SpySpot
Seeing is believing

NWO
Netherlands Organisation for Scientific Research

Bram C.M. Cappers
b.c.m.cappers@tue.nl

Jarke J. van Wijk
j.j.v.wijk@tue.nl

SEMANTIC NETWORK TRAFFIC ANALYSIS USING DEEP PACKET INSPECTION AND VISUAL ANALYTICS

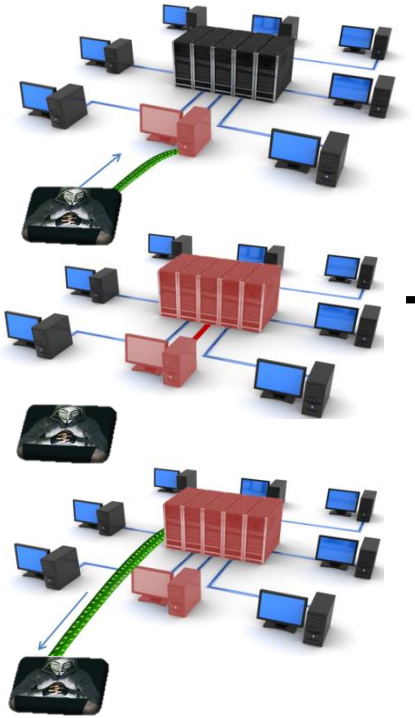
More Info: www.bramcappers.nl

Advanced Persistent Threats (APTs)

Infiltration

Expansion

Sabotage

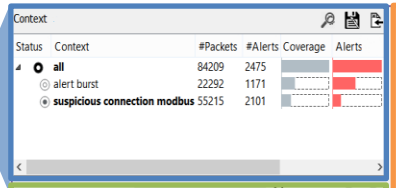


Wireshark
Protocol
Analyzer

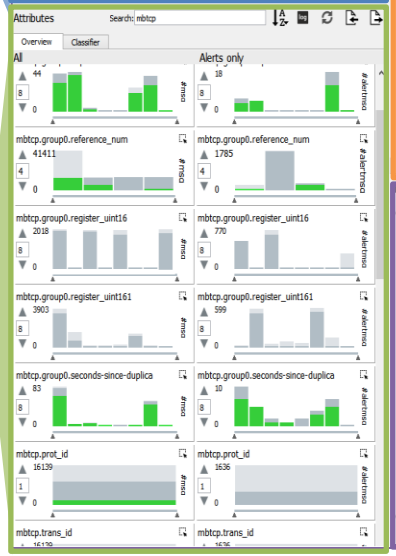
ip.version	ip.src	ip.dst	tcp.srcport	tcp.flag	tcp.flag.SYN	tcp.flag.ACK	smb.header	smb.cmd	smb.type	smb.file	smb.bytecount	dcerpc.call_id	dcerpc.opnum
4	192.168.0.1	192.168.0.2	80	2	true	false	smb	5	readFile	a.txt			
⋮													
4	192.168.0.3	192.168.0.2	91	1	false	true	smb	3	IOControl		20	0	3

Overview

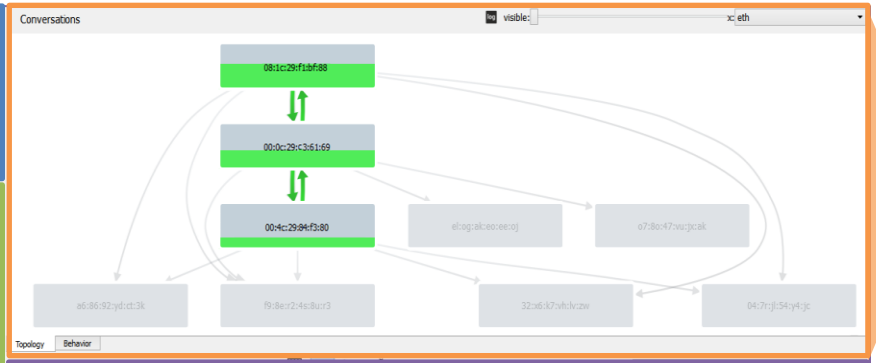
Filtering



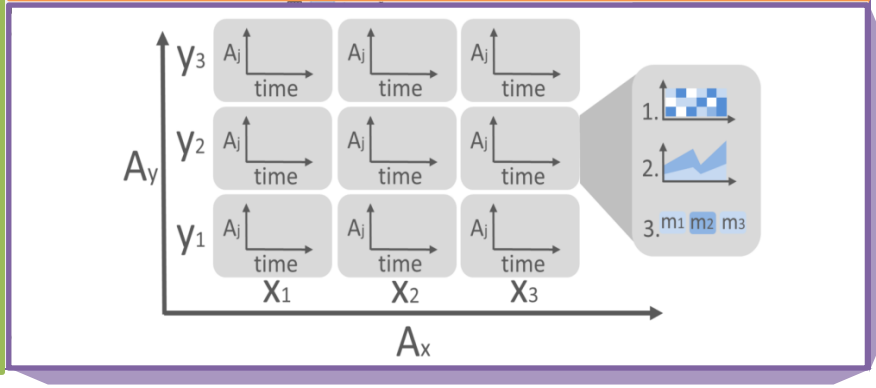
Attributes

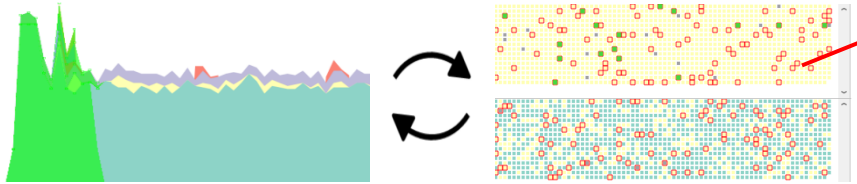


Conversations

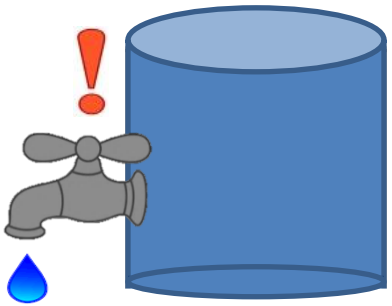


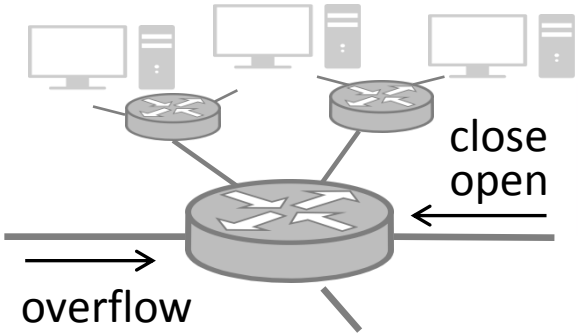
Messages + Alerts



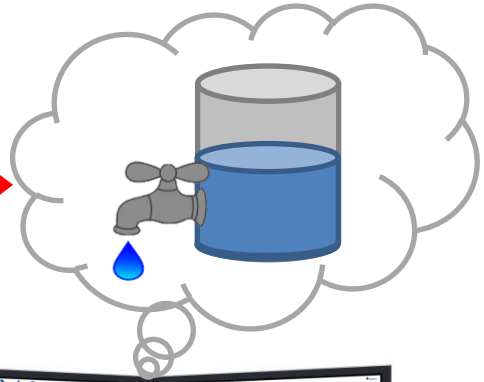


Results




close
open
overflow


Context
Conversations
Attributes
Time Table



Netherlands Organisation for Scientific Research

Bram C.M. Cappers
b.c.m.cappers@tue.nl

Jarke J. van Wijk
j.j.v.wijk@tue.nl

THANKS FOR YOUR ATTENTION!

SpySpot
Seeing is believing

More Info: www.bramcappers.nl