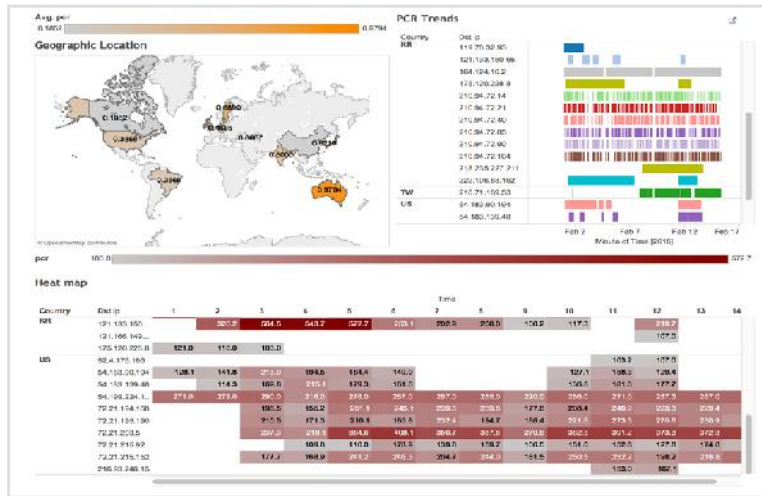


# ConnecTome - Tracks Every Persistent traffic in Network

## Detects Hidden Adversaries via Cyber-Kill-Chain Analysis



HOST	구분	1단계 (비무부차원 침해)	2단계 (명령어 치환)	3단계 (공격도구 전송)	4단계 (비무부 이동)	5단계 (정보유출)	위험도
10.122.103.234	Trigger	0	4	10	0	9	89%
	Trace	0	0	0	14	8	
10.122.103.107	Trigger	0	4	7	1	1	85%
	Trace	0	0	0	9	3	
10.122.104.99	Trigger	0	3	4	1	1	85%
	Trace	0	0	0	1	11	
10.122.103.203	Trigger	0	2	6	1	1	78%
	Trace	0	0	0	2	13	
10.122.103.132	Trigger	0	10	1	1	1	67%
	Trace	0	2	0	11	1	

### Transforms Incident Response Procedures

Through Big Data Analysis, it Recognizes hidden adversaries and provide information of how deep they have infiltrated into your network.

### C2 Identification

Tracks every persistent traffic in your network and categorize them in terms of its characteristics. It does also counts the number of clients bound to the specific C2 destination.

### Cyber-Kill-Chain Analysis

Tracks multi-staged movements of 'adversaries' in your network from beachhead, establishing command and control, lateral movement and data exfiltration.



## Key Features

### Situation Awareness

Dynamically Create The View of Your Network From the Nr. of Network Sessions and Hosts, Operating Systems and Activate Network Services and more.

### Threat Recognition

Identifies Threats in Your Networks From Policy Violation, Covert Channels, and Command and Control Channels, Internal Scans, and many more Suspicious Activities of you Internal Hosts.

### Incident Detection

Cyber-Kill-Chain Based Incident Tracking Capability Detects Adversaries' Movements in Your Network From Initial Compromise, Command and Control Channel, Reinforcement and Lateral Movement.

[www.narusec.com](http://www.narusec.com)

**Naru Security, Inc.**

+82-2-522-7912  
 9F, 621 Building, 621  
 YoungDong DaeRo, GangNam-Gu,  
 Seoul 06087 South Korea

# “INSIDE OUT” Security Intelligence by Situation Awareness



## INSEDE OUT Security Intelligence provides you inside-out knowledge about your Network.

Deployed with “INSIDE OUT” Security Intelligence, customers can easily become aware of its security posture via number of security metrics that measure and track complete persistent traffics, backdoors along with its geolocation information, number of internal connectivity, and the progressive ratio of amount of data exchanged between inside and outside of the network through PC and portable mobile devices. “INSIDE OUT” Security Intelligence updates AS number, domain-IP tuple, L4/L7 protocol, type and category of the destination regularly to provide accurate information.