Incident Information Exchange in Darknet Monitoring System

draft-suzuki-mile-darknet-00

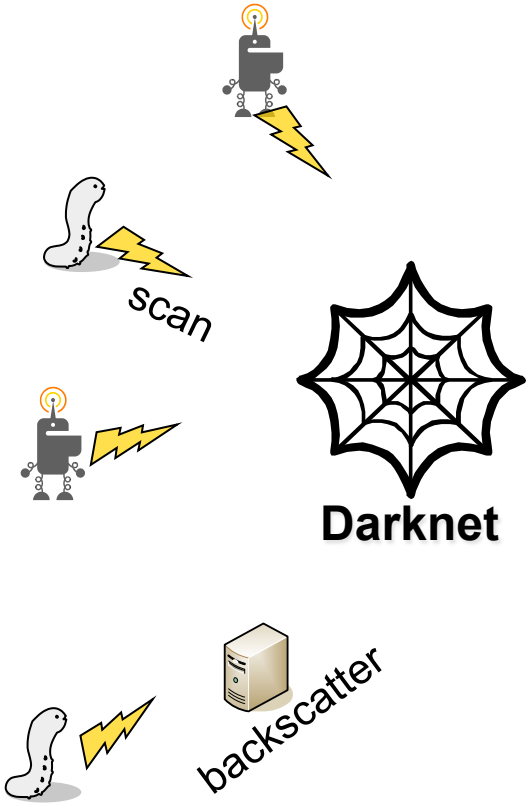
Mio Suzuki
Cybersecurity Laboratory
Network Security Research Institute
National Institute of Information and Communications Technology, Japan

Overview

- This draft (draft-suzuki-mile-darknet-00) shows current alert schema of our darknet monitoring system called DAEDALUS
- Background of current schema
  - What's darknet?
  - Overview of our operating nicter and DAEDALUS system
  - Use cases of DAEDALUS
- Current schema
  - Schema expression
  - An example
- Discussion

What is Darknet?

- **Darknet**: Unused IP addresses space
- **In theory**: any packets should **NOT** arrive at the darknet because they are not connected to any hosts.
- **In fact**: quite a few packets **DO** arrive!
- Packets arriving at the darknet are…
  - Scans by malwares
  - Backscatter (reflection of DDoS attack)
  - Miss configurations etc.
- Darknet traffic reflects **global trend in malicious activities** on the Internet.
- Darknet is also monitored on…
  - CAIDA
  - Team Cymru
  - University of Michigan etc.



Overview of our project NICTER

nicter = **N**etwork **I**ncident analysis **C**enter for **T**actical **E**mergency **R**esponse

Target:

Comprehensive analysis of security threats on the Internet

- What happens on the Internet?
- What is the root cause?

Strategy:

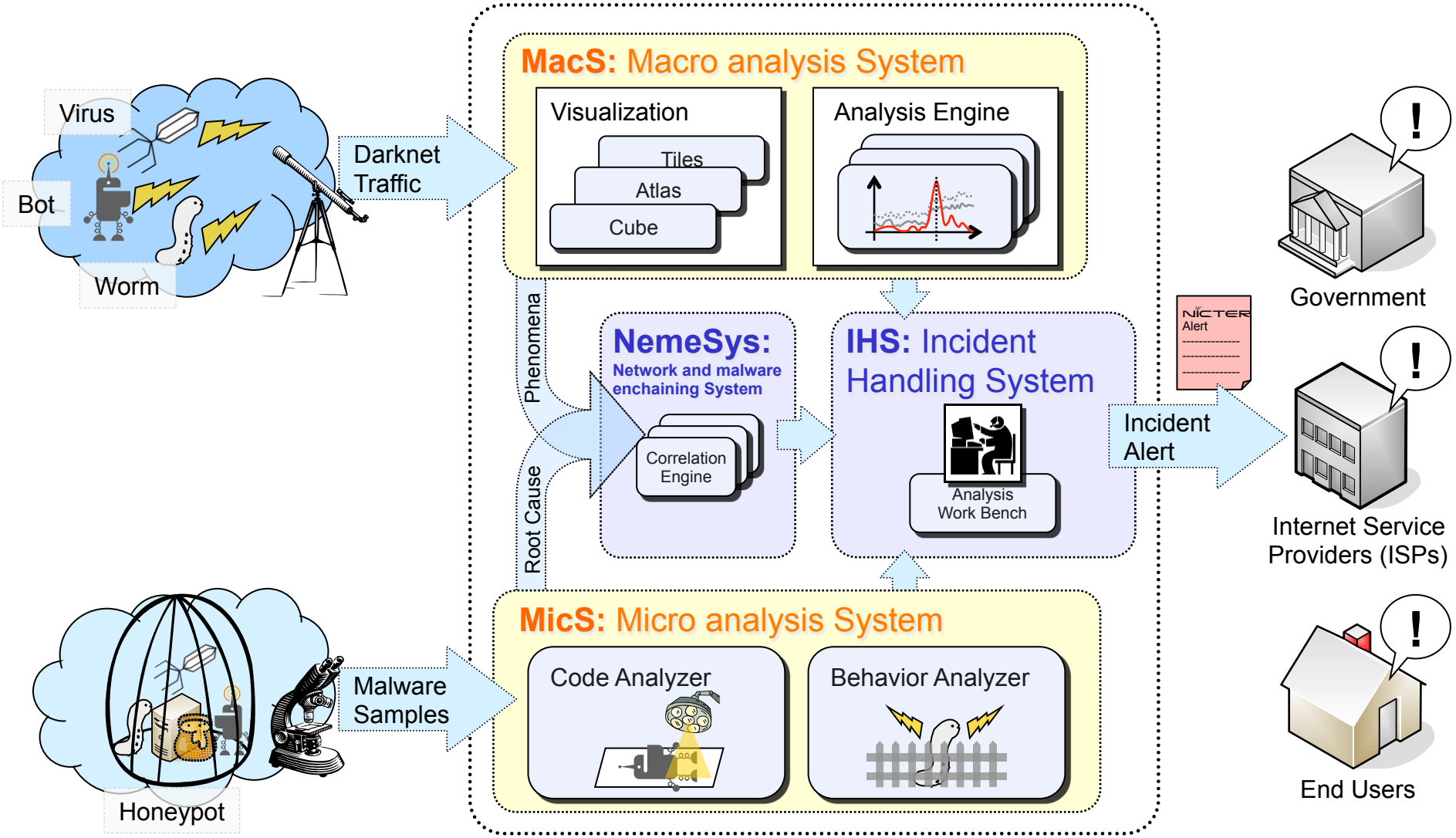
Network monitoring

+

Malware analysis

nicter Operation Room

NICTER System Overview



Goal and Mechanism of DAEDALUS

(**D**irect **A**lert **E**nvironment for **D**arknet **A**nd **L**ivenet **U**nified **S**ecurity)

Goal:

Utilize the darknet monitoring results

for securing the livenet.

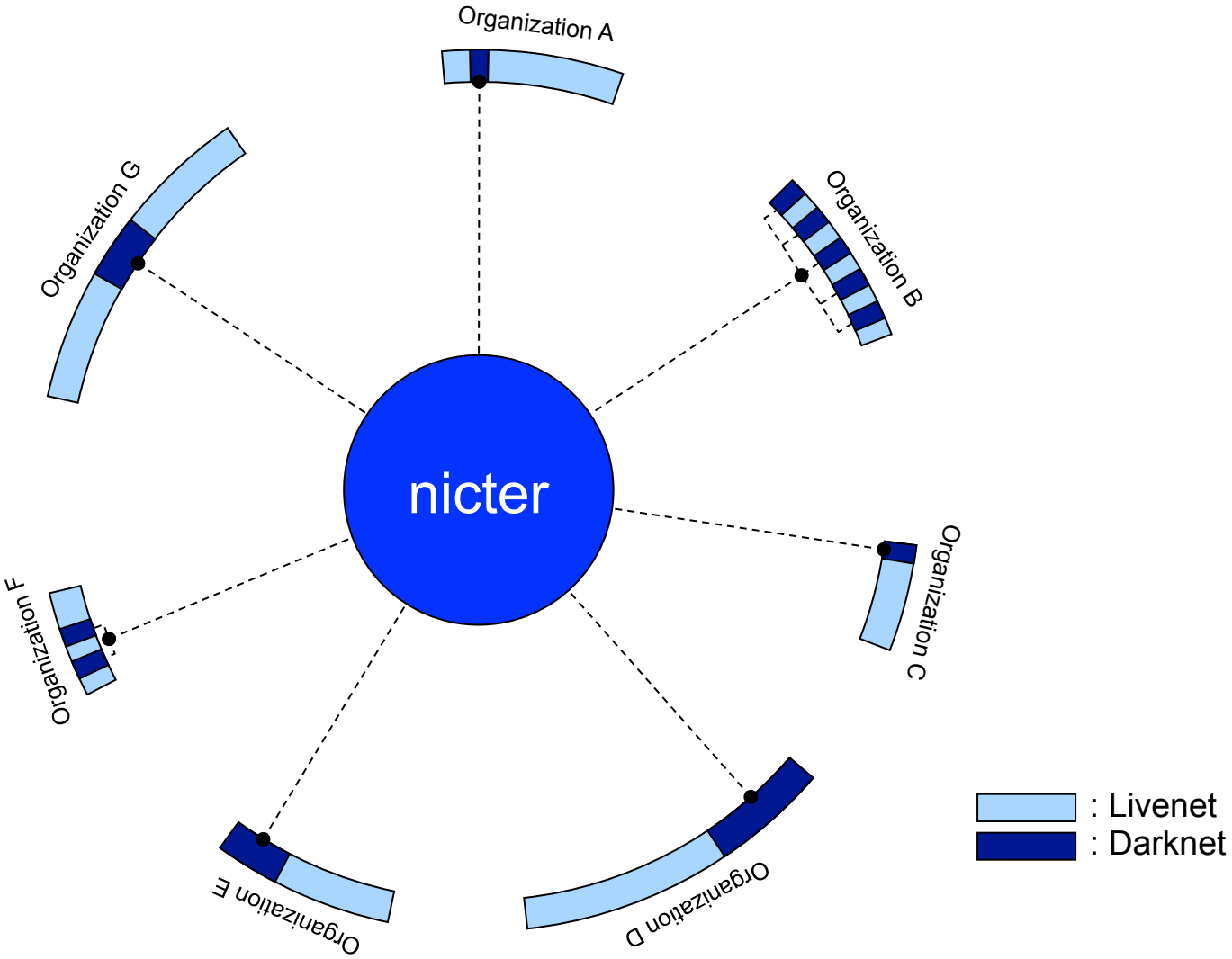
Mechanism:

if (nicter receives packets

from a cooperative organization)

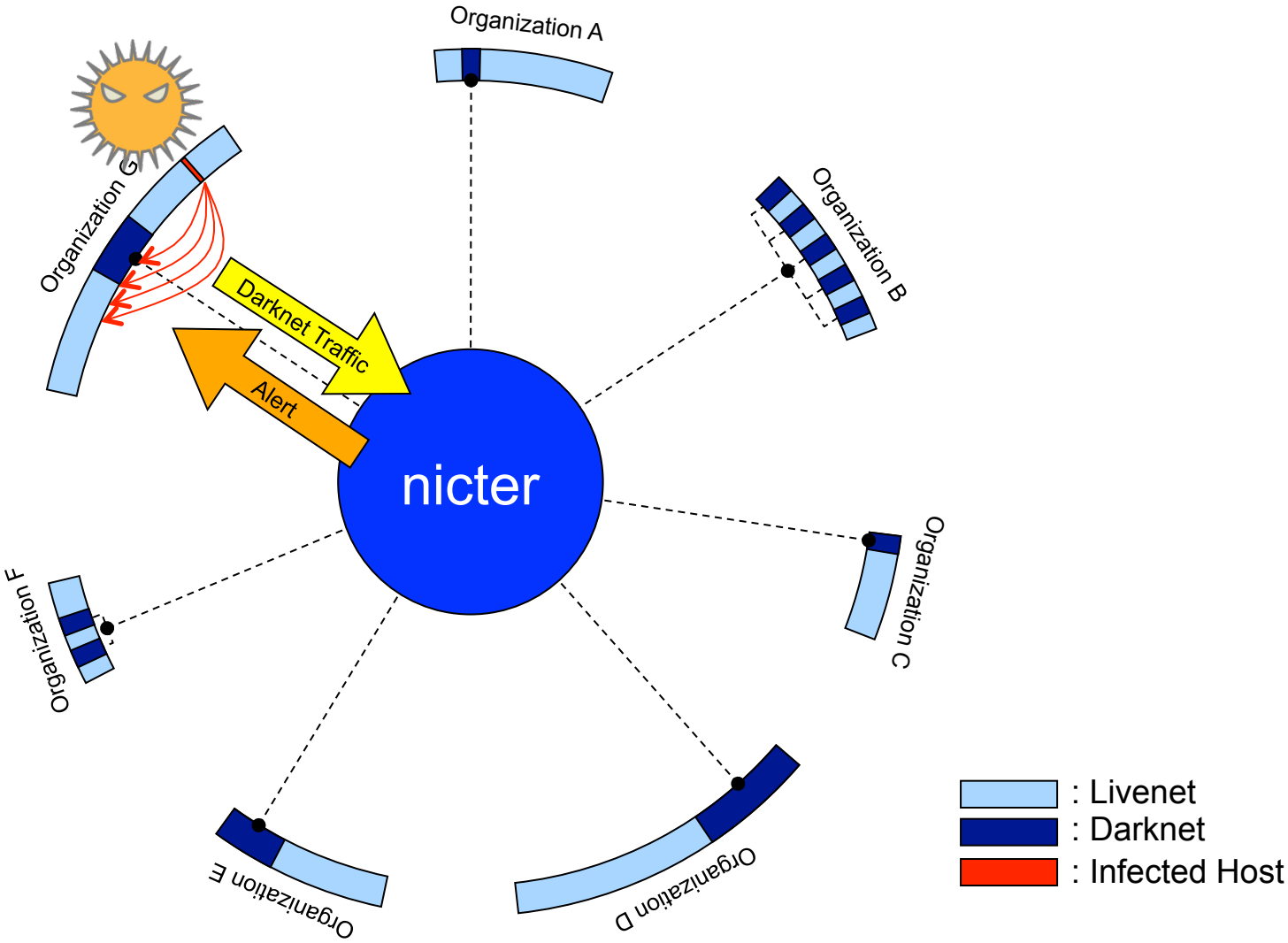
alert;

System Overview



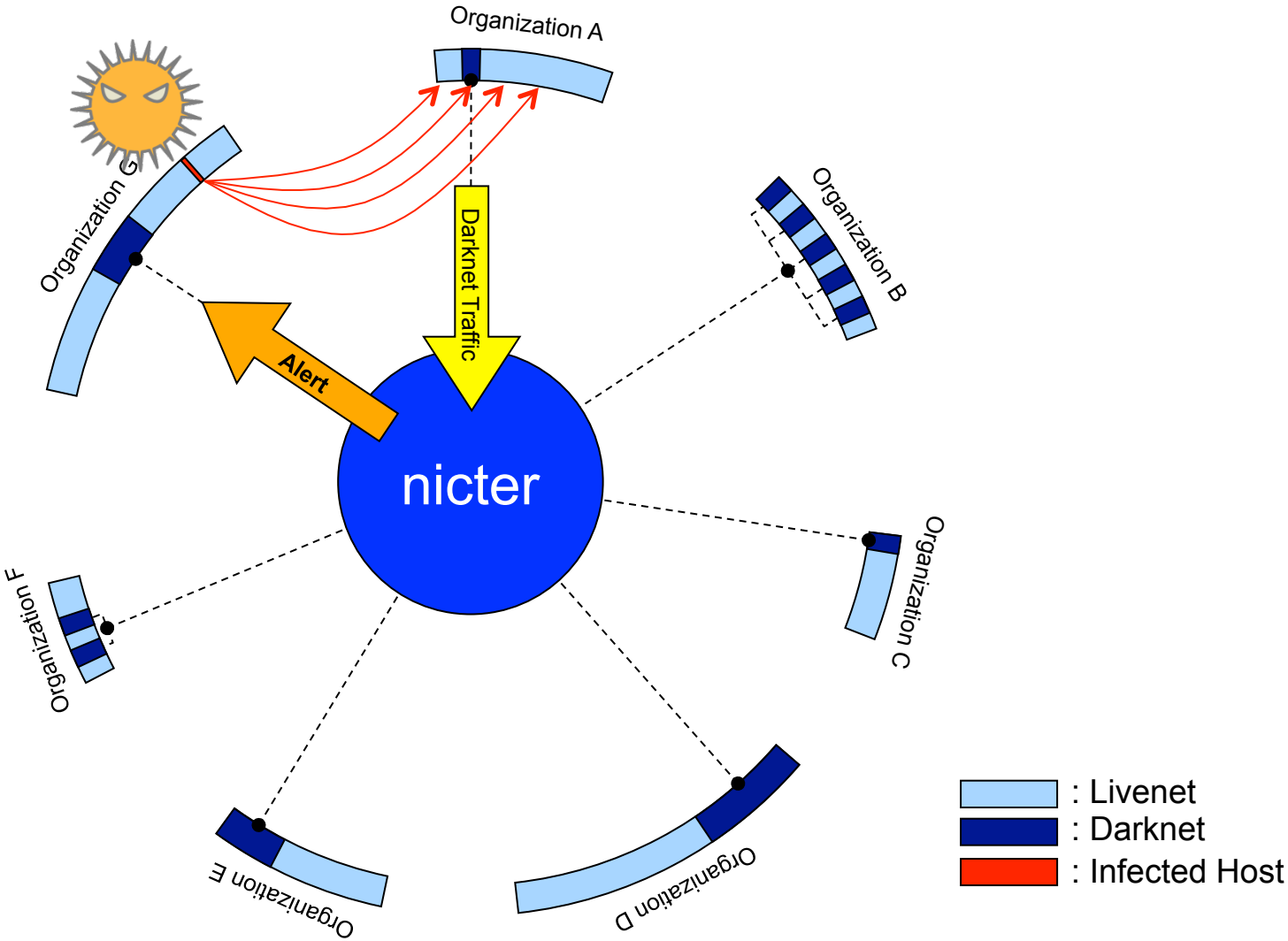
Use Case 1

Internal Darknet Alert (Local Scan)



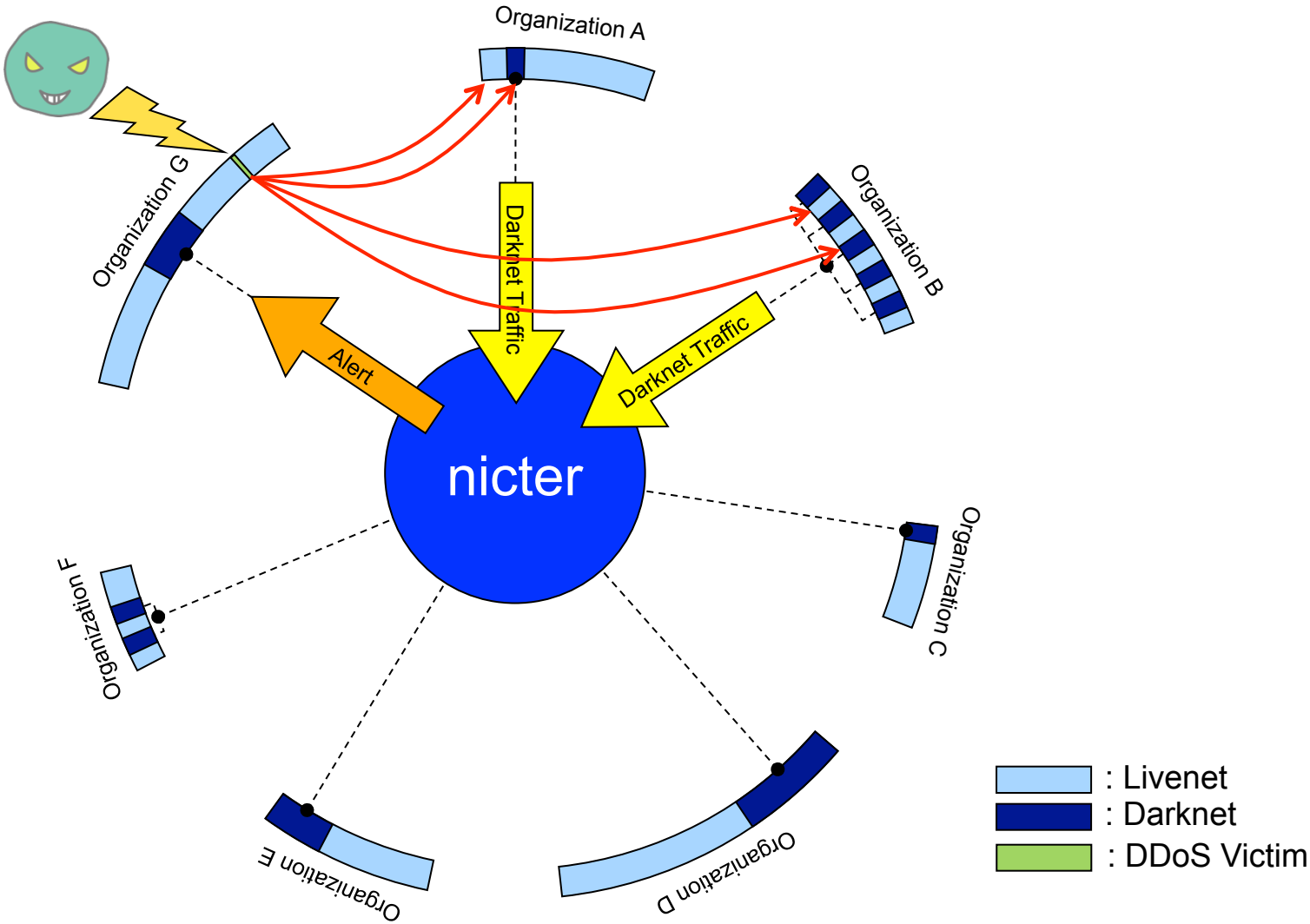
Use Case 2

External Darknet Alert (Global Scan)



Use Case 3

External Darknet Alert (Backscatter)

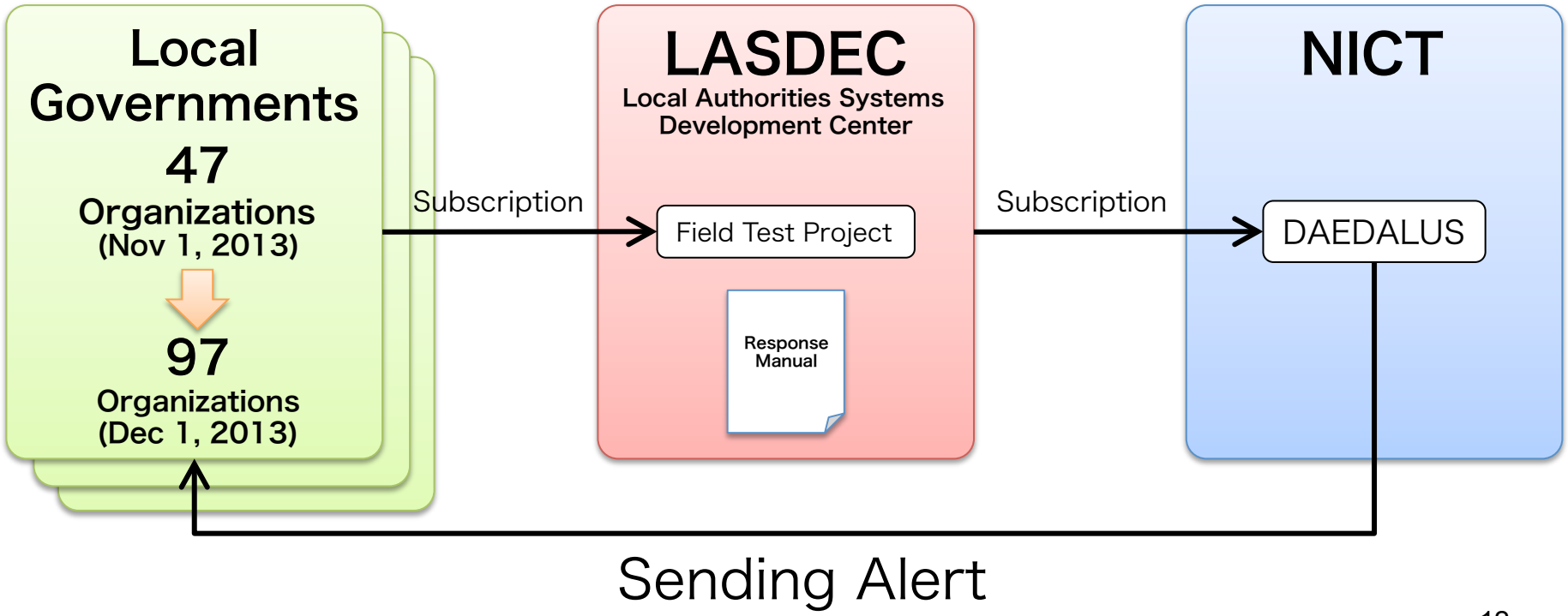


DAEDALUS-VIZ
https://www.youtube.com/results?search_query=DAEDALUS+NICT

DAEDALUS for LG

DAEDALUS has started to provide the alert service to local governments in Japan.

- ✓ From Nov. 1, 2013.
- ✓ Start with 47 local governments.



Current Schema of DAEDALUS Alert

- <NicterEvent> and <Header> element
  - Common header of our whole project
- <DaedalusAlertHeader> element
  - Contains alert identifier, organization identifier, trigger of alert , and monitored duration
- <AlertData> element
  - Per source IP address
  - Contains time, identifier, source IP address, source country code, number of related packets, and frequency information
  - Subsequent <Packet> element contains actual packet information
- <Packet> element
  - Per packet basis
  - Not session basis because darknet doesn't respond incoming packets
  - Contains protocol number, 5-tuple information in case of TCP or UDP, TCP flag and ICMP type if possible, observed time
  - Also contains where the packet come from
    - From the network of a monitored organization (internal)
    - From outside of the network of the organization (external)

An Example of Alert


```
<!-- SNIP -->
 <DaedalusAlertHeader>
   <AlertID>277761</AlertID>
   <OrgID>2</OrgID>
   <Trigger>Periodic</Trigger>
   <Duration>3600</Duration>
  </DaedalusAlertHeader>
  <AlertData EventTime="2011-12-19 11:00:39" EventID="1096117" SrcIP="xxx.yyy.236.116" SrcCC="JP"
TotalPacketCount="878" DisplayedPacketCount="878" Type="Continued">
   <Packet PacketTime="2011-12-19 10:01:21" DstIP="xxx.yyy.241.101" DstCC="JP” DstPort=""
SrcPort="" Protocol="1" Flag="8" DarknetType="internal"/>
   <Packet PacketTime="2011-12-19 10:01:31" DstIP="xxx.yyy.241.101" DstCC="JP” DstPort=""
SrcPort="" Protocol="1" Flag="8" DarknetType="internal"/>
   <Packet PacketTime="2011-12-19 10:01:33" DstIP="xxx.yyy.241.101" DstCC="JP” DstPort=""
SrcPort="" Protocol="1" Flag="8" DarknetType="internal"/>
   <Packet PacketTime="2011-12-19 10:01:35" DstIP="xxx.yyy.241.101" DstCC="JP” DstPort="445"
SrcPort="3580" Protocol="6" Flag="2" DarknetType="internal"/>
   <Packet PacketTime="2011-12-19 10:01:38" DstIP="xxx.yyy.241.101" DstCC="JP” DstPort="445"
SrcPort="3580" Protocol="6" Flag="2" DarknetType="internal"/>
<!-- SNIP -->
```

Discussion

- Give me honest feedbacks.
- Based on the discussion, we would like to consider further development of our schema; compatibility with IODEF, or extension to IODEF, or just using IODEF, could be considered.

Mio Suzuki
Contact: mio@nict.go.jp