Bro Network Programming Language & Bro-ids v2.1

Detecting Expiring SSL Certificates

Presented by
Liam Randall
2013-3

ABOUT ME

History

- 17 Years Consulting (1995)
- BS in CS from XU
- Dozens of Vender Certs
- Speak/Train- Shmoocon, Skydogcon
- “Applied NSM” Summer of 2013

- #Bro
- #SecurityOnion

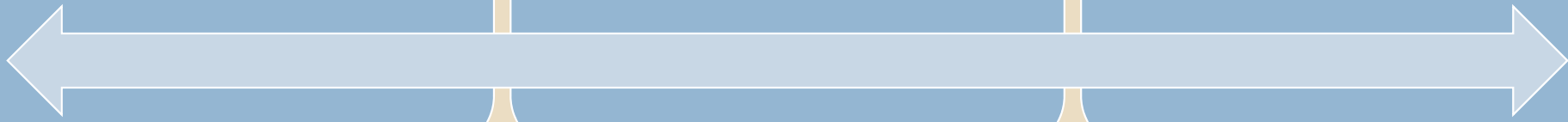
- Liam.Randall@gmail.com
- @Hectaman Twitter/IRC

LINKS

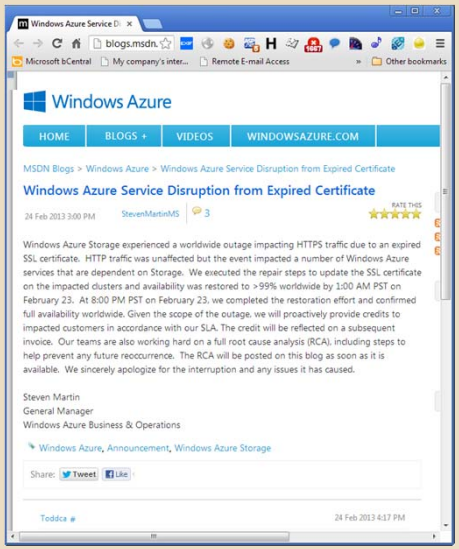
github.com/bro
github.com/liamrandall

#Bro_IDS
@Hectaman
@Bro_IDS

http://bro-ids.org
http://liamrandall.com



OVERVIEW



"Can Bro IDS tell me when my SSL/TLS Certificates are about to expire?"

It already does.

FOLLOW ALONG

Documentation

http://www.bro-ids.org/documentation-git/scripts/policy/protocols/ssl/expiring-certs.html

TL;DR: Add the following to your local.bro

- @load policy/protocols/ssl/expiring-certs.bro
- redef SSL::notify_certs_expiration = ALL_HOSTS;

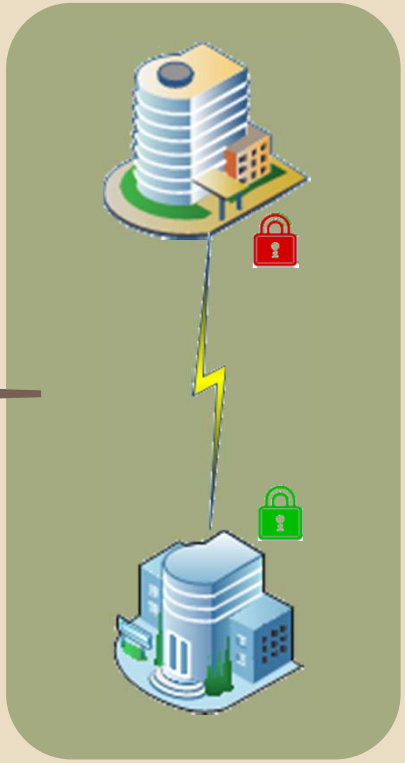
(**LOCAL_HOSTS**, REMOTE_HOSTS, ALL_HOSTS, NO_HOSTS)

SSL/TLS USE CASES

Widespread

+ Credit Checks
+ Authorization and Accounting
+ Supply Chain Management
+ e-Commerce
+ Marketing

HTTPS	SMTP POP/IMAP	SSL/TLS VPN	SIP (DTLS)



DEMONSTRATION

```
@load policy/protocols/ssl/expiring-certs.bro
redef SSL::notify_certs_expiration = ALL_HOSTS;
```

```
sudo broctl check
sudo broctl install
sudo broctl restart
```

DEMONSTRATION

```
@load policy/protocols/ssl/expiring-certs.bro
redef SSL::notify_certs_expiration = ALL_HOSTS;
```

```
sudo broctl check
sudo broctl install
sudo broctl restart
```

DEMONSTRATION

```
@load policy/protocols/ssl/expiring-certs.bro
redef SSL::notify_certs_expiration = ALL_HOSTS;
sudo broctl check
sudo broctl install
sudo broctl restart
```

DEMONSTRATION

```
@load policy/protocols/ssl/expiring-certs.bro
redef SSL::notify_certs_expiration = ALL_HOSTS;
sudo broctl check
sudo broctl install
sudo broctl restart
```

DEMONSTRATION

```
@load policy/protocols/ssl/expiring-certs.bro
redef SSL::notify_certs_expiration = ALL_HOSTS;
sudo broctl check
sudo broctl install
sudo broctl restart
```

DEMONSTRATION

```
@load policy/protocols/ssl/expiring-certs.bro
redef SSL::notify_certs_expiration = ALL_HOSTS;
sudo broctl check
sudo broctl install
sudo broctl restart
```

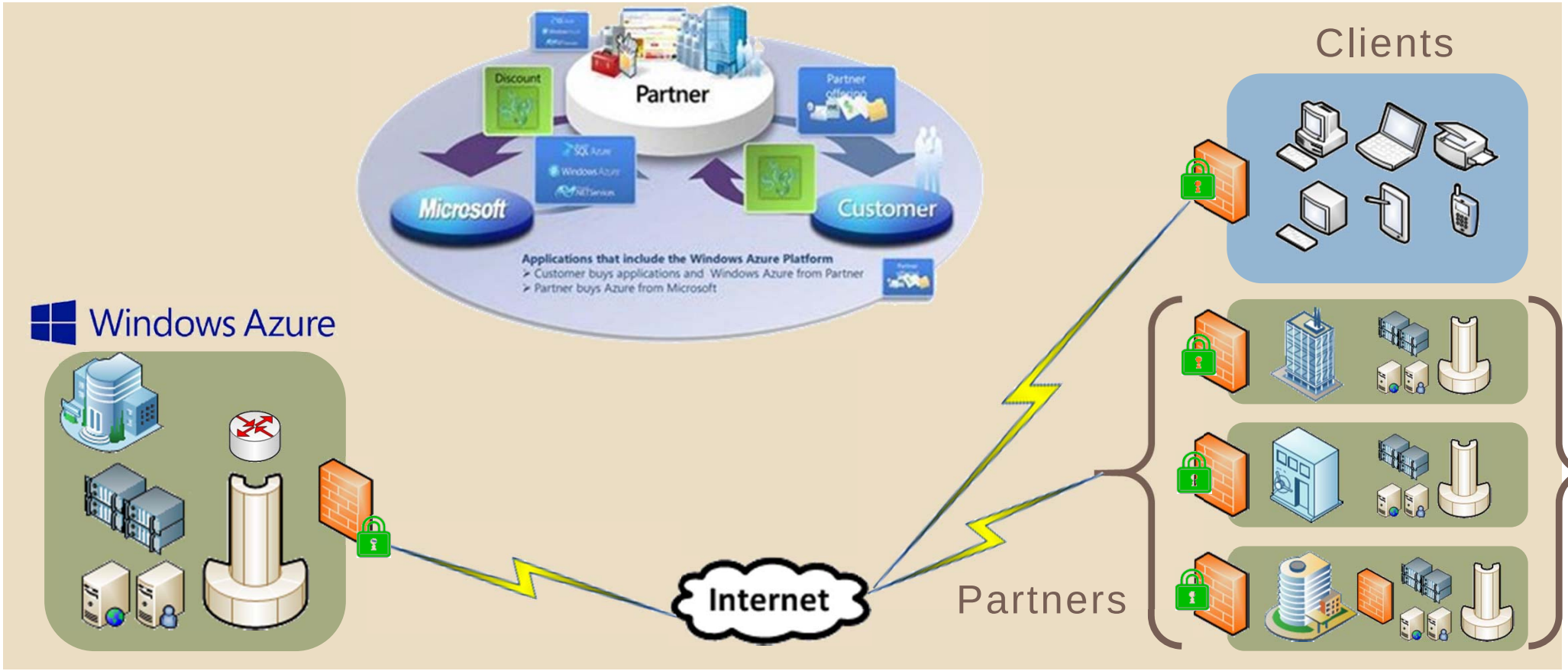
DEMONSTRATION

```
@load policy/protocols/ssl/expiring-certs.bro
redef SSL::notify_certs_expiration = ALL_HOSTS;
sudo broctl check
sudo broctl install
sudo broctl restart
```

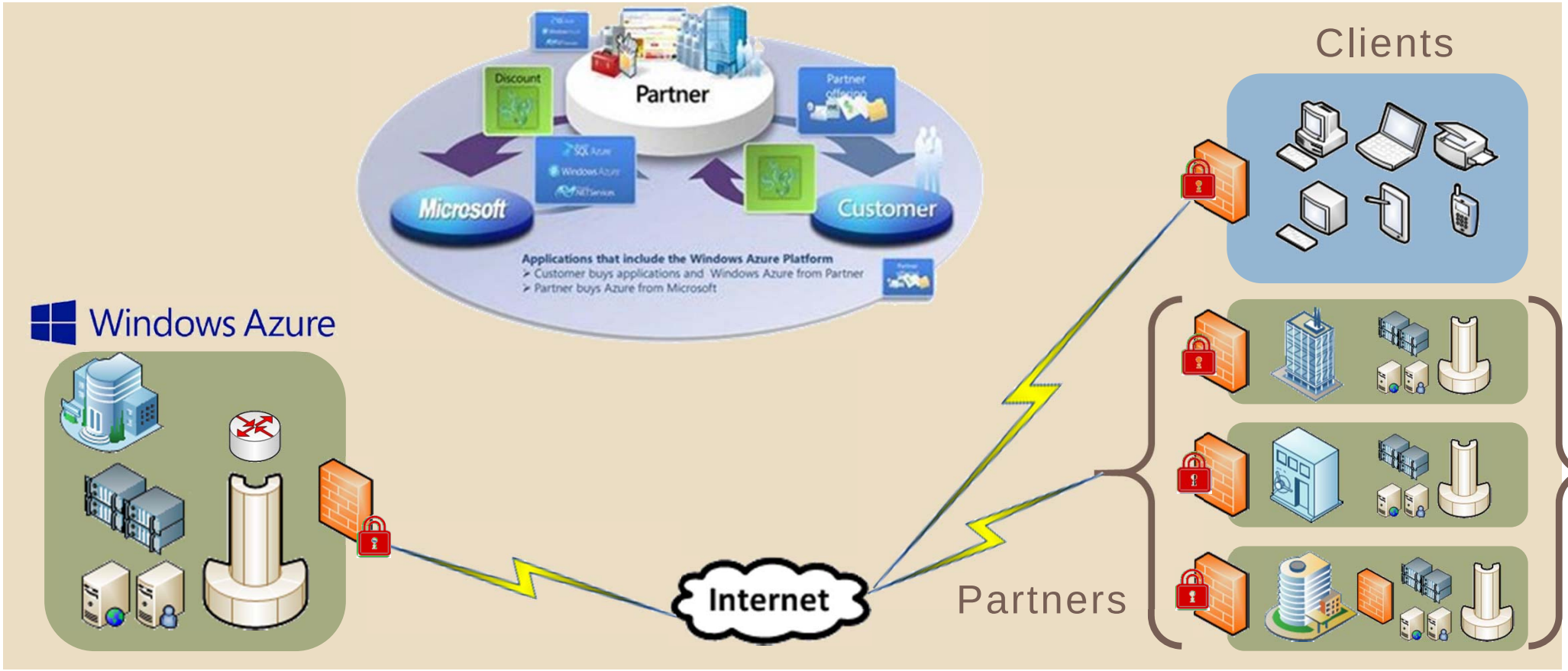
- or test from the command line -

```
bro –r test.pcap expiring-certs.bro config.bro
```

REAL WORLD: TLS EDITION

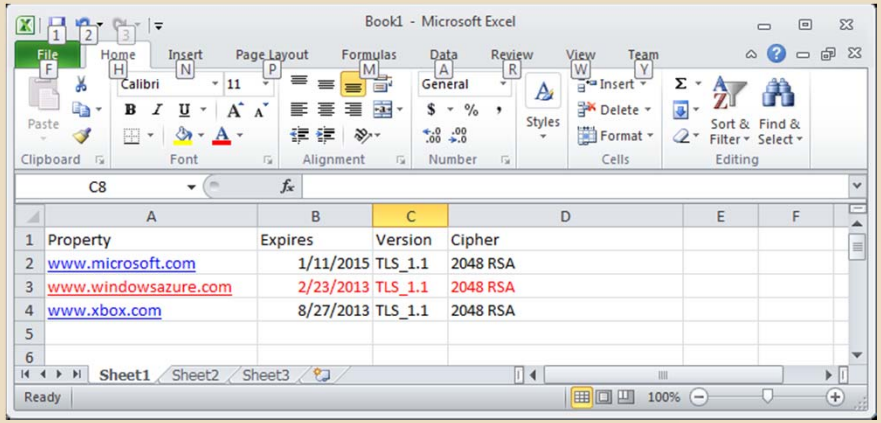


REAL WORLD: TLS EDITION

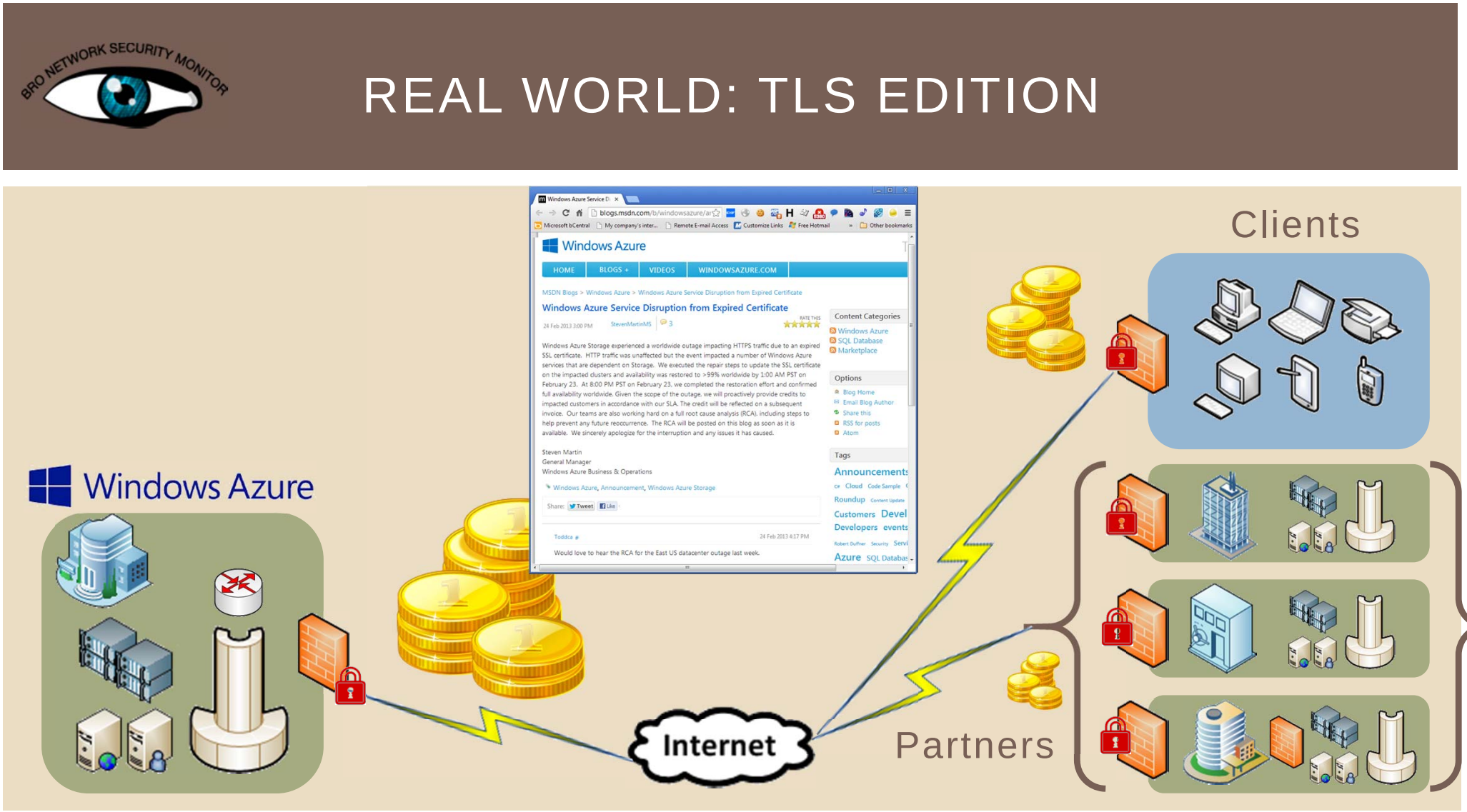


REAL WORLD: TLS EDITION

REAL WORLD: TLS EDITION



	A	B	C	D
1	Property	Expires	Version	Cipher
2	www.microsoft.com	1/11/2015	TLS_1.1	2048 RSA
3	www.windowsazure.com	2/23/2013	TLS_1.1	2048 RSA
4	www.xbox.com	8/27/2013	TLS_1.1	2048 RSA
5				
6				


BRO NETWORK SECURITY MONITOR
REAL WORLD: TLS EDITION
Windows Azure
Windows Azure
HOME
BLOGS +
VIDEOS
WINDOWSAZURE.COM
Windows Azure Service Disruption from Expired Certificate
Windows Azure Storage experienced a worldwide outage impacting HTTPS traffic due to an expired SSL certificate. HTTP traffic was unaffected but the event impacted a number of Windows Azure services that are dependent on Storage. We executed the repair steps to update the SSL certificate on the impacted clusters and availability was restored to >99% worldwide by 1:00 AM PST on February 23. At 8:00 PM PST on February 23, we completed the restoration effort and confirmed full availability worldwide. Given the scope of the outage, we will proactively provide credits to impacted customers in accordance with our SLA. The credit will be reflected on a subsequent invoice. Our teams are also working hard on a full root cause analysis (RCA), including steps to help prevent any future reoccurrence. The RCA will be posted on this blog as soon as it is available. We sincerely apologize for the interruption and any issues it has caused.
Steven Martin
General Manager
Windows Azure Business & Operations
Would love to hear the RCA for the East US datacenter outage last week.
Clients
Internet
Partners

REAL WORLD: TLS EDITION

Clients

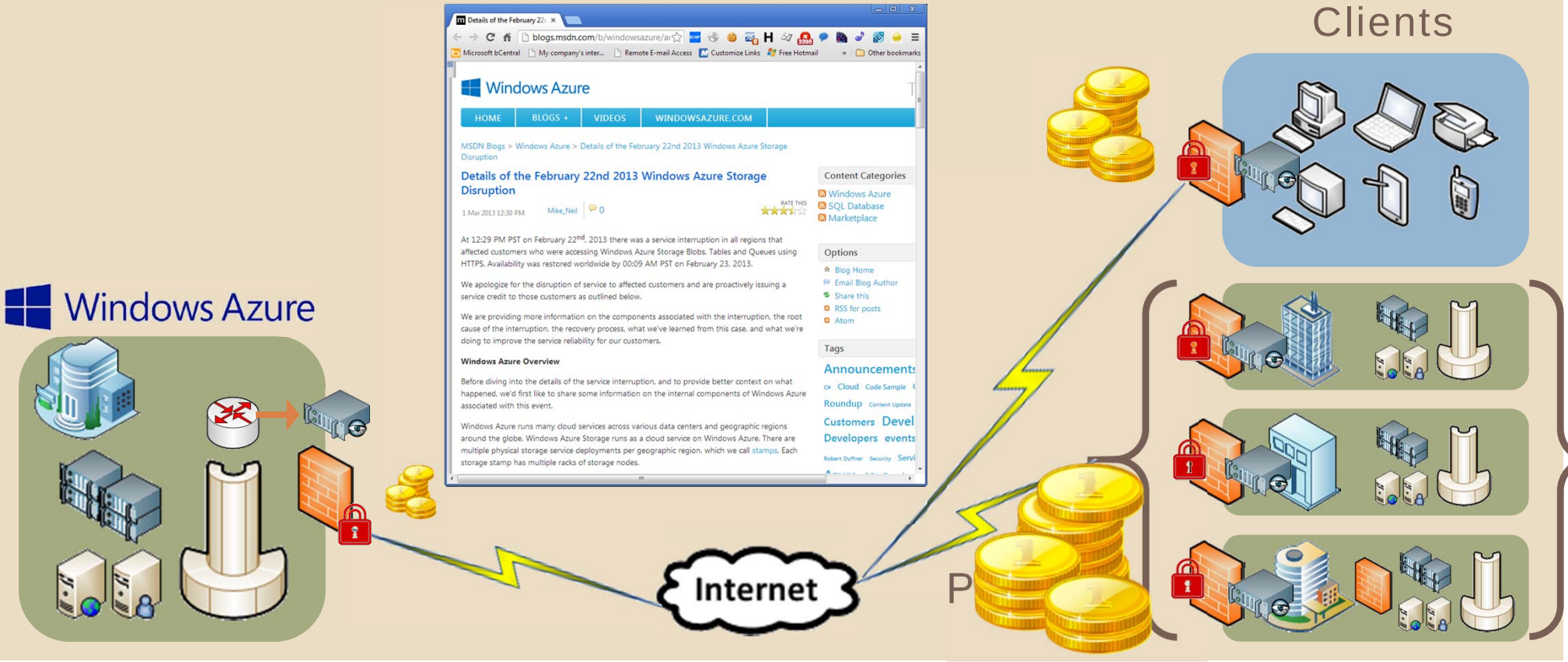
Windows Azure

Internet

Partners

REAL WORLD: TLS EDITION

REAL WORLD: TLS EDITION



CONCLUSION

"How much will it cost your organization to not run Bro IDS?"