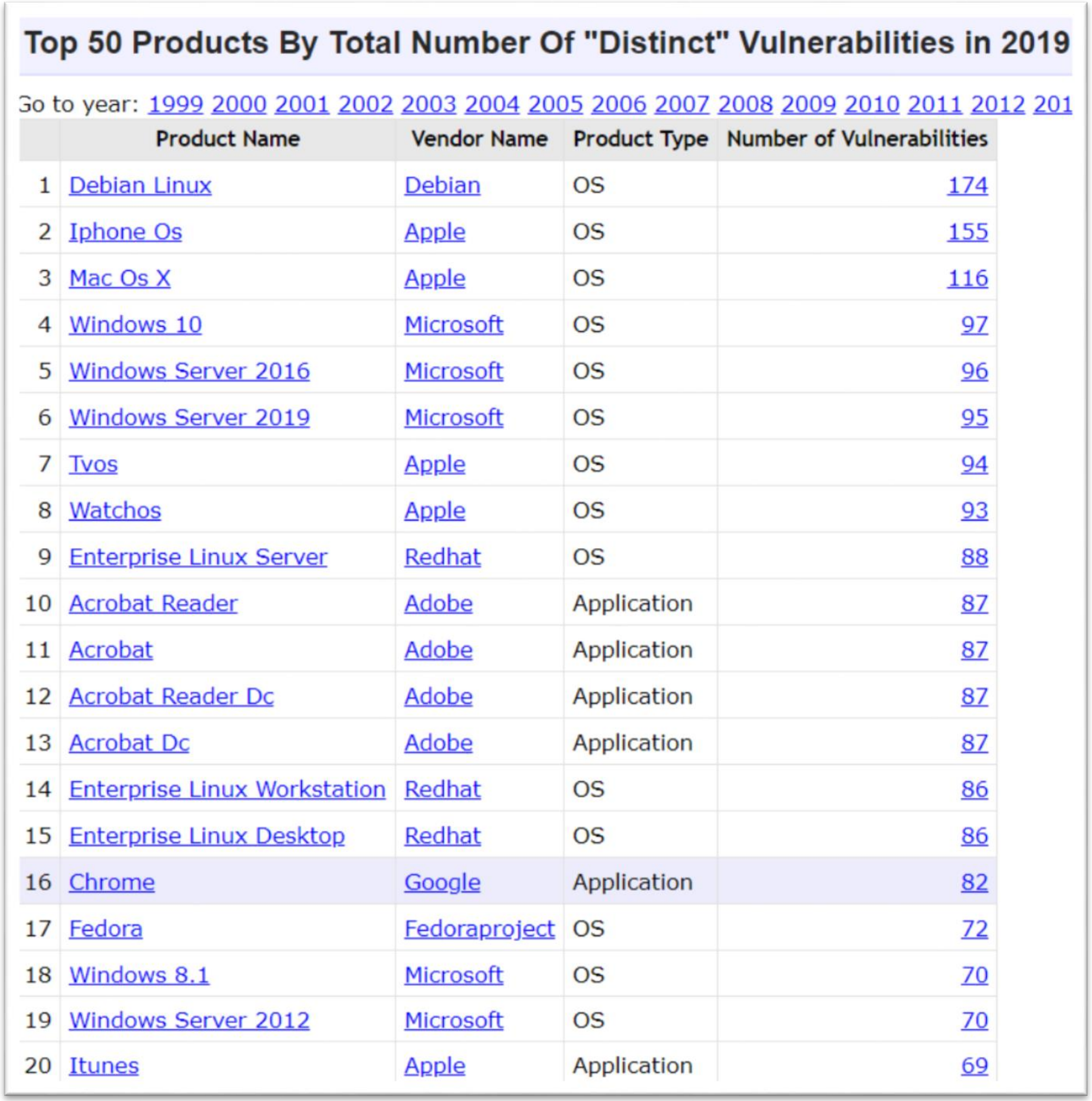
Vertaling weergeven

878

80 commentaren

Onbekenden

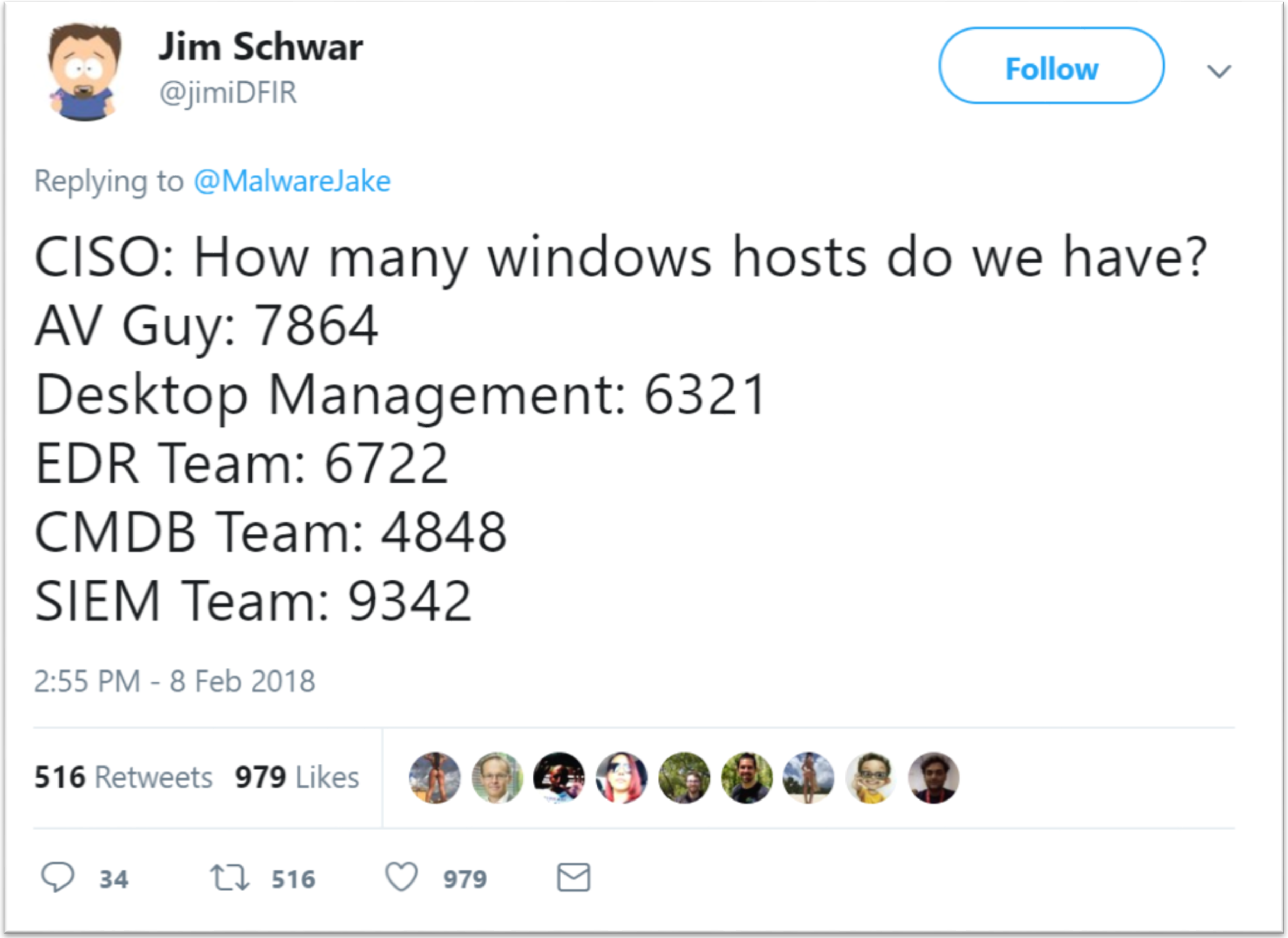
- Wat heb je in huis? (IoT?)
- Welke vulnerabilities zijn gepubliceerd?
- Welke vormen een probleem voor jou?
- Zijn er oplossingen voor?
- Heb je voldoende capaciteit om het aan te pakken?



Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2019

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 201

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	174
2	Iphone Os	Apple	OS	155
3	Mac Os X	Apple	OS	116
4	Windows 10	Microsoft	OS	97
5	Windows Server 2016	Microsoft	OS	96
6	Windows Server 2019	Microsoft	OS	95
7	Tvos	Apple	OS	94
8	Watchos	Apple	OS	93
9	Enterprise Linux Server	Redhat	OS	88
10	Acrobat Reader	Adobe	Application	87
11	Acrobat	Adobe	Application	87
12	Acrobat Reader Dc	Adobe	Application	87
13	Acrobat Dc	Adobe	Application	87
14	Enterprise Linux Workstation	Redhat	OS	86
15	Enterprise Linux Desktop	Redhat	OS	86
16	Chrome	Google	Application	82
17	Fedora	Fedoraproject	OS	72
18	Windows 8.1	Microsoft	OS	70
19	Windows Server 2012	Microsoft	OS	70
20	Itunes	Apple	Application	69



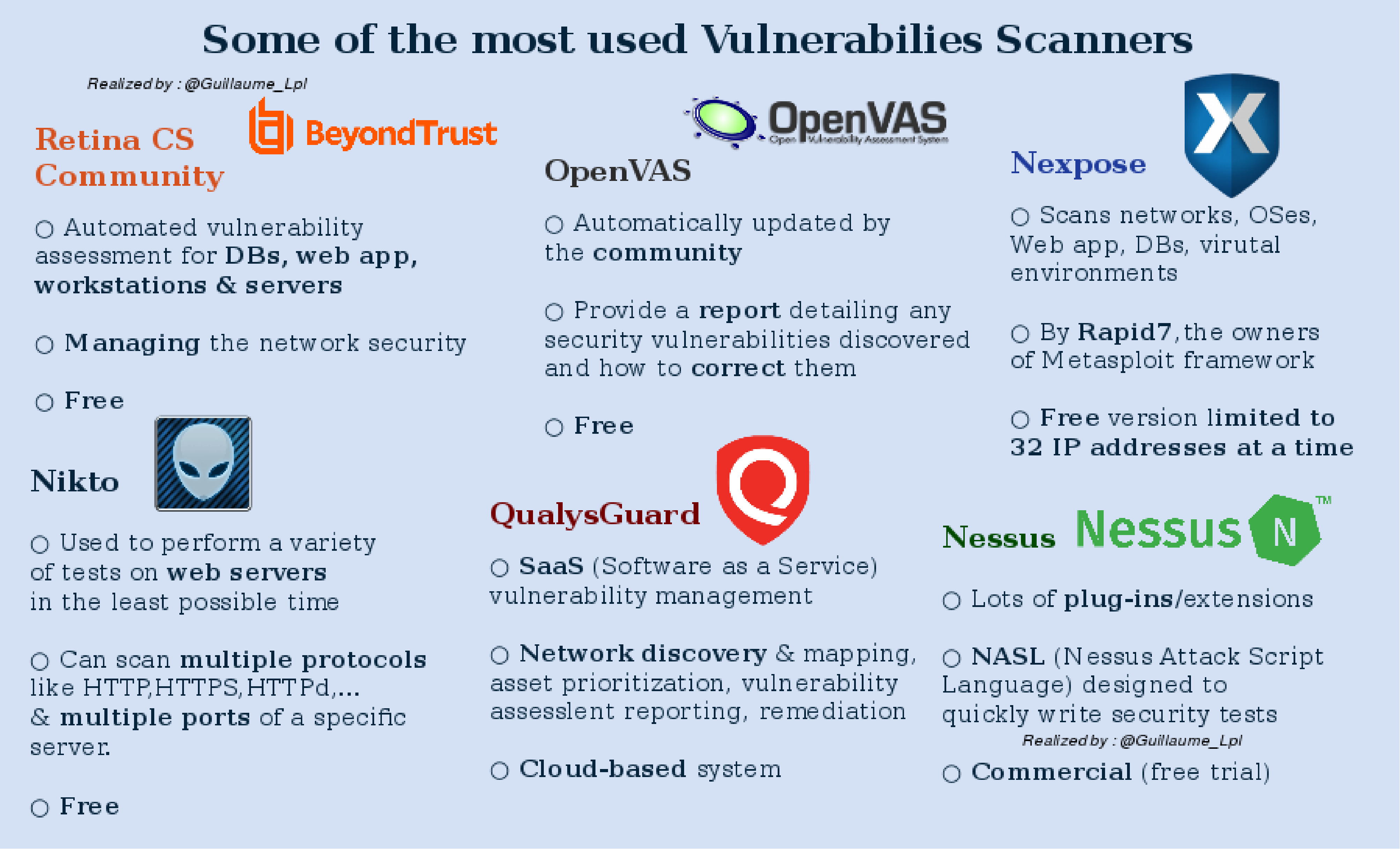
Jim Schwar
@jimiDFIR

Replying to @MalwareJake

CISO: How many windows hosts do we have?
AV Guy: 7864
Desktop Management: 6321
EDR Team: 6722
CMDB Team: 4848
SIEM Team: 9342

2:55 PM - 8 Feb 2018

516 Retweets **979** Likes



Some of the most used Vulnerabilies Scanners

Realized by : @Guillaume_Lpl

Retina CS Community

BeyondTrust

○ Automated vulnerability assessment for **DBs, web app, workstations & servers**

○ **Managing** the network security

○ **Free**

Nikto

○ Used to perform a variety of tests on **web servers** in the least possible time

○ Can scan **multiple protocols** like HTTP,HTTPS,HTTPd,**...** & **multiple ports** of a specific server.

○ **Free**

OpenVAS

OpenVAS Open Vulnerability Assessment System

○ Automatically updated by the **community**

○ Provide a **report** detailing any security vulnerabilities discovered and how to **correct** them

○ **Free**

QualysGuard

○ **SaaS** (Software as a Service) vulnerability management

○ **Network discovery** & mapping, asset prioritization, vulnerability assesslent reporting, remediation

○ **Cloud-based** system

Nexpose

○ Scans networks, OSes, Web app, DBs, virutal environments

○ By **Rapid7**, the owners of Metasploit framework

○ **Free** version **limited to 32 IP addresses at a time**

Nessus

Nessus™

○ Lots of **plug-ins**/extensions

○ **NASL** (Nessus Attack Script Language) designed to quickly write security tests

Realized by : @Guillaume_Lpl

○ **Commercial** (free trial)

Source: Guillaume_Lpl/Twitter

Strategie

- Scan
- identify false positives and remove them from the list
- identify and solve disasters to happen as quickly as possible
- identify low hanging fruit and solve quickly
- handle the rest

Tip: Patch niet op vrijdagmiddag…

Stappen voor risico management

- Wat wil je beschermen?
- Wat is de waarde (BIA)?
- Wat zijn de dreigingen (en dreigers)?
- Wat zijn de vulnerabilities (bedrijfskundig gezien)?
- Wat is het risico?
- Welk risico wil de organisatie nemen?

Rapporteer erover:

- Vulnerability scanning coverage
- Percent of systems with no known (severe) vulnerabilities
- Mean time to mitigate vulnerabilities
- Number of known vulnerabilities
- Mean cost to mitigate vulnerabilities
- Patch policy compliance
- Patch management coverage
- Mean time to patch
- Mean cost to patch

CIS® Center for Internet Security®

Betere strategie: vermijd vulnerabilities

- Zorg voor een robuste architectuur
  - Minimaliseer toegepaste software (legacy)
  - Minimaliseer toegepaste hardware (drivers!)
  - (Netwerk) scheiding van systemen
  - Hardening van systemen
  - Automatiseer updates (workstations)
  - Zorg voor een Secure Development Lifecycle
  - Verplaats naar de cloud (outsource het probleem)
- Awareness sessies (gebruikers als vulnerability)

Chris van den Hooven
chris.vandenhooven@nixu.com

https://www.linkedin.com
/in/cvdhooven/