RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: MBS-T11

Battling Daily Cyberattacks: A Day in the Life of Orange Israel's CISO

Arieh Shalem

Chief Information Security Officer
Orange Israel
@ariehs

#RSAC

Who Am I?

43 Y,
M + 3

>25 Y IT & IS EXPERIENCE

FROM CISO TO CCMM

3 Y @ ORANGE ISRAEL AS CCMM

FAMOUS FOR: “YES, I’LL APPROVE IT BUT…”

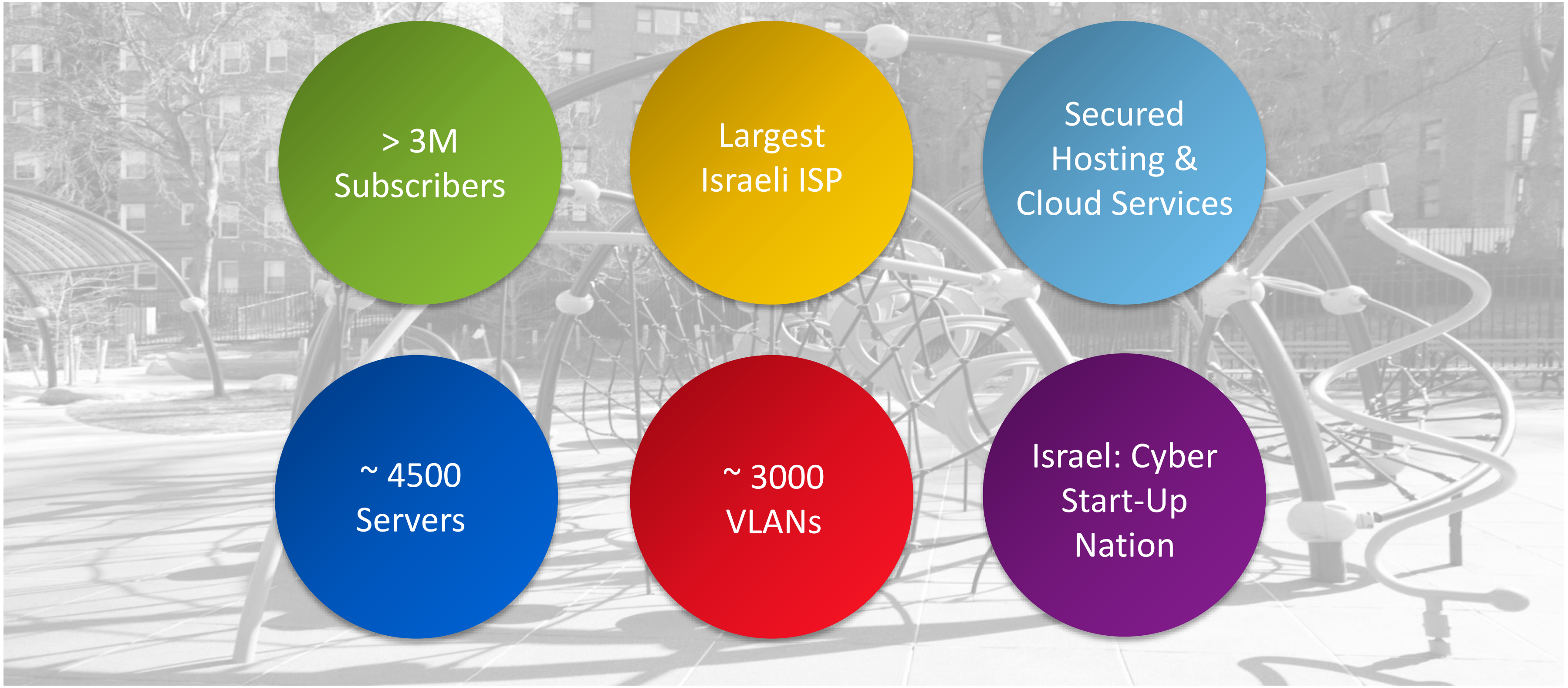
MY EMAILS ARE SIGNED WITH THE CISO OATH:

IN GOD WE TRUST -
THE REST WE MONITOR ☺

Let’s Talk About…

- My office day
- Cyber for 4G TELCO era
- Network & employee protection
- On-premise \ Hybrid \ Cloud
- SIEM\SOC challenges
- Cyber security: 2016 & beyond

My Playground



> 3M Subscribers

Largest Israeli ISP

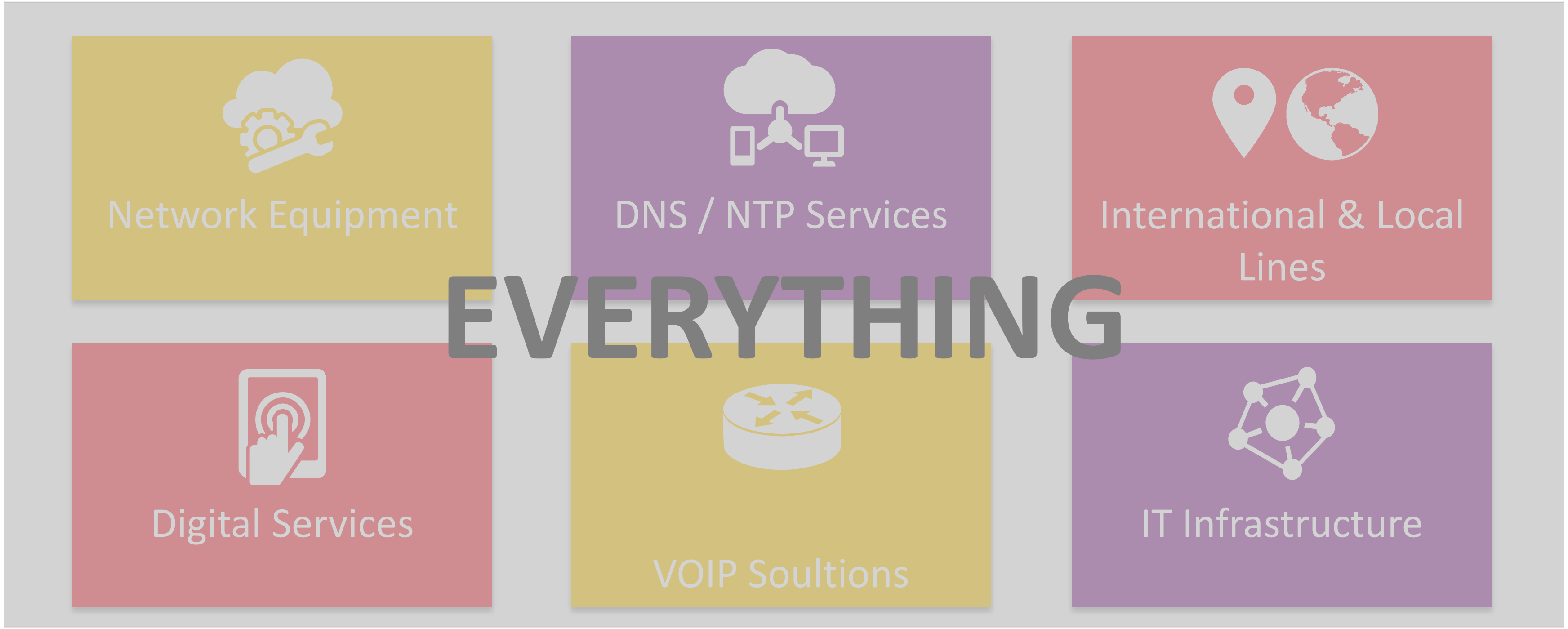
Secured Hosting & Cloud Services

~ 4500 Servers

~ 3000 VLANs

Israel: Cyber Start-Up Nation

Main Assets Requiring Protection



Network Equipment

DNS / NTP Services

International & Local Lines

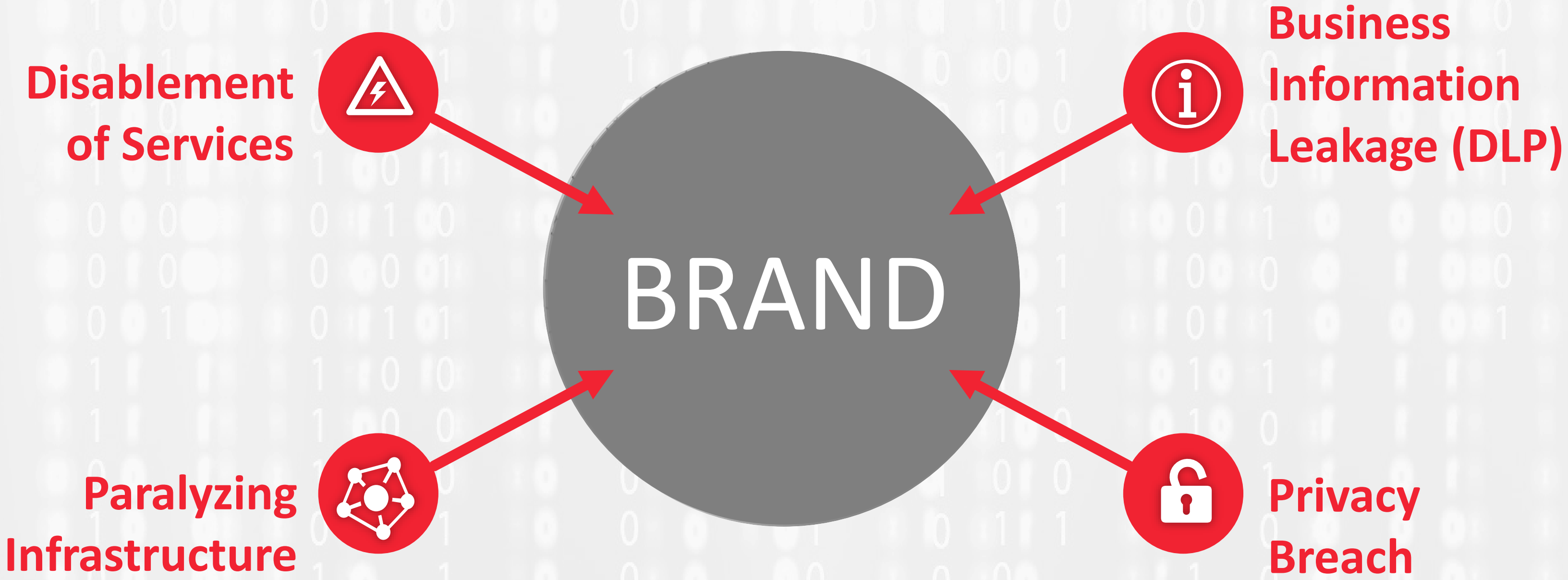
EVERYTHING

Digital Services

VOIP Soultions

IT Infrastructure

Potential Cyber Threat Disasters



A Day in the Life of a CISO in Israel…

Working

SLA 24/7*

response ti

VoLTE

C

ON-CALL

Employee meeti

WIFI calling

meeting

4G/5G designs

technologies

DDoS Protection at its Best!

- Allot Service Gateway Tera framework: One year
- Provides best DPI & DDoS
- Manual\Auto Block: Allot ServiceProtector
- Full SIEM\SOC integration

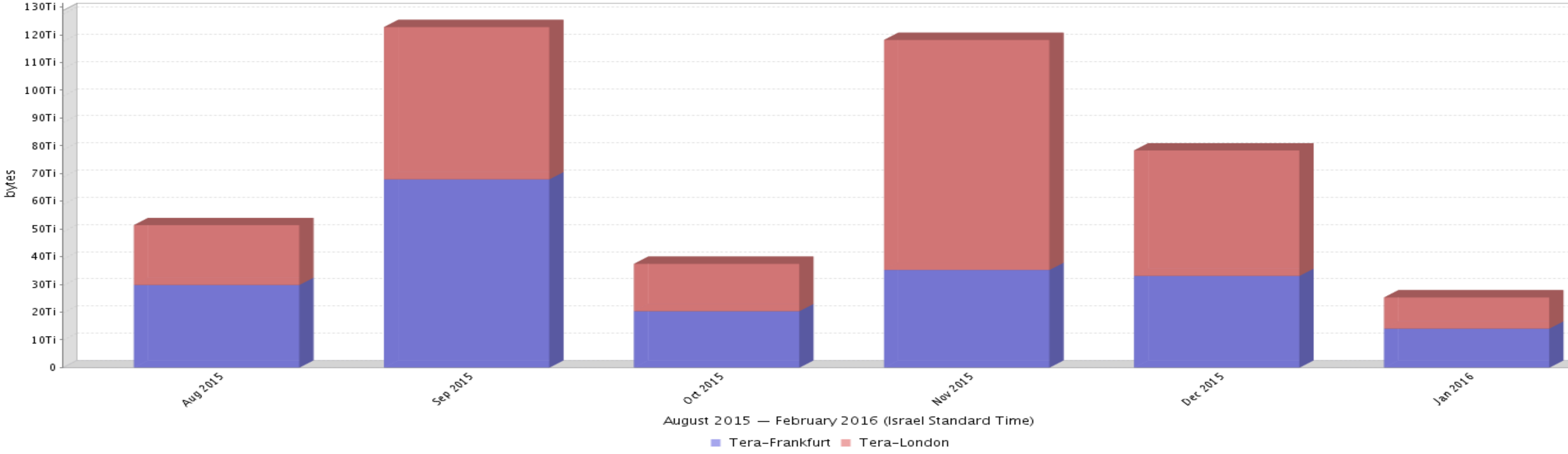
Last Year, Allot ServiceProtector Saved our Network from Several Huge DDoS Attacks with ZERO False Positives!

Allot communications

orange™ Partner

ALLOT SERVICEPROTECTOR GRAPH

780 TB not legit traffic blocked in the last 6 month!

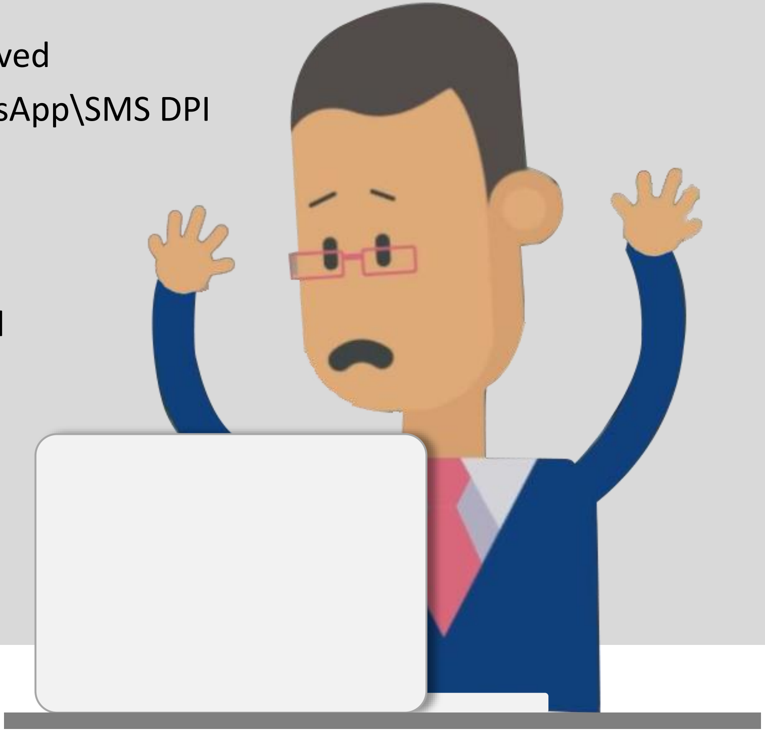


orange Partner

Zero-Day\APT Madness: The Counter Strike

Network Protection

- Ability to receive ZD\APT removed
- Mail\web\FTP\CyberArc\WhatsApp\SMS DPI
- Network anomalies monitored
- Traffic recorded & monitored
- HoneyPot solutions
- SSL traffic monitored & blocked
- Cloud secured
- Everything goes to SIEM\SOC…



Zero-Day\APT Madness: The Counter Strike

End Point Protection

- Admin privileges restricted
- Malicious code blocked
- Web browsing secured
- DOK removed
- ZD\APT solution implemented

Attacking Phishing Attacks

Huge ransomware attack blocked!

Employee Awareness Education

Monthly Cyber Training

Demos, Lectures & *Drama*

cyberspace DATA SECURITY

Cyber terrorism: counter-measures

It sounds scary no matter how one frames the issue. Clearly there is need to accelerate the requisite counter-measures suggested by those who know the full dimension of the problem. The tragedy could well be that the demands of Information Technology could carry within itself the seeds of insecurity.

[illegible]

Unprepared

New techniques

Large loophole

Three-stage attack

Counter measures

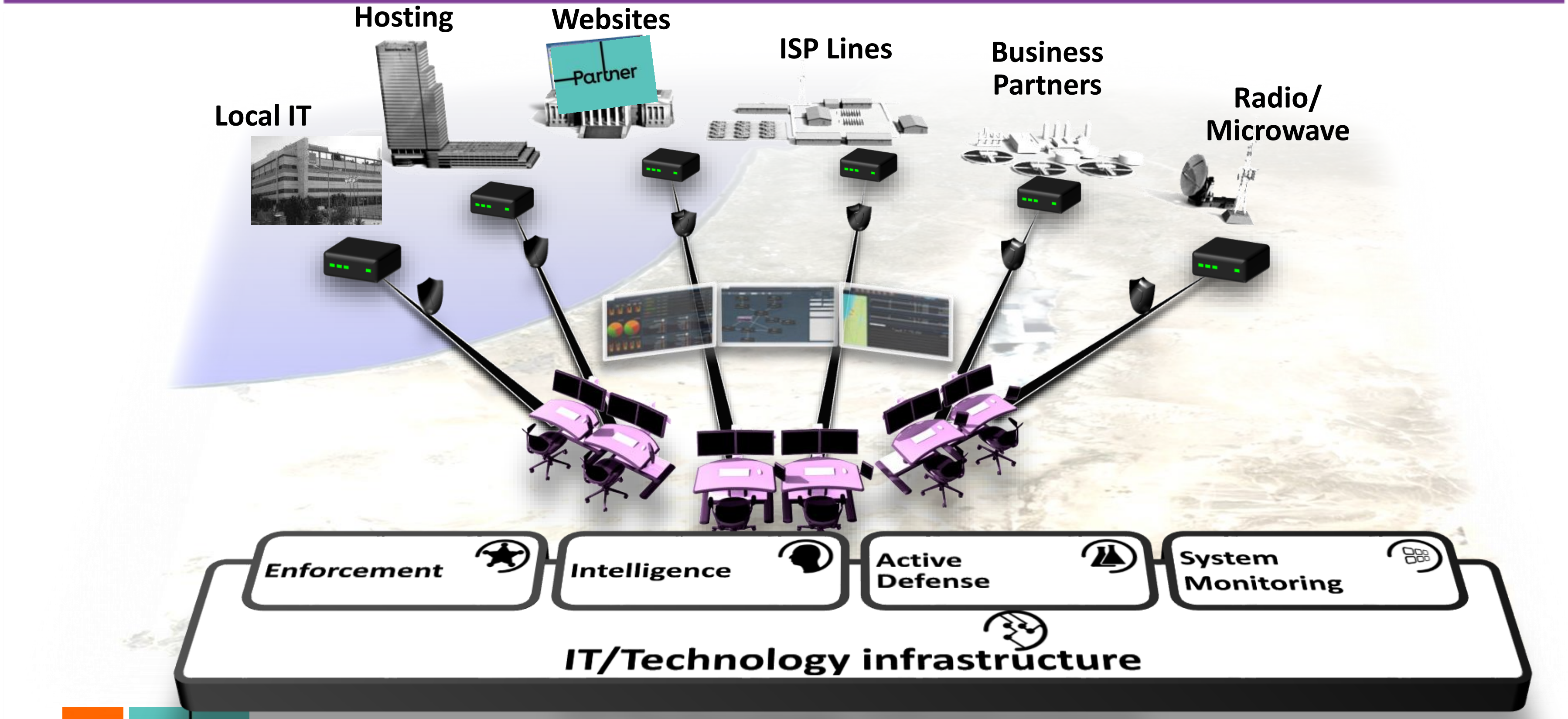
Monthly Cyber Attack Newsletter

On-Premise vs Hybrid vs Cloud

To Cloud or Not to Cloud?

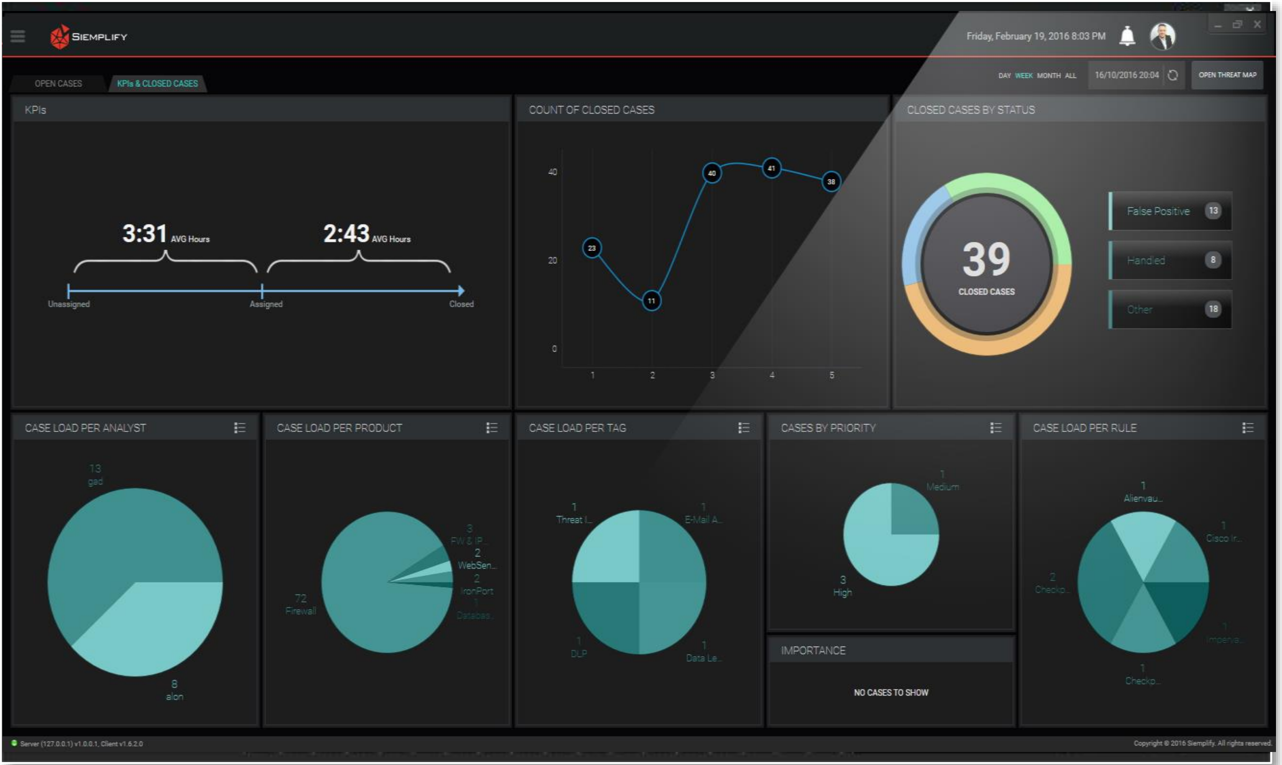
- Why ?
- Where & how will my data be stored & encrypted?
- Who has access to my data?
- What regulation & security standards support is there?
- Where is authentication done?
- What happens with DLP issues & AV/ZD/APT support?

Partner Cyber SOC



Cyber Security Operations Center

- Threat
  - ISP s
  - Hos
  - IT
  - Frau
- Suspici
- Threat
- IR man
- Visual



Cyber "Guidelines" for 2016-2017

Threat Intelligence for the Masses

Secure / Private Cloud Solutions

IoT– Secure / Monitor / Network Capacity / etc.

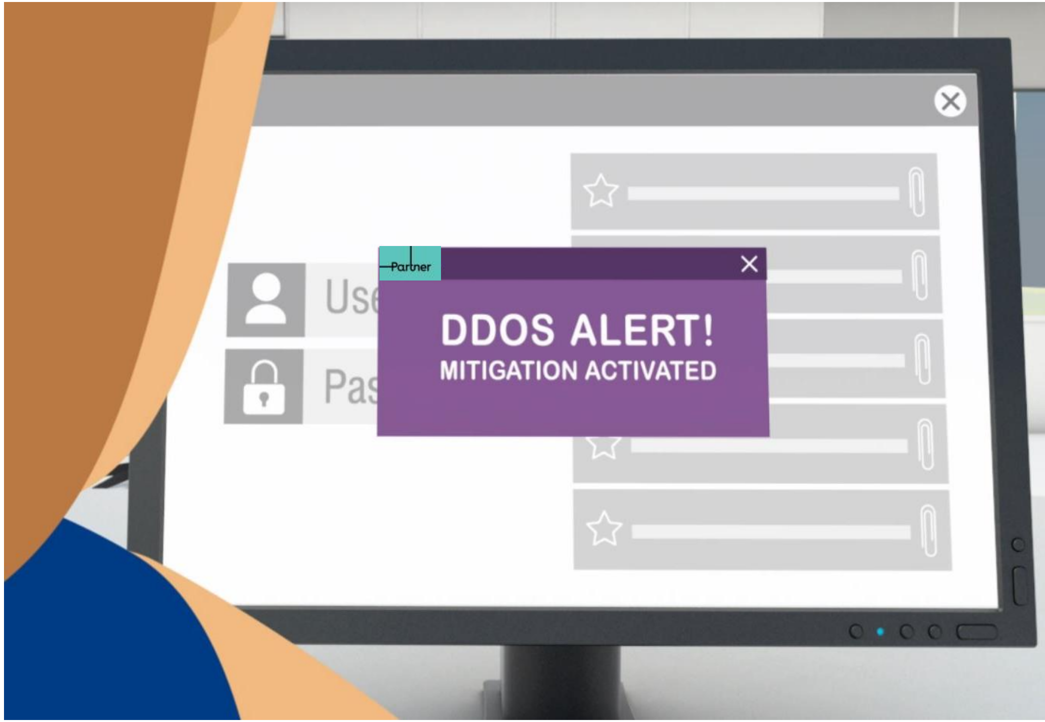
Cyber Drills inside out

Supply Chain Monitoring & Mitigation

Employee Awareness, Awareness, Awareness

Apply What You Have Learned Today

- Next week you should:
  - Have an employee cyber risks training
- In the first three months following this presentation you should:
  - Build a “game plan” for a ZD\APT defense program considering:
    - Network Monitoring
    - EndPoint blocking
    - Traps to SD
    - SIEM logs & correlations
    - External threat analysis service
  - Database controls
- Within six months you should:
  - Cyber incident response program
  - “Table TOP” drill

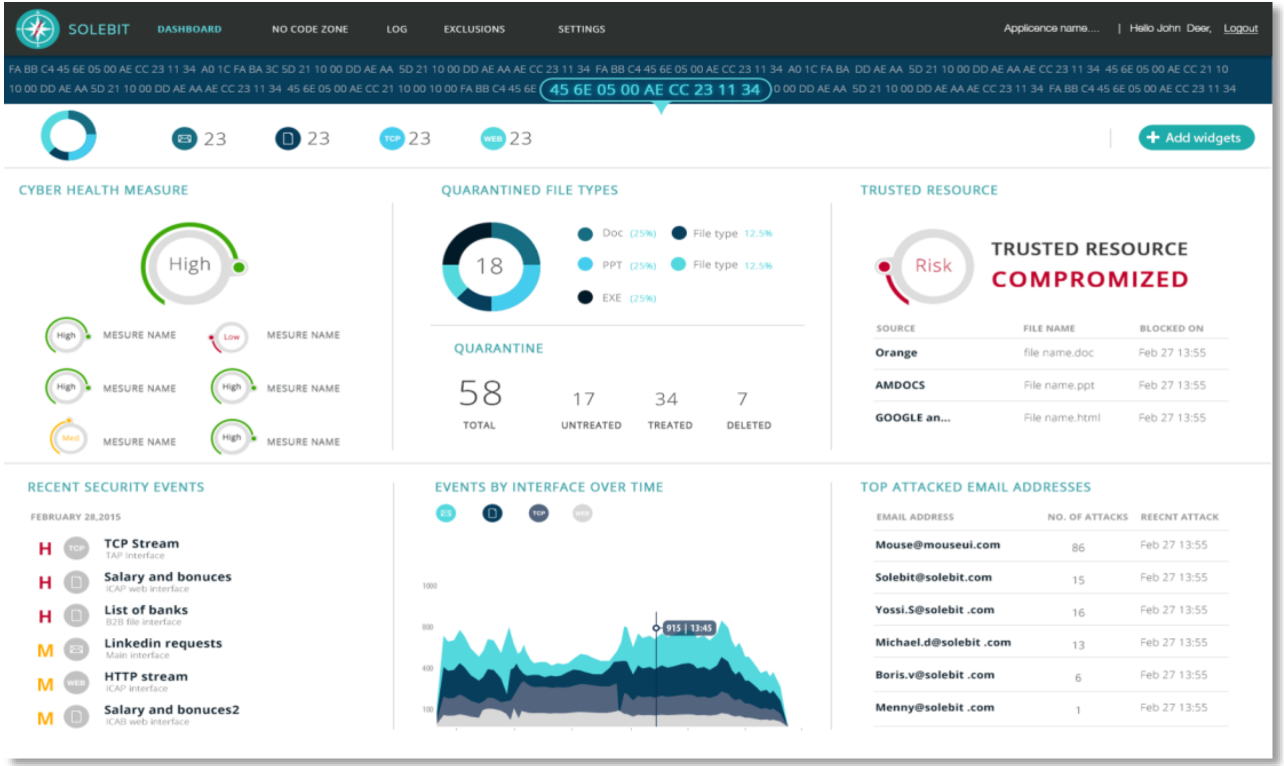


RSAConference2016

THANK YOU!

ANY QUESTIONS? NOW’S THE TIME…

SoleBit



```
FA BB C4 45 6E 05 00 AE CC 23 11 34  A0 1C FA BA 3C 5D 21 10 00 DD AE AA  5D 21 10 00 DD AE AA AE CC 23 11 34  FA BB C4 45 6E 05 00 AE CC 23 11 34  A0 1C FA BA  DD AE AA  5D 21 10 00 DD AE AA AE CC 23 11 34  45 6E 05 00 AE CC 21 10
10 00 DD AE AA 5D 21 10 00 DD AE AA AE CC 23 11 34  45 6E 05 00 AE CC 21 10 00 10 00 FA BB C4 45 6E  45 6E 05 00 AE CC 23 11 34  0 00 DD AE AA  5D 21 10 00 DD AE AA AE CC 23 11 34  FA BB C4 45 6E 05 00 AE CC 23 11 34
```

CYBER HEALTH MEASURE

High

High MESURE NAME

Low MESURE NAME

High MESURE NAME

High MESURE NAME

Med MESURE NAME

High MESURE NAME

QUARANTINED FILE TYPES

QUARANTINE

58	17	34	7
TOTAL	UNTREATED	TREATED	DELETED

TRUSTED RESOURCE

Risk

TRUSTED RESOURCE
COMPROMIZED

SOURCE	FILE NAME	BLOCKED ON
Orange	file name.doc	Feb 27 13:55
AMDOCS	File name.ppt	Feb 27 13:55
GOOGLE an...	File name.html	Feb 27 13:55

RECENT SECURITY EVENTS

FEBRUARY 28,2015

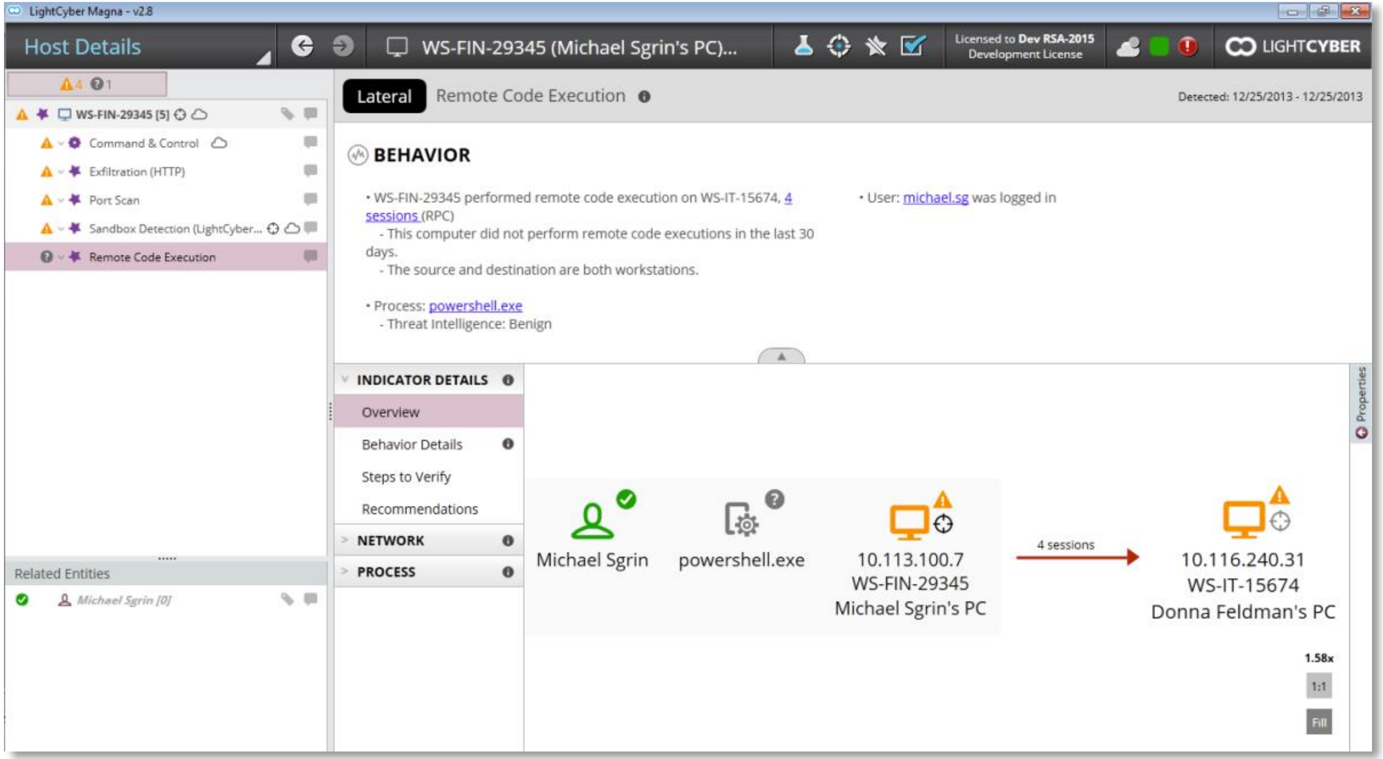
H	TCP	**TCP Stream** TAP Interface
H		**Salary and bonuces** ICAP web interface
H		**List of banks** B2B file interface
M		**Linkedin requests** Main interface
M	WEB	**HTTP stream** ICAP interface
M		**Salary and bonuces2** ICAB web interface

EVENTS BY INTERFACE OVER TIME

TOP ATTACKED EMAIL ADDRESSES

EMAIL ADDRESS	NO. OF ATTACKS	REECNT ATTACK
Mouse@mouseui.com	86	Feb 27 13:55
Solebit@solebit.com	15	Feb 27 13:55
Yossi.S@solebit .com	16	Feb 27 13:55
Michael.d@solebit .com	13	Feb 27 13:55
Boris.v@solebit .com	6	Feb 27 13:55
Menny@solebit .com	1	Feb 27 13:55

LightCyber



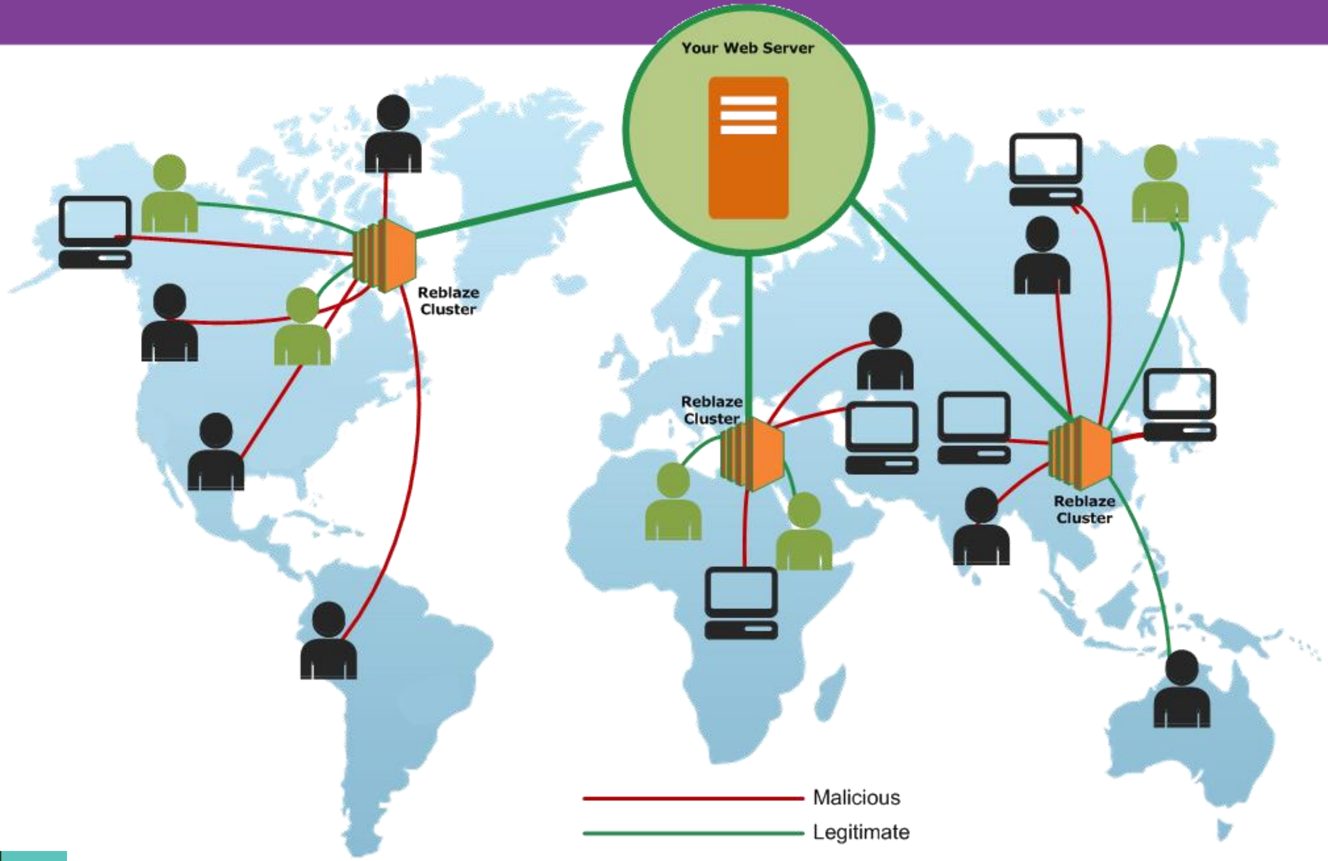
Lateral Remote Code Execution

Detected: 12/25/2013 - 12/25/2013

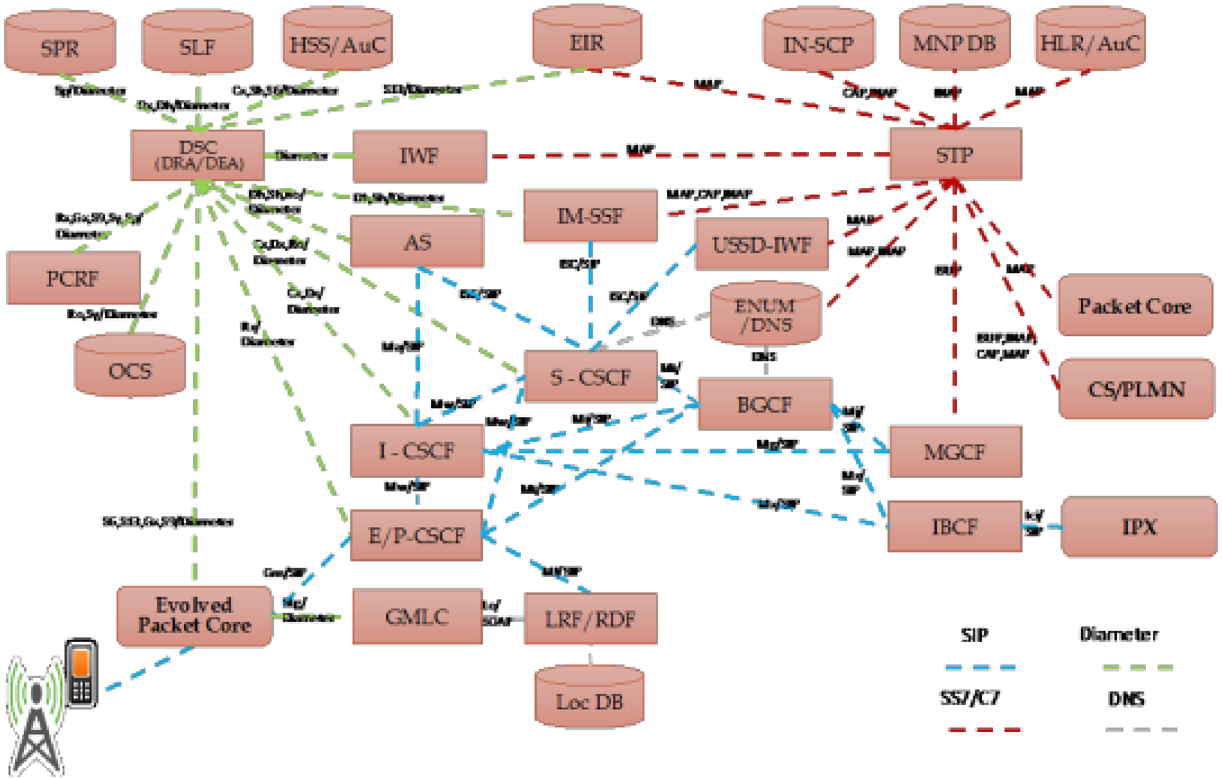
BEHAVIOR

- WS-FIN-29345 performed remote code execution on WS-IT-15674, 4 sessions (RPC)
  - This computer did not perform remote code executions in the last 30 days.
  - The source and destination are both workstations.
- Process: powershell.exe
  - Threat Intelligence: Benign
- User: michael.sg was logged in

ReBlaze WAF, DDOS, BOT…



VoLTE at Glance ☺


SPR
SLF
HSS/ AuC
EIR
IN-SCP
MNP DB
HLR/ AuC
Sp/Diameter
Cx,Dh/Diameter
Cx,Sh,S6/Diameter
S13/Diameter
MAP
CAP,INAP
INAP
MAP
DSC
(DRA/DEA)
Diameter
IWF
MAP
STP
Dh,Sh,Ro/
Diameter
Dh,Sh/Diameter
IM-SSF
MAP,CAP,INAP
Rx,Gx,S9,Sy,Sd/
Diameter
AS
USSD-IWF
MAP
MAP,INAP
PCRF
Cx,Dx,Rx/
Diameter
ISC/SIP
ISC/SIP
ISC/SIP
ISUP
MAP
Packet Core
Ro,Sy/Diameter
Cx,Dx/
Diameter
ENUM
/DNS
DNS
Rx/
Diameter
OCS
Mw/SIP
DNS
ISUP,BSSAP,
CAP,MAP
S - CSCF
Mi/
SIP
BGCF
CS/PLMN
Mw/SIP
Mw/SIP
Mg/SIP
Mj/
SIP
I - CSCF
Mg/SIP
MGCF
Mw/SIP
Mx/SIP
Mx/
SIP
S6,S13,Gx,S9/Diameter
E/P-CSCF
Mx/SIP
IBCF
Ici/
SIP
IPX
Gm/SIP
Ml/SIP
Evolved
Packet Core
SLg/
Diameter
GMLC
Le/
SOAP
LRF/ RDF
Loc DB
SIP
Diameter
SS7/C7
DNS