

SD-WAN INTERNET CENSUS

or
How to Find SD-WANs and not to Lose
Yourself



**ZERO
NIGHTS
2018**

Denis Kolegov
Oleg Broslavsky
Anton Nikolaev

A NEW
SDWANNEWHOPE

A LONG
TIME AGO
IN A GALAXY
FAR, FAR AWAY...

Wait, stop!



ZERO
NIGHTS
2018

2³
EDITION

Not (really) so long time ago,
we decide to start a big SD-WAN
journey



SECURITY!

SD-WAN is Driving a New Approach to **Security**

by Derek Granath | Published Feb 6, 2018

<http://blog.silver-peak.com/sdwan-driving-new-approach-to-security>

The many benefits of SD-WAN for today's networks

SD-WAN ... offer internet connectivity advantages, like reduced cost, by alleviating concerns about internet reliability and **security**

<https://searchsdn.techtarget.com/answer/What-is-SD-WAN-and-should-I-consider-it>

Four Reasons Why SD-WAN Makes Sense

By [Peter Scott](#), SD-WAN Contributor

2. Better **Security**

Unlike traditional WAN solutions, which handle security through multiple appliances at each branch office, SD-WAN can include all of these functions in-box and at lower cost.

<https://www.sdwansource.com/articles/419405-four-reasons-why-sd-wan-makes-sense.htm>



A U.S. Air Force tactical network operations technician adjusts an AV-211 antenna at Diyarbakir Air Base, Turkey. The latest networking techniques, such as software-defined wide area networks, may offer both budgetary and operational benefits for the Defense Department.

The Rise of the SD-WAN

August 2, 2017

By [Tony Bardo](#)

<https://www.afcea.org/content/rise-sd-wan>



ZERO
NIGHTS
2018

2³
EDITION

The Security of SD-WAN



Michael Wood, Vice President - Marketing, VeloCloud Networks,
6/5/2017

Email This Print Comment

[Login](#)



50% 50%

Perhaps we exaggerate, but IT professionals, especially those involved in telecommunications, should always beware of anything that's connected to the Internet, as well as services provided across the Internet. That includes websites, email, cloud-based applications, and of course, WANs.

“SD-WAN is perfectly safe for implementing wide-area networks affordably, efficiently and securely.”



ZERO
NIGHTS
2018

2³
EDITION

**Perfectly safe?
Not exactly...**

[2018.ZERONIGHTS.ORG](http://2018.zeronights.org)



ZERO
NIGHTS
2018

2³
EDITION

XSS

Snapshot of Cpe generated by [ServiceStack](#) on 2018-06-21 4:00:18 AM

view json datasource from original url: [?>](#) cpes/version:"">>[?>](#) in other formats: [?format=json">>json](#) [?format=xml">>xml](#) [?format=csv">>csv](#) [?format=jsonv">>jsv](#)

Response Status

Error Code `SerializationException`

Message `Unable to bind to request 'Cpe'`

Stack Trace

```
at ServiceStack.Serialization.StringMapTypeDeserializer.PopulateFromMap(Object instance, IDictionary`2 keyValuePairs, String queryStringAndFormData, Object fromInstance) at ServiceStack.Host.RestHandler.CreateRequest(IRequest httpReq, IRestPath restPath) at ServiceStack.Host.RestHandler.<ProcessRequestAsync>d__14.MoveNext()
```

Errors

Error Code	Field Name	Message
<code>SerializationException</code>	<code>Id</code>	<code>'version:"">>' is not a valid value for 'Id'</code>

Meta

OK



ZERO
NIGHTS
2018

2³
EDITION

Client-side Authentication

```
function LoginController($scope, $state, $q, AuthenticationService) {
  var vm = this;
  vm.username = '';
  vm.password = '';
  vm.error = false;
  vm.rememberMe = false;

  vm.login = function(){
    // AuthenticationService.authenticate(vm.username, vm.password, vm.rememberMe).then(function ( response ){
    //   $state.go("home");
    // }).catch( function ( response ){
    //   $state.go("login");
    // }).finally( function() {
    // });

    if(vm.username === '████████' && vm.password === '████████') {
      $state.go("home");
    }else{
      vm.error = true;
      $state.go("/");
    }
  };
}
```

?

!

// TODO: fix in prod ?



ZERO
NIGHTS
2018

2³
EDITION

OS Command Injection



```
$response = shell_exec(  
    "cat /home/REDACTED/regions_by_name/"  
    . $_GET["region"].  
    "/maintenanceCurrentCompleted");
```



ZERO
NIGHTS
2018

2³
EDITION

OS Command Injection

```
● ● ●  
  
$response = shell_exec(  
    "cat /home/REDACTED/regions_by_name/"  
    . $_GET["region"].  
    "/maintenanceCurrentCompleted");
```

← → C ⚠ Не защищено | <https://10.30.37.115/storageMigrationCompleted.php?region=:sudo%20id;>
uid=0(root) gid=0(root) groups=0(root)



ZERO
NIGHTS
2018

2³
EDITION

Unfortunately, this talk is not about sophisticated hacking techniques (cause you do not need them to hack SD-WAN)



This talk about how to find those low-hanging fruits on the Internet?



ZERO
NIGHTS
2018

2³
EDITION

The Main Questions

- How many SD-WAN nodes on the Internet?
- Do we need new techniques to scan and fingerprint them?
- How to find vulnerable SD-WAN nodes?





ZERO
NIGHTS
2018

2³
EDITION

Approach

Best Effort

*When you have to underline the **best effort** approach but
you don't know exactly how to*



2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION



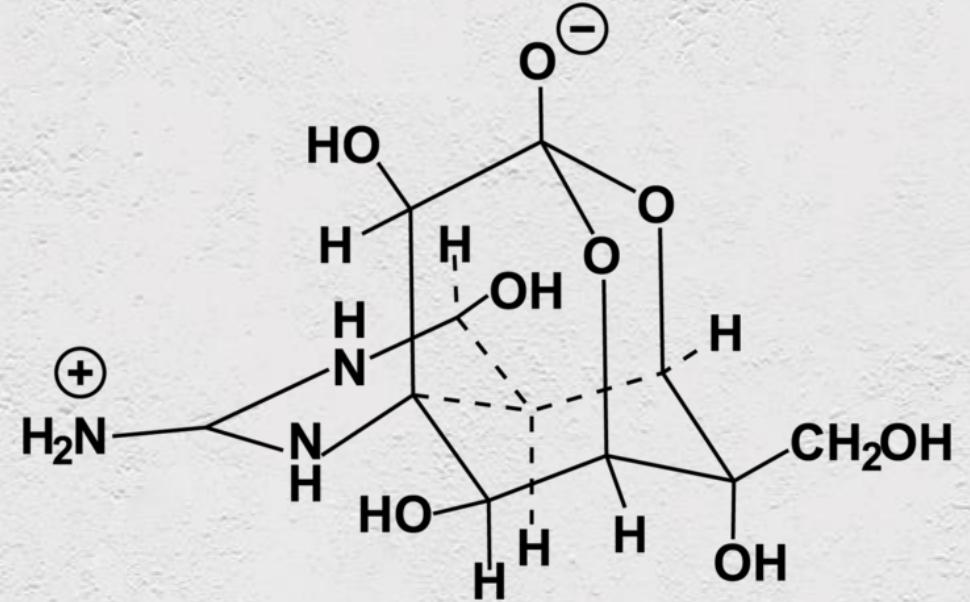
But nevertheless,
let's start!

2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

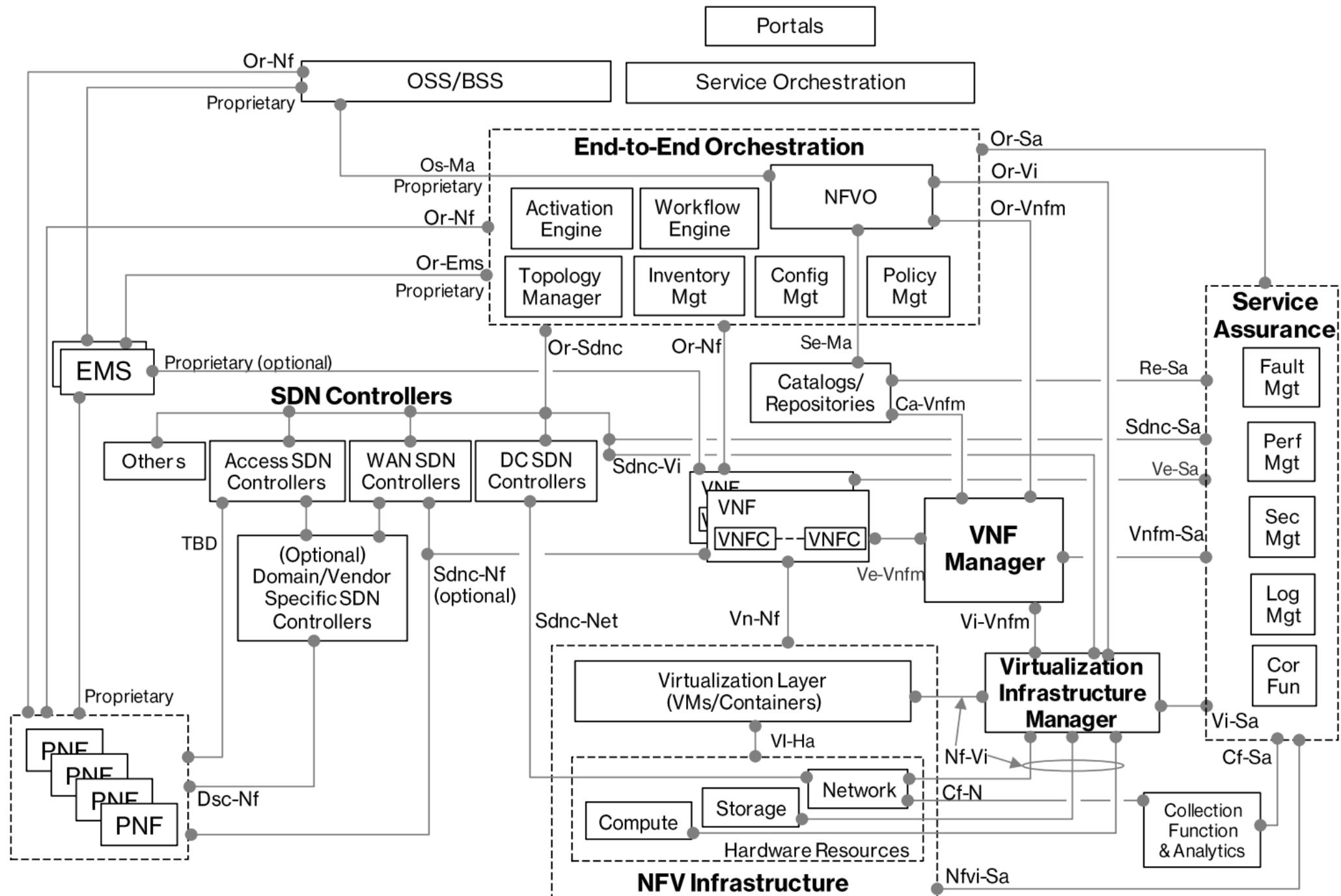
2³
EDITION



SD-WAN Essence

or

That Boring Part of Slides Again

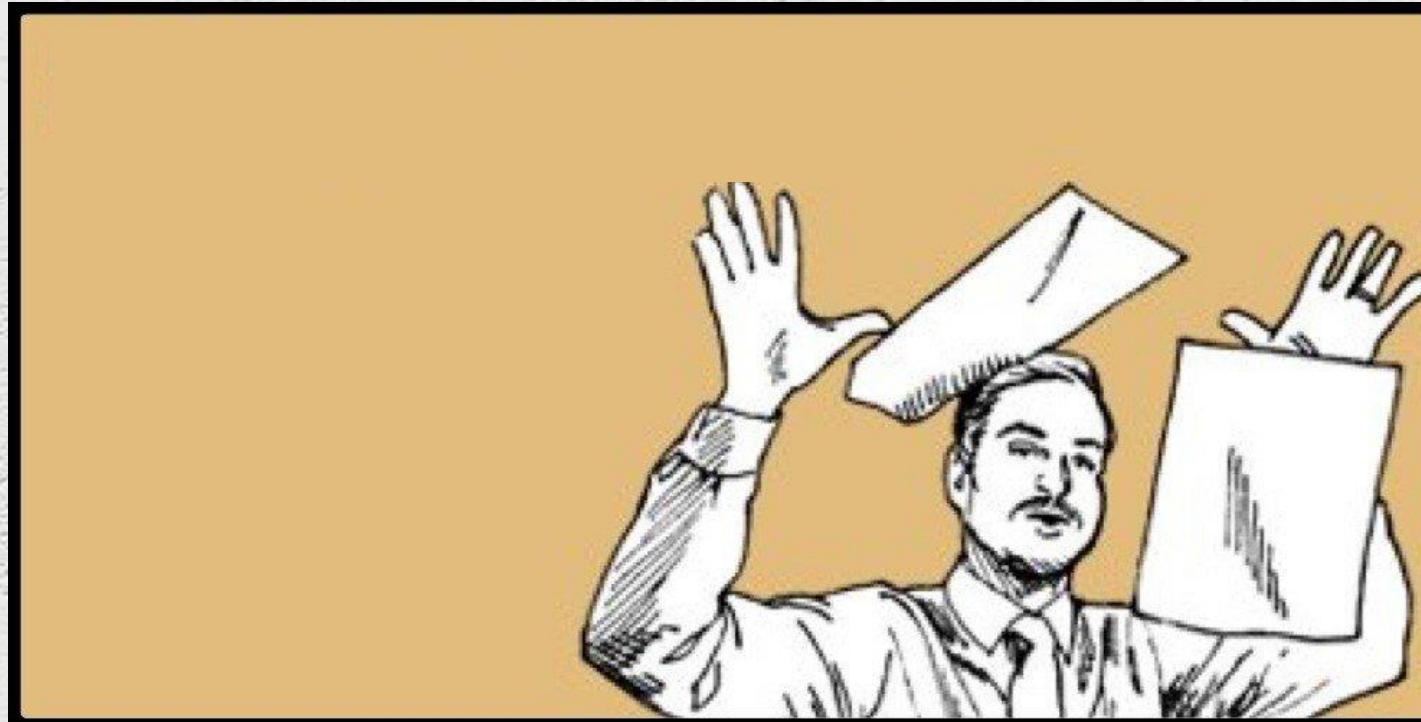




ZERO
NIGHTS
2018

2³
EDITION

F*ck that shit! We are hackers!



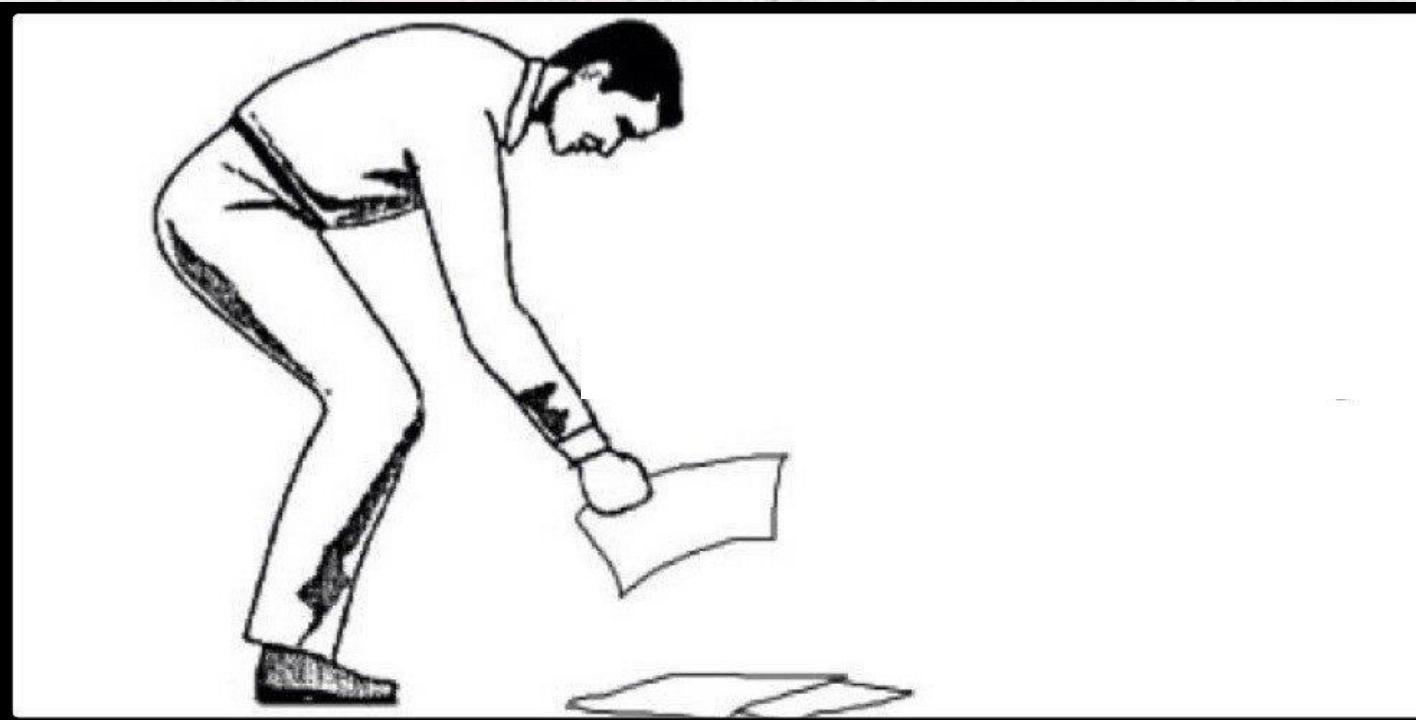
2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION

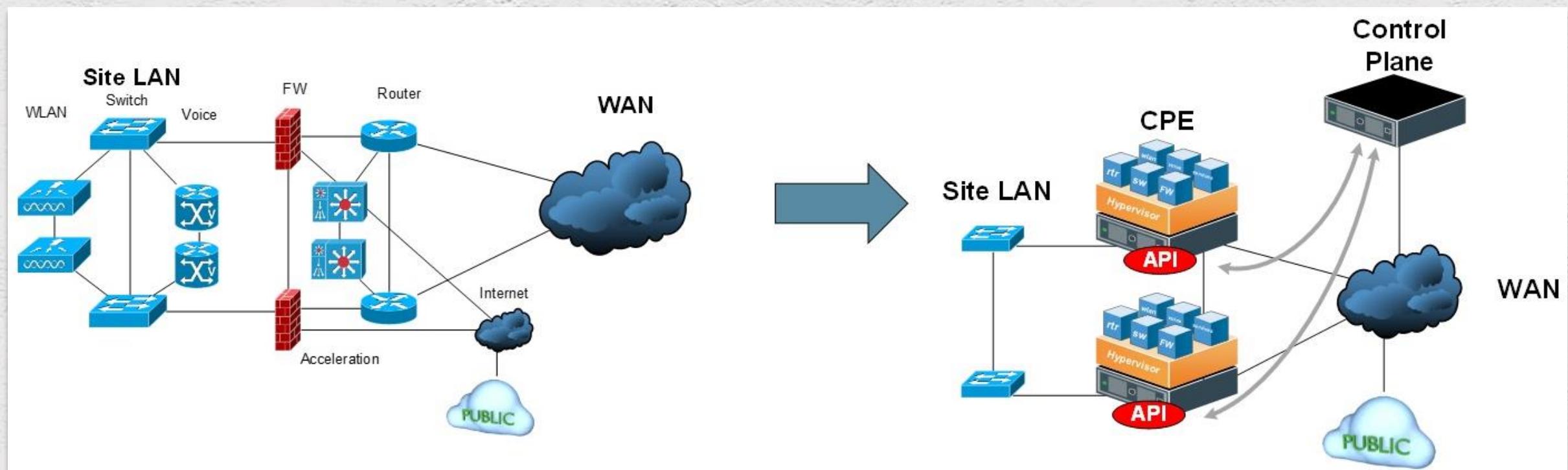
Just kidding.
We need it for understanding.



2018.ZERONIGHTS.ORG



Traditional WAN vs Software-defined WAN





ZERO
NIGHTS
2018

2³
EDITION

So, we are

Gotta catch 'em all!™



2018.ZERONIGHTS.ORG



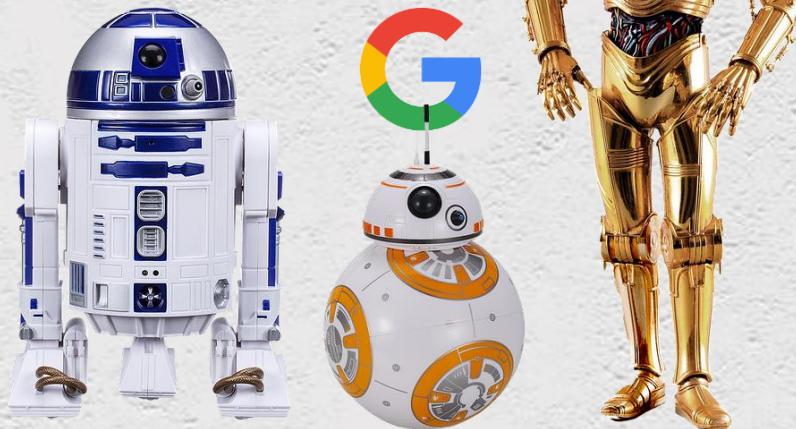
ZERO
NIGHTS
2018

2³
EDITION

Search Engines



SHODAN



2018.ZERONIGHTS.ORG



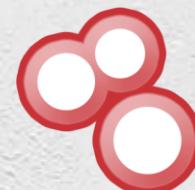
ZERO
NIGHTS
2018

2³
EDITION

Straightforward Examples



```
title:"Viptela vManage"
title:"Cisco vManage"
title:"Flex VNF Web-UI"
```



SHODAN

 censys



```
80.http.get.title: "Viptela vManage"
80.http.get.title: "Cisco vManage"
80.http.get.title: "Flex VNF Web-UI"
```



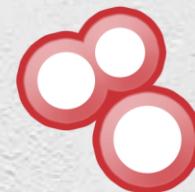
ZERO
NIGHTS
2018

2³
EDITION

More Sophisticated Examples



http.favicon.hash:-1338133217
ssl:"Riverbed Apache"



SHODAN

 censys



80.http.get.body_sha256:
"867f6fead63c8809f2..."



ZERO
NIGHTS
2018

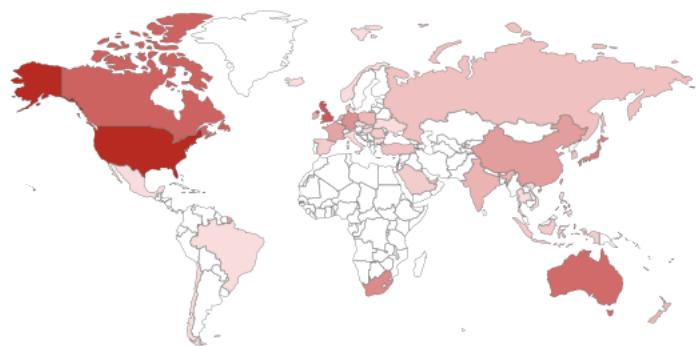
2³
EDITION

Query Correction

TOTAL RESULTS

488

TOP COUNTRIES



html : Sonus

←

+ title:
"SBC Management
Application"

→

TOTAL RESULTS

3

TOP COUNTRIES





More Query Correction!

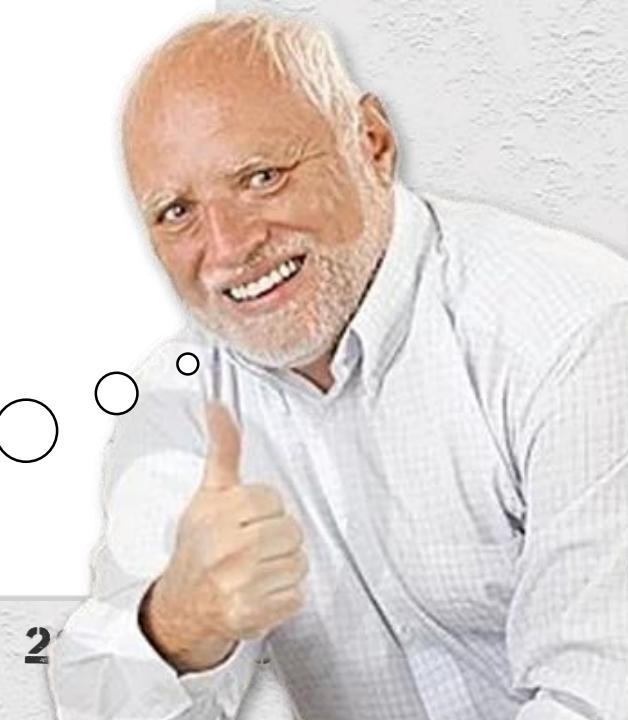
<https://github.com/sdnewhop/sdwannewhope/issues/7>



All Sonus results = 408:

- 349 - SBC:
 - 196 - SBC Edge
 - 150 - SBC 1000/2000 Web-interface
 - 3 - SBC Management Application
- 5 - SecureLink
- 5 - Configuration Management Unit
- 4 - FTP Servers
- 20 - Switches
- 24 - Trash

We can use
corrections to
build full
product map!





ZERO
NIGHTS
2018

2³
EDITION

Query Confidence



Tentative



Firm



Certain



ZERONIGHTS
2018

2³
EDITION



Bugbounty using SDNEWHOP queries

pikabu.ru

2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION



Version Leakage

2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION

Version Leakage Patterns



```
yalegko:~ $ ssh admin@REDACTED
viptela 17.2.4
admin@REDACTED password:
```



```
<h2 style="margin-top:5px;">FatPipe WARP</h2>
<h5>9.1.2r142</h5>
```



```
<link href="/br_ui/rdx/core/css/rdx.css?v=9.3.1.35" rel="stylesheet" type="text/css"/>
<link href="/br_ui/app/css/br.css?v=9.3.1.35" rel="stylesheet" type="text/css"/>
```



**ZERO
NIGHTS
2018**

**2³
EDITION**

How to Find Them All?

Let's help Dora!



2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION



We have a
leakage!



ZERO
NIGHTS
2018

2³
EDITION



We have a
NMAP!



2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION



2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION

SD-WAN Infiltrator



2018.ZERONIGHTS.ORG

Starting Nmap 7.70 (https://nmap.org) at 2018-11-21 02:14 RTZ 6 (ceia)
Nmap scan report for REDACTED
Host is up (0.13s latency).

PORT	STATE	SERVICE
80/tcp	open	http
infiltrator:		
status:	success	
method:	http-title	
product:	Citrix NetScaler SD-WAN VPX	
host_addr:	REDACTED	
_ host_port:	80	
443/tcp	open	https
infiltrator:		
status:	success	
method:	http-title	
product:	Citrix NetScaler SD-WAN VPX	
host_addr:	REDACTED	
host_port:	443	
_ version:	9.3.4.29	
161/udp	open filtered	snmp

Documents

2 semestr



ZERO
NIGHTS
2018

2³
EDITION

What About Really Hard Cases?

Easy Peasy Lemon Squeeezy?
Difficult Difficult Lemon Difficult!



2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION

SD-WAN version in
/etc/issue message



```
yalecko:~ $ ssh admin@REDACTED
viptela 17.2.4
admin@REDACTED password:
```

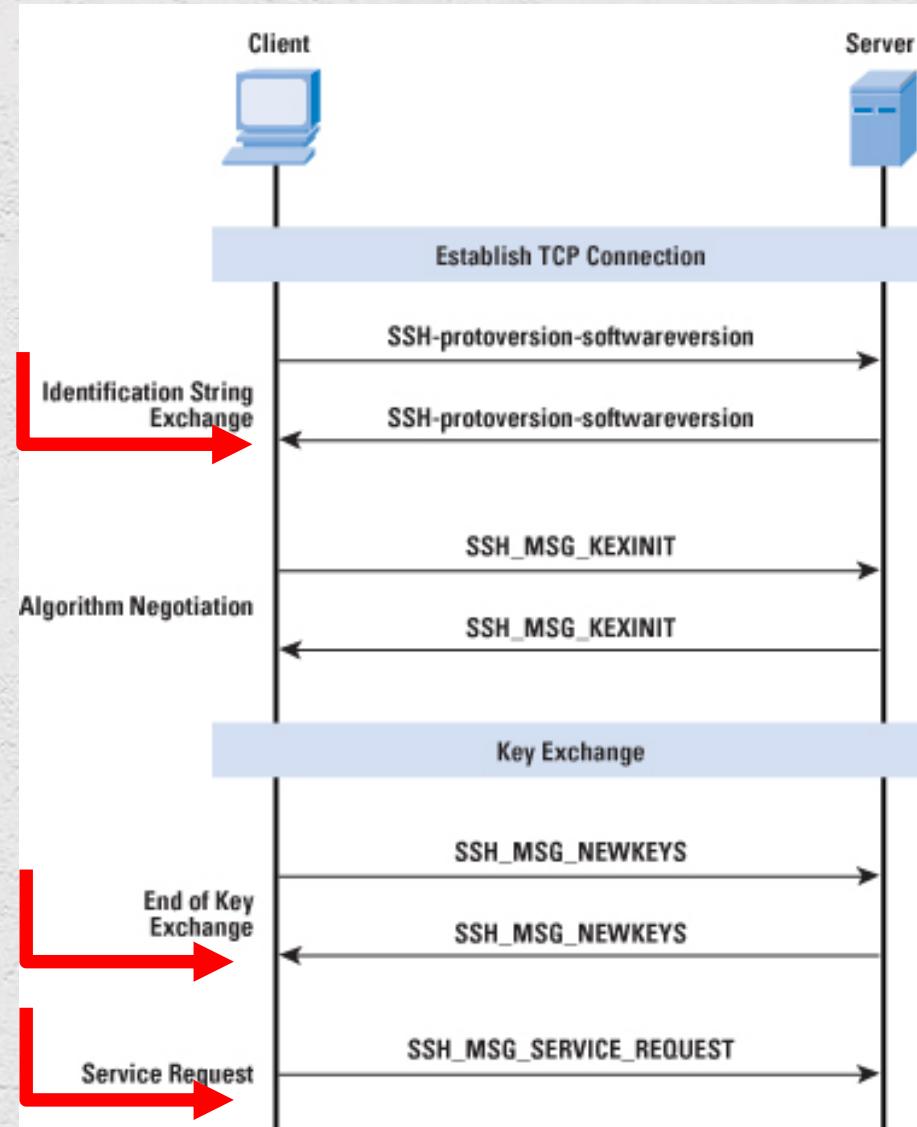


[/nmap/nmap/issues/1389](https://nmap/nmap/issues/1389)
[/sdnewhop/zgrab2](https://sdnewhop/zgrab2)

SSH Fingerprinting

masscan

zgrab
our
banner





ZERO
NIGHTS
2018

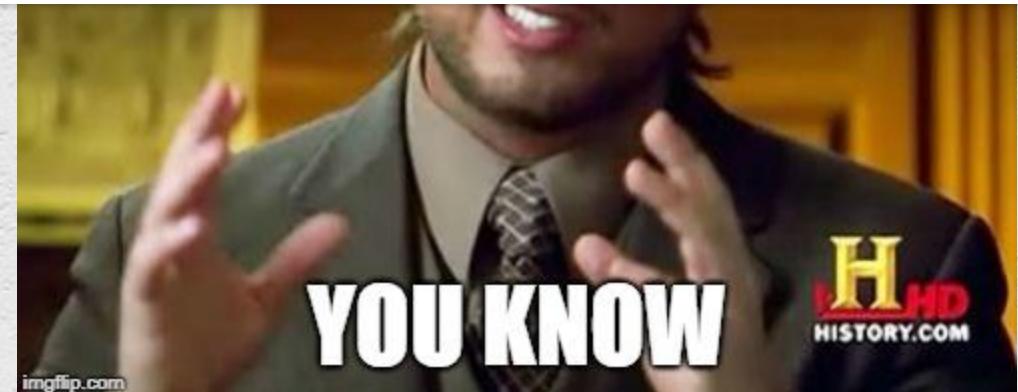
2³
EDITION

Websocket

- Nmap can't scan Websocket
- **No standard NSE** Websocket libraries
- Weird behavior in **custom** NSE Websocket libraries



```
▼431[{type: "sync", complete: true,...}]  
  ▼0: {type: "sync", complete: true,...}  
    complete: true  
    payload: "{#  "gluware_version": {#  
      type: "sync"  
    }"name": "Gluware 3.4",#  
  }"
```



imgflip.com



ZERO
NIGHTS
2018

2³
EDITION

Indirect Version Leakage

Riverbed SteelHead

Disclosure: indirect version

Source: HTML

Example:

```
<meta name="application-name" content="web3 v0.15.8" />
```

Teloip Orchestrator API

Disclosure: API version

Source: HTML

Example:

```
{"usage": "append '?debug=requestinfo' to any querystring. Optional params: virtualPathCount",  
"host": "_v5.02_Teloip Orchestrator API", "hostType": "SelfHost (AppHostBase)", ...}
```

VeloCloud Network Orchestrator

Disclosure: UI info

Source: HTTP response

Example:

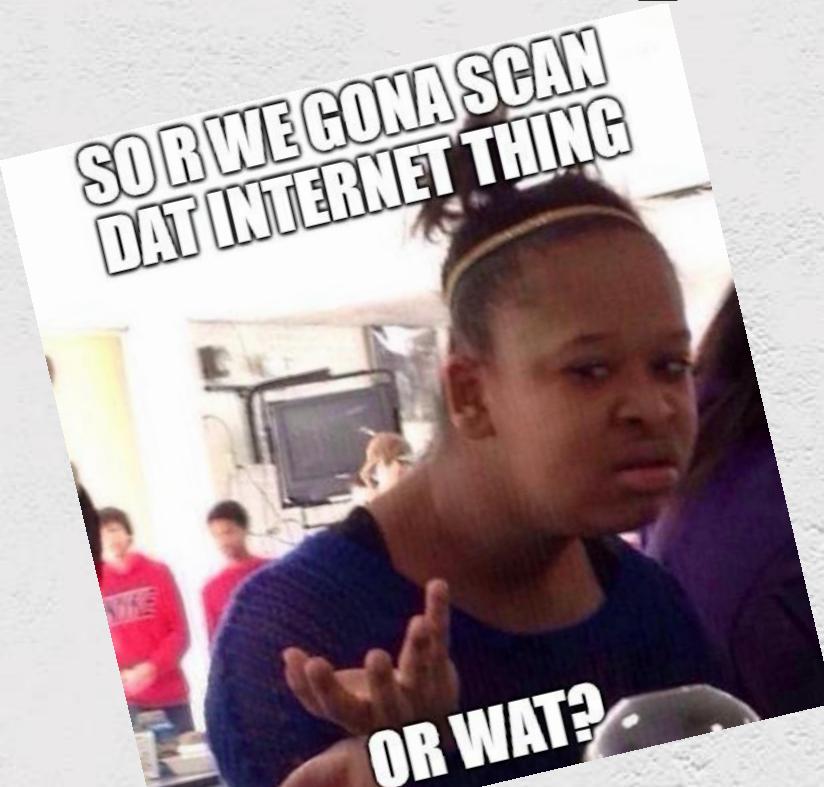
```
<link href="/css/vco-ui.3.0.0.1509625568730.common.css" rel="stylesheet">
```



ZERO
NIGHTS
2018

2³
EDITION

Stop! What about Internet scanning?



2018.ZERONIGHTS.ORG

**Almost same time
Almost same place**



You should scan
all Internet using
`masscan`

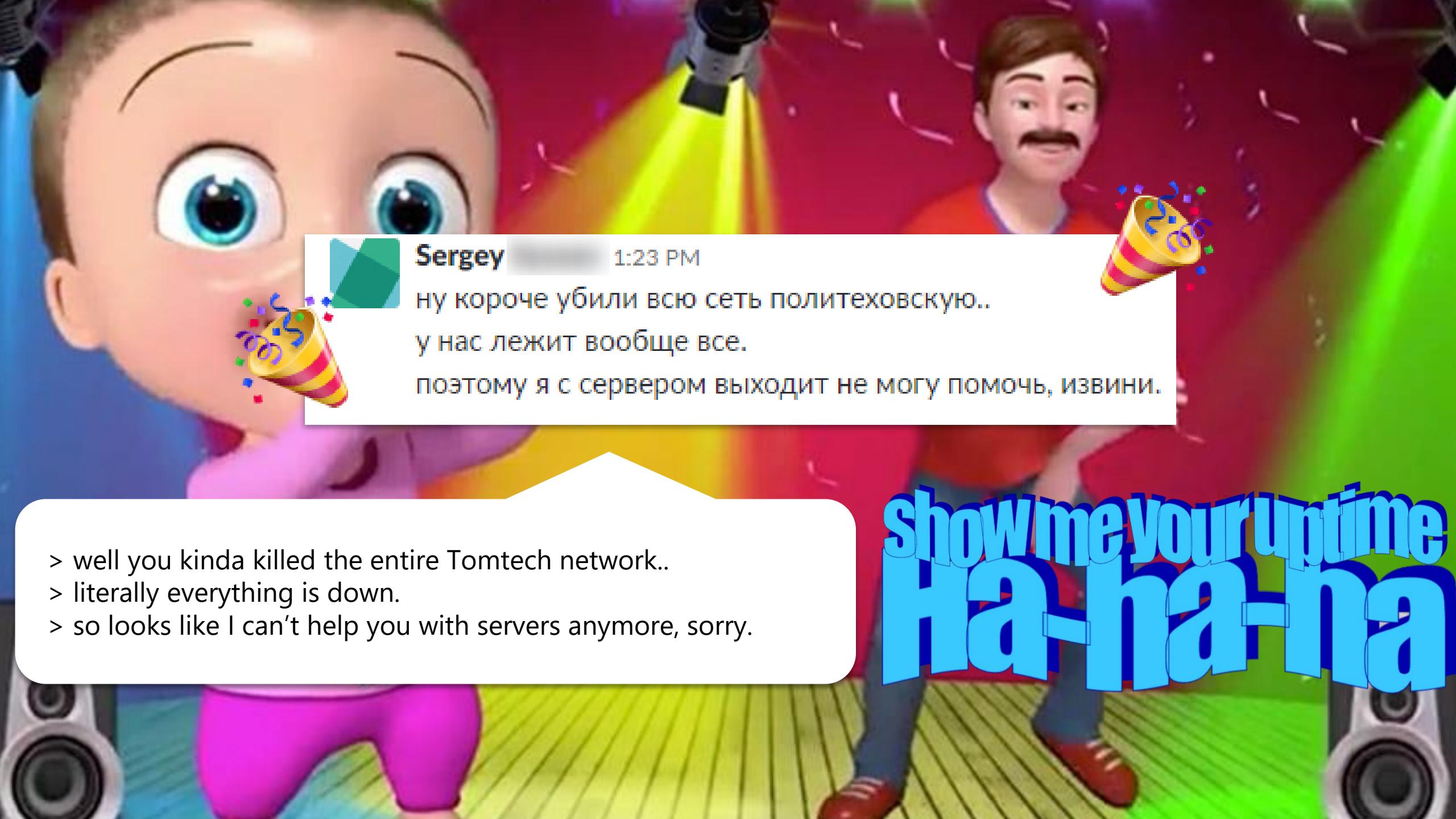


ZERO
NIGHTS
2018

2³
EDITION



- Johny, Johny?
- Yes, papa
- Scanning Internet?
- No, papa
- Telling lies?
- No, papa

A cartoon illustration of a baby with large blue eyes and a blue headband, wearing a yellow and red striped party hat. The background is a vibrant, colorful stage with spotlights and confetti falling.

Sergey

1:23 PM

ну короче убили всю сеть политеховскую..
у нас лежит вообще все.
поэтому я с сервером выходит не могу помочь, извини.

> well you kinda killed the entire Tomtech network..
> literally everything is down.
> so looks like I can't help you with servers anymore, sorry.

show me your uptime
на-на-на

And now back



ZERO
NIGHTS
2018

2³
EDITION

SD-WAN Harvester



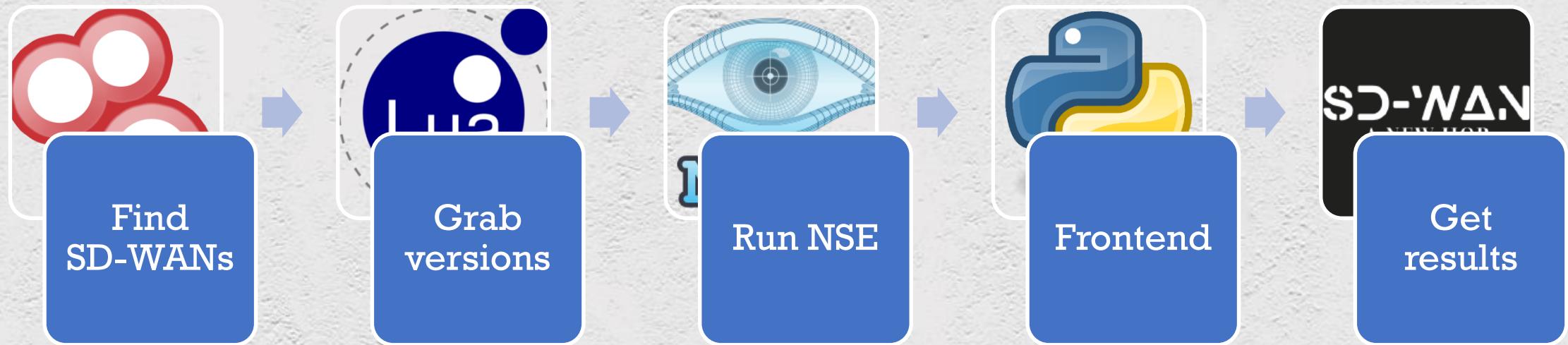
2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION

SD-WAN Harvester Workflow





ZERO
NIGHTS
2018

2³
EDITION



drum roll
please...

Results

2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION

SD-WAN Map



2018.ZERONIGHTS.ORG

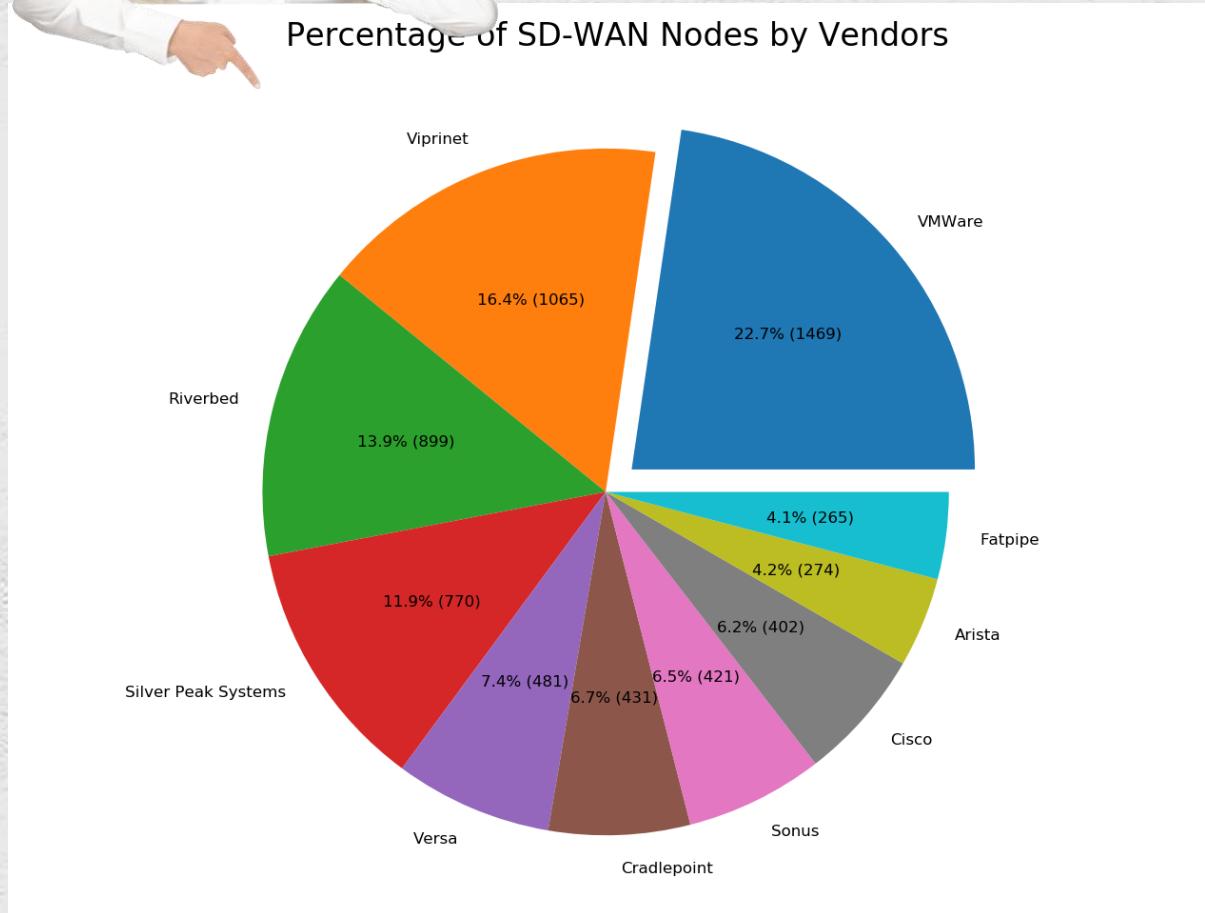


ZERO
NIGHTS
2018

2³
EDITION



Top of founded SD-WAN Vendors





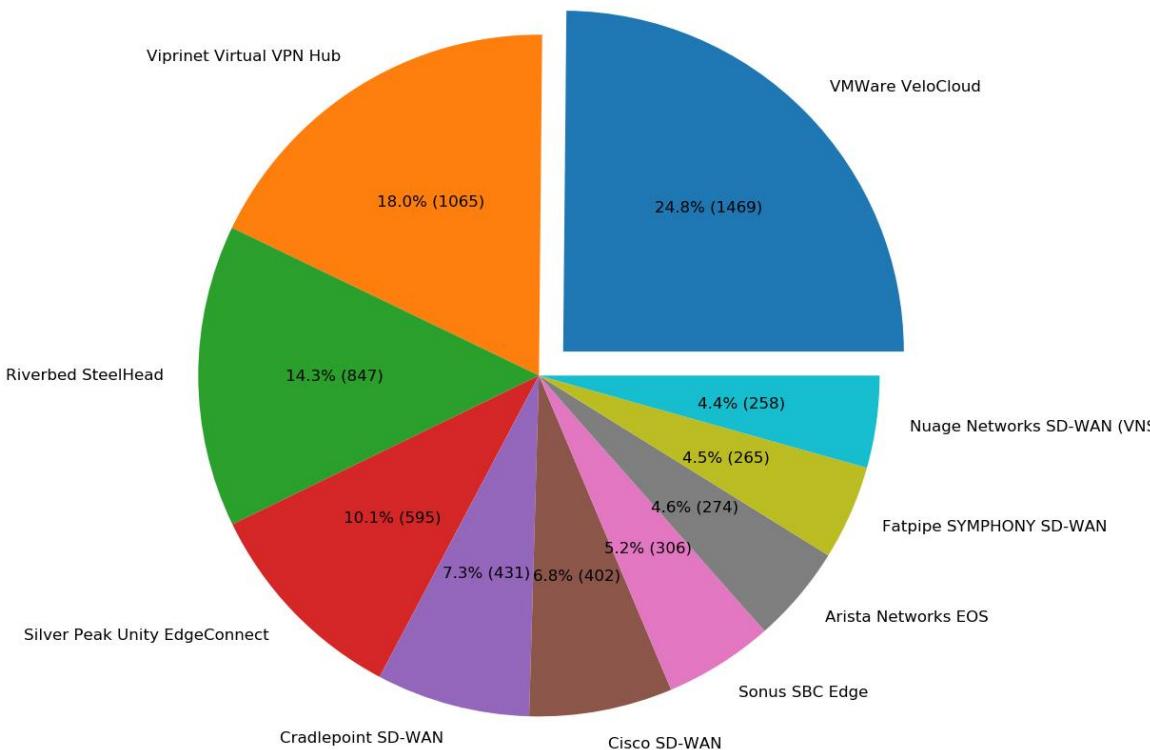
ZERO
NIGHTS
2018

2³
EDITION



Top of founded SD-WAN Solutions

Percentage of SD-WAN Nodes by Products



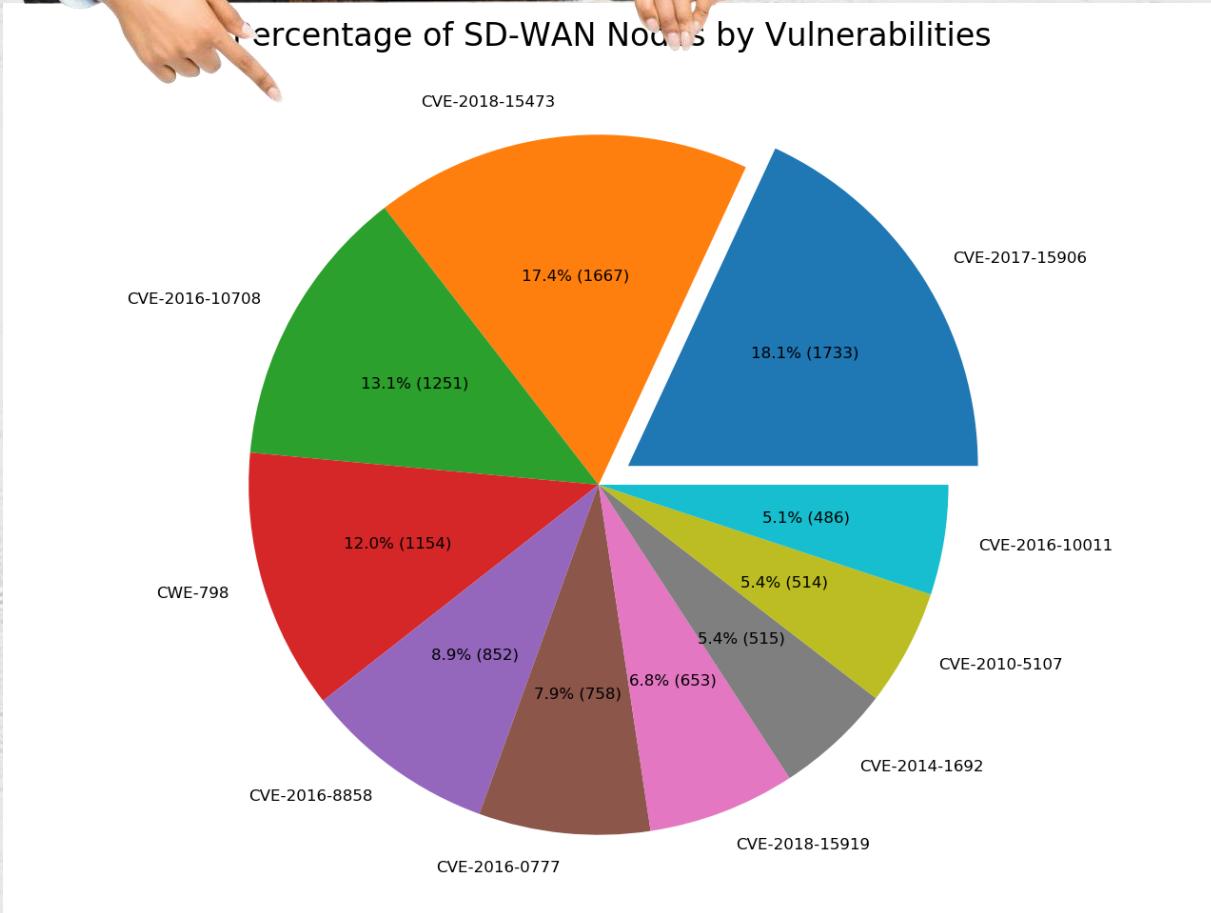


ZERO
NIGHTS
2018

2³
EDITION



Top SD-WAN Vulnerabilities





ZERO
NIGHTS
2018

2³
EDITION

Harvester Charts

But seriously, harvester can build next pie charts by:

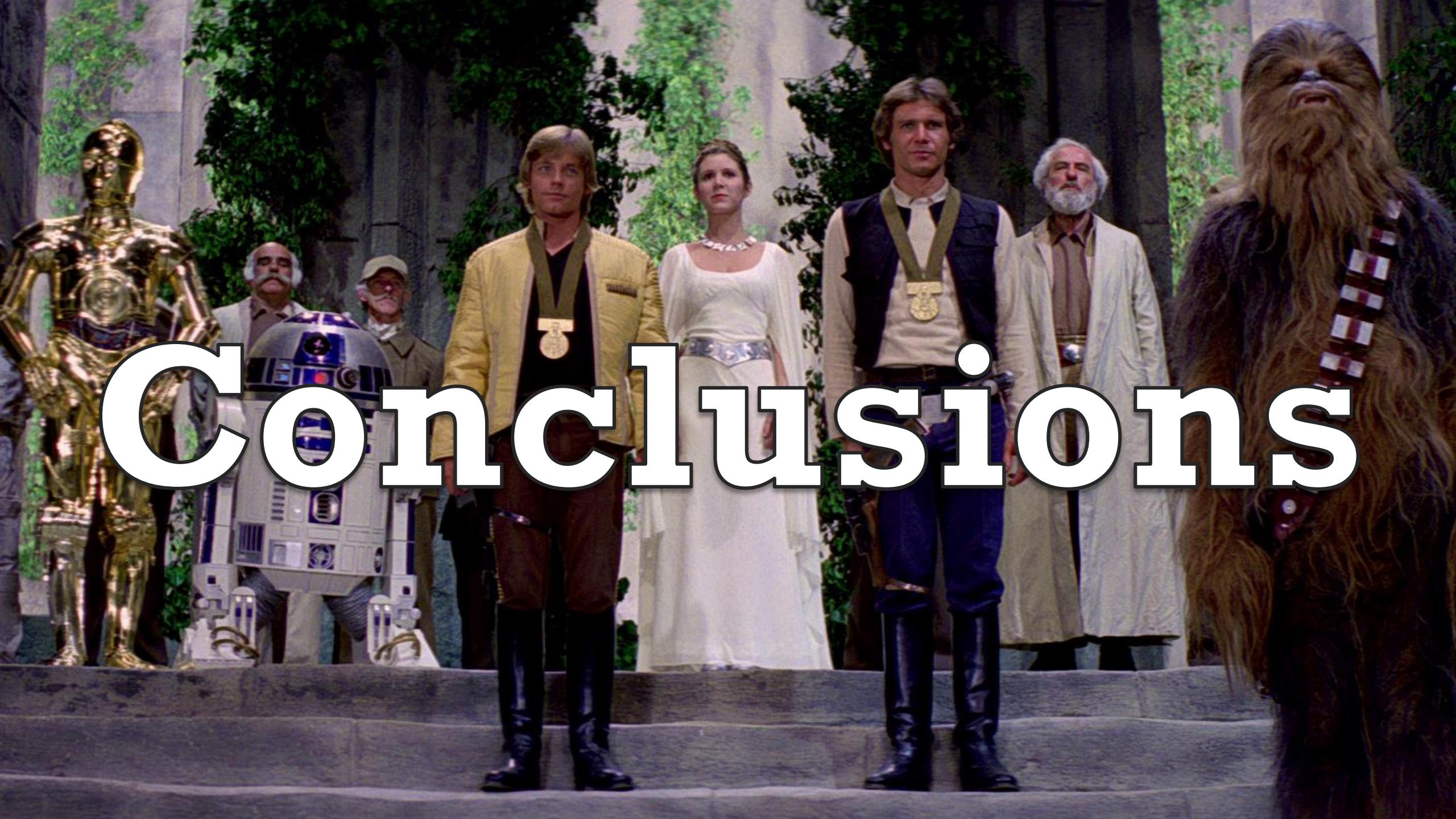
- vulnerabilities
- vendors
- products
- countries
- continents



<https://github.com/sdnewhop/sdwan-harvester/tree/master/samples>



Conclusions





ZERO
NIGHTS
2018

2³
EDITION

Conclusions

- Many different vendors and related products have been found
- Most products are susceptible to version leakage
- More often products are leaky and vulnerable





ZERO
NIGHTS
2018

2³
EDITION

SD-WAN New Hope

- Sergey Gordeychik
- Denis Kolegov
- Oleg Broslavsky
- Max Gorbunov
- Nikita Oleksov
- Nikolay Tkachenko
- Anton Nikolaev
- SD-WAN Internet Census
- SD-WAN Harvester
- SD-WAN Infiltrator
- SD-WAN Threat Landscape



<https://github.com/sdnewhop/>

THANKS FOR ATTENTION

@dnkolegov

@yalegko

@manmoleculo

