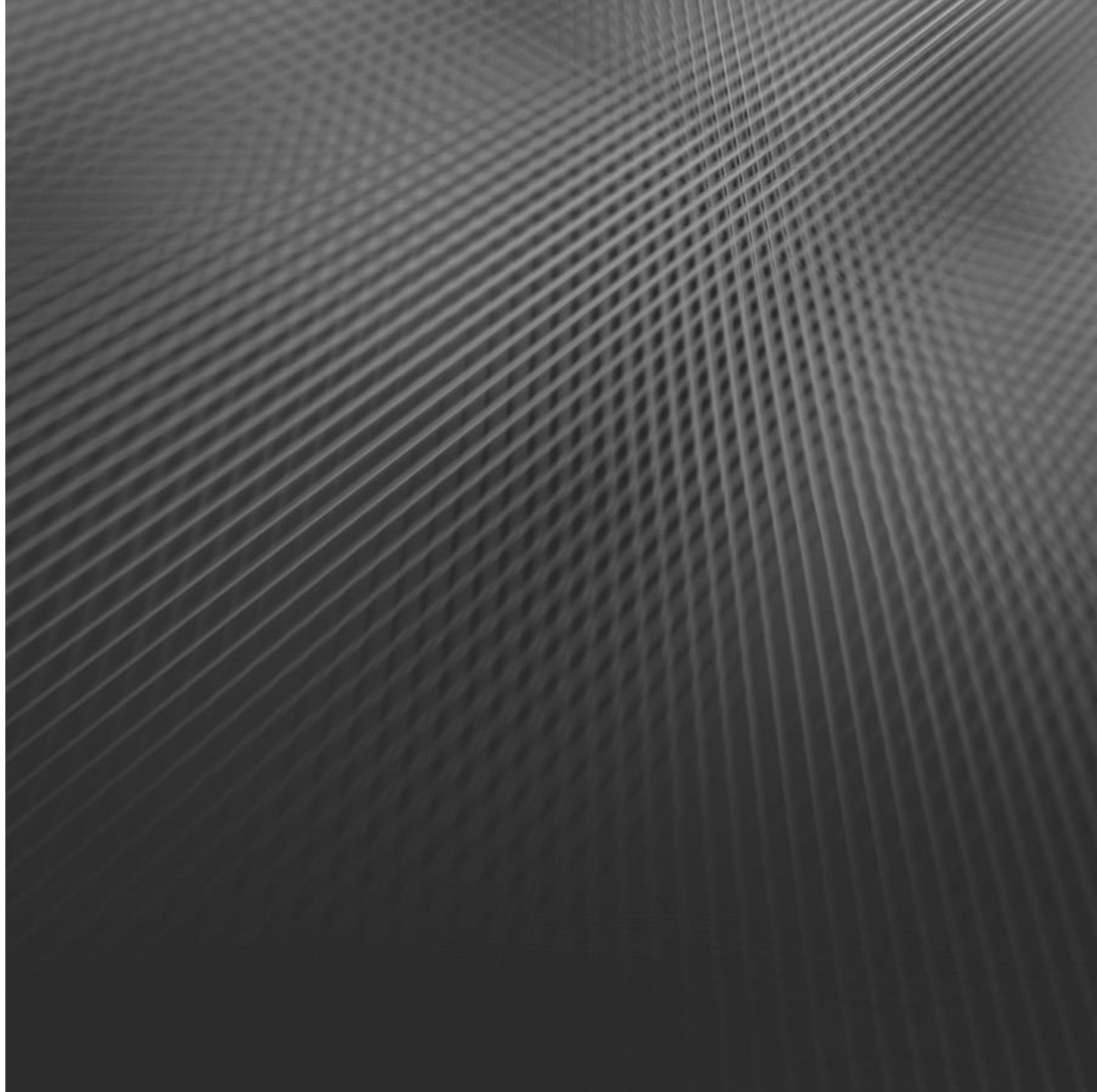
Pacific Northwest
NATIONAL LABORATORY

FLOWER – Network FLOW analyzER

DARREN CURTIS

PNNL April 17, 2020



U.S. DEPARTMENT OF ENERGY BATTELLE

PNNL is operated by Battelle for the U.S. Department of Energy

Pacific Northwest
NATIONAL LABORATORY

Deep network packet header inspection across an enterprise

Pacific Northwest NATIONAL LABORATORY

What is FLOWER?

SOFTWARE – TRL9

- **Linux based Application (CentOS 7+ / RHEL 7+ / Ubuntu 16.04)***
- **Captures real-time IPv4 and IPv6 data**
  - Cannot be Detected on Network (listen only)
  - Data records are bidirectional versus unidirectional network flows
  - Data is parsed using **RFC** specifications
  - Data logged in a well-defined structured **CSV** format
  - Deep **packet header** inspection
  - Detect **anomalies** (e.g., malformed/corrupt headers)
  - Reveal tunneled communications (GRE, IPv6 over IPv4, Teredo, etc.)
  - Read pre-recorded PCAP data files

*Limited availability on Windows/macOS X

Where is FLOWER?

Deployments

- **In production for 10+ years**
  - ~100 US DOE facilities in 2008
  - ~75% of bulk electricity transmission grid
  - Used at PNNL on 40G enterprise backbone
    - ✓ Living Lab
  - Independently tested by AIS* on 100G network
  - Licensed to Z-SofTech Solutions, LLC.
  - 1 prototype to collect wireless data
  - 1 collaboration with edge computing

*Assured Information Security

Pacific Northwest NATIONAL LABORATORY

What FLOWER is NOT

- Comprehensive data analytic and visualization tool
- Zeek (Bro) – Deep packet inspection
- GrassMarlin – Exploratory tool (limited)
- PacketBeats – Data Lake
- Can’t run on AWS or Azure without Packet Forwarding or PCAP files
  - no physical tap in the cloud

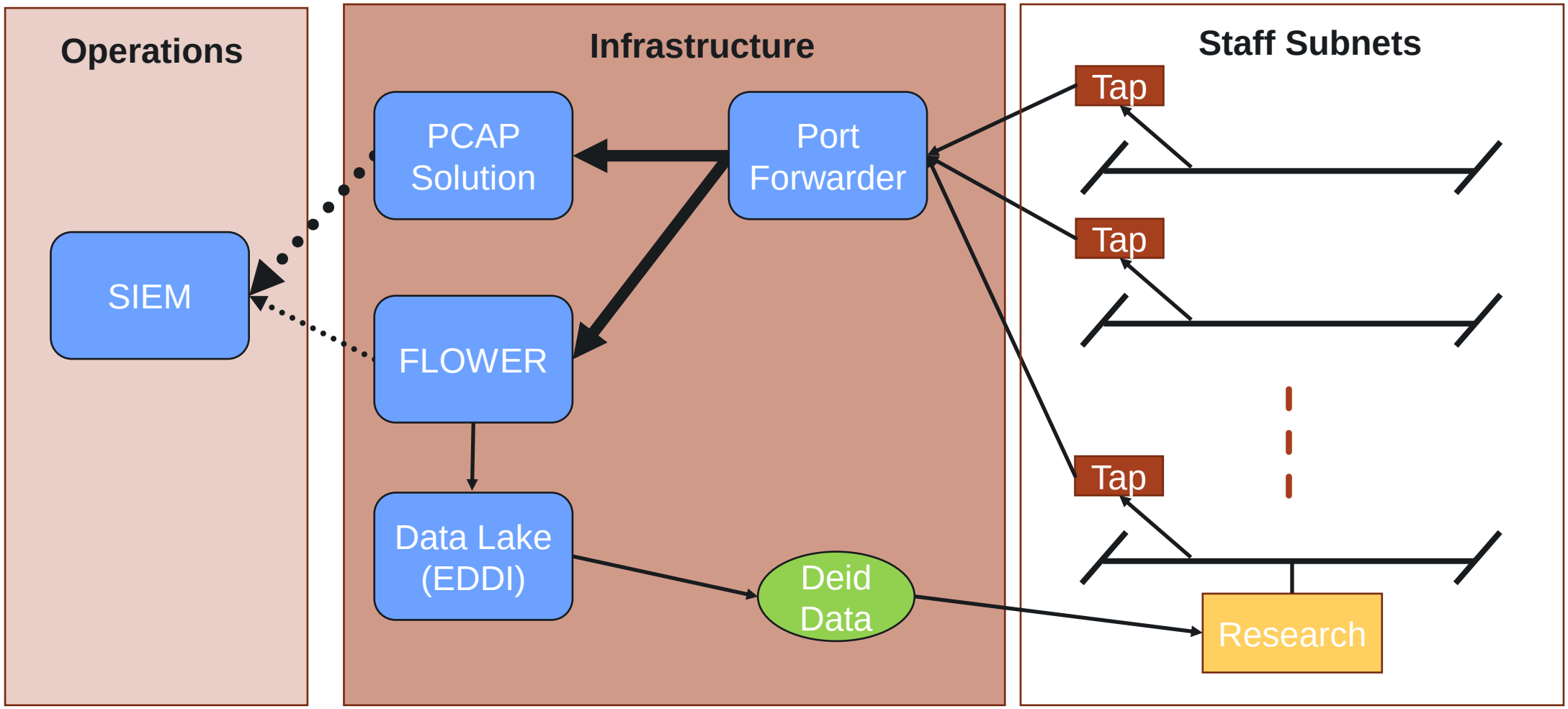
Pacific Northwest NATIONAL LABORATORY

Why use FLOWER?

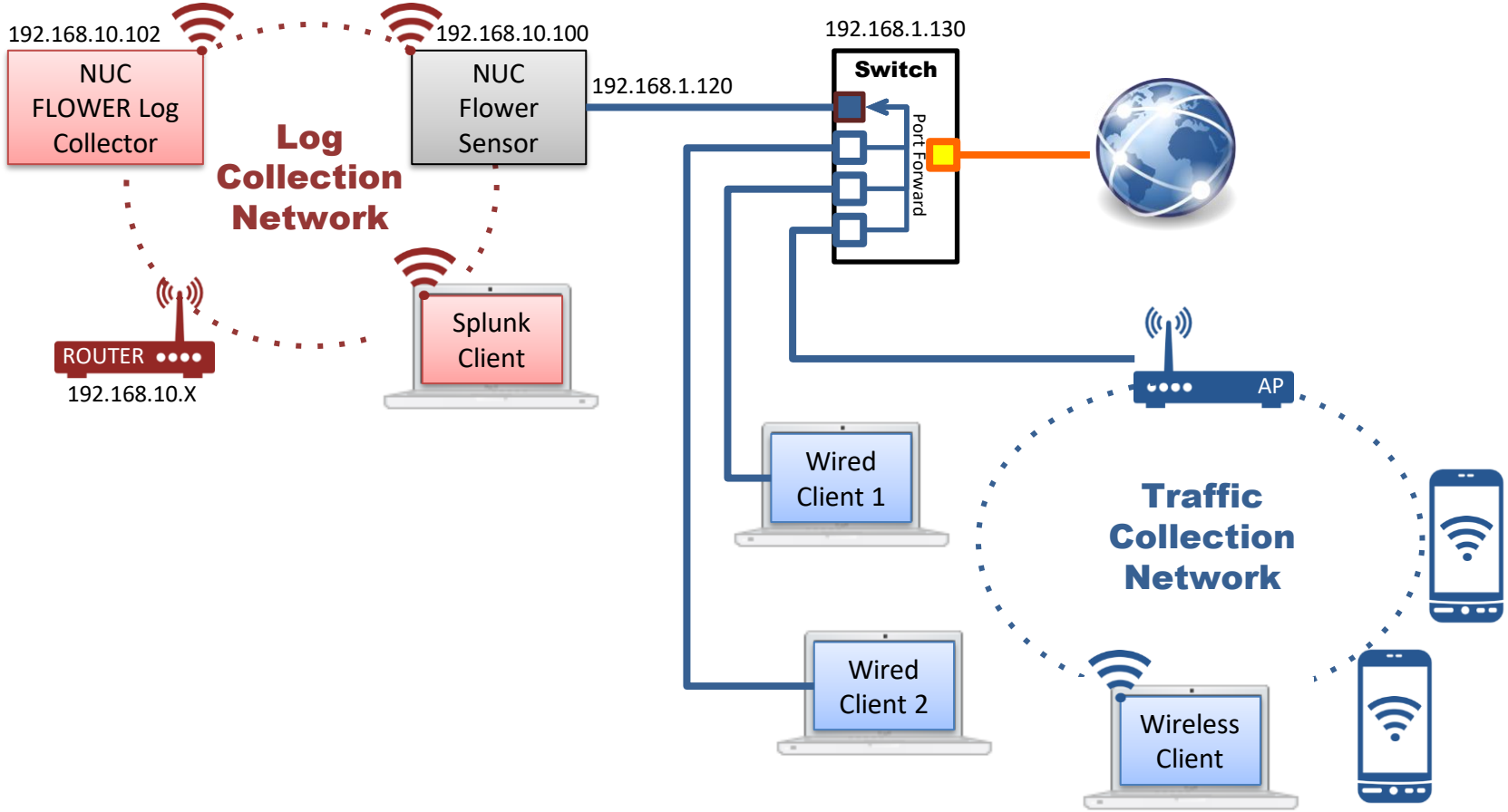
- **Simple to Deploy Almost Anywhere**
  - As software on existing servers (small footprint)
  - Dedicated appliance (Pi, NUC, Data Center)
  - Works on VMs, Docker, systemd-nspawn
  - Collect Data via back channel (stealth)
- **FAST!**
  - Can capture millions of packets per second
- **Integrates with existing SIEM and data archives**
  - Splunk, Hadoop, InfluxDB, and RDBMS
- **Independently tested and verified**
  - Assured Information Security, Inc. (https://www.ainfosec.com)
- **Well Documented**
  - Build, Installation, Data, and Operations Guides

Pacific Northwest NATIONAL LABORATORY

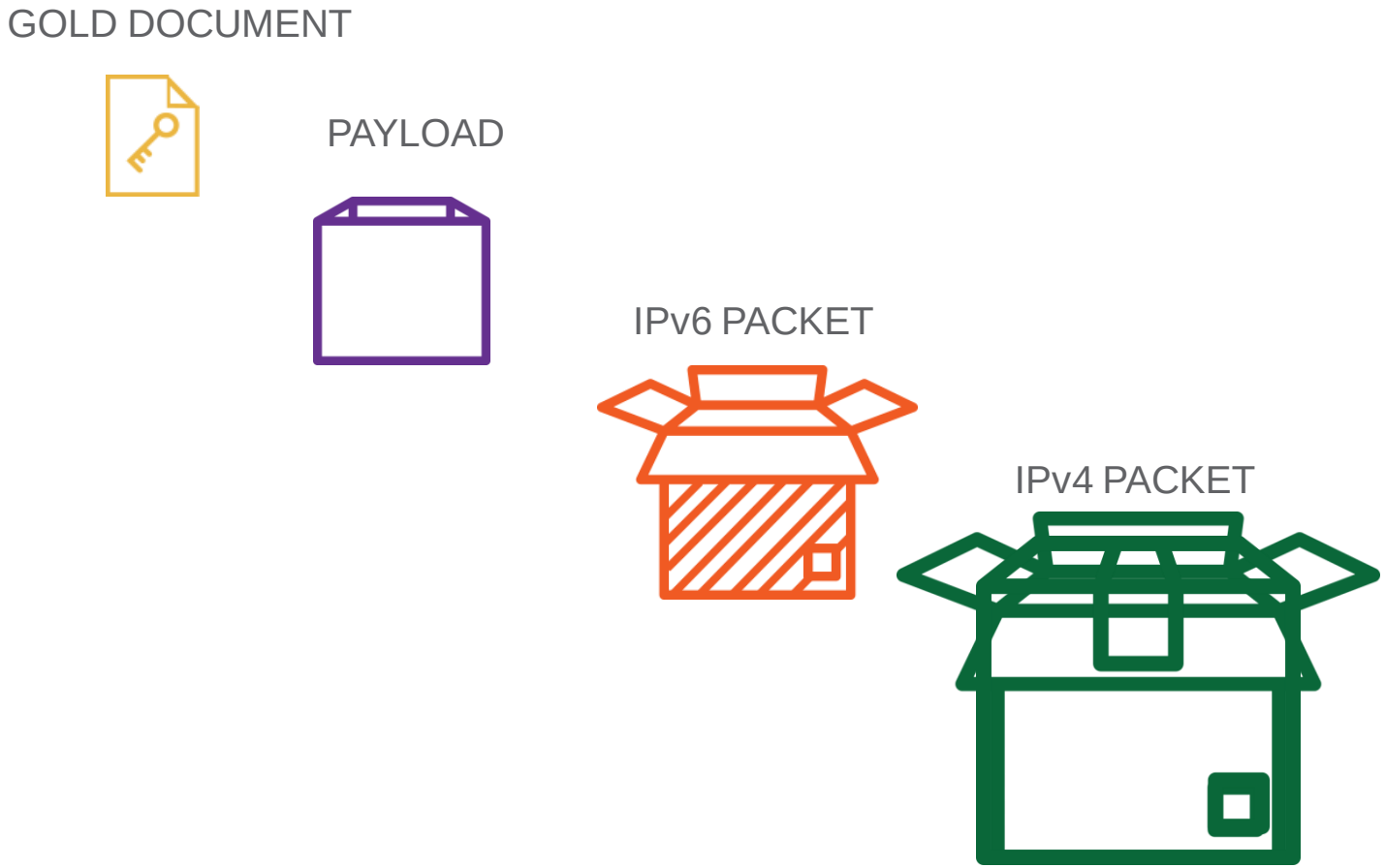
Enterprise Taps



Capture FLOWER Data at Conference

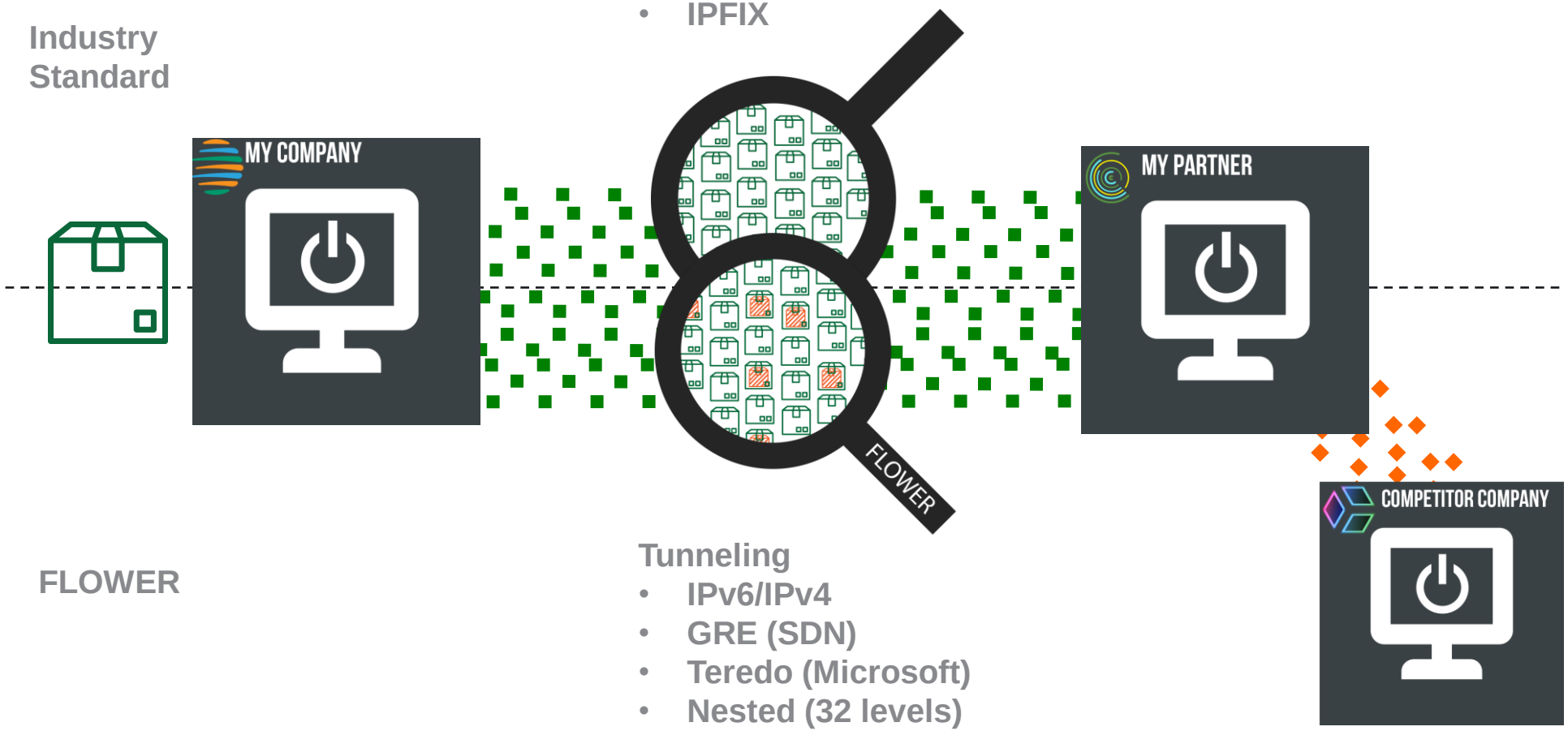


Example: Insider Threat – Data Loss



US-CERT SiLK
SolarWinds
- network flows
- IPFIX

Industry
Standard



FLOWER

Tunneling
- IPv6/IPv4
- GRE (SDN)
- Teredo (Microsoft)
- Nested (32 levels)

Anomaly Detection (RFCs)
VLAN Detection

Pacific Northwest NATIONAL LABORATORY

Ex: Splunk view of FLOWER Data

Industry Standard

	sTime	eTime	dur	sIP	dIP	sPort	dPort	pro	packets
1	2016/02/15T22:16:12.822	2016/02/15T22:16:12.841	0.019	172.31.28.230	172.31.0.2	46725	53	17	1
2	2016/02/15T22:16:12.841	2016/02/15T22:16:12.841	0.000	172.31.0.2	172.31.28.230	53	46725	17	1
3	2016/02/15T22:16:01.143	2016/02/15T22:16:12.928	11.785	172.31.28.230	216.218.226.238	0	0	41	11
4	2016/02/15T22:16:01.150	2016/02/15T22:16:12.928	11.778	216.218.226.238	172.31.28.230	0	0	41	9

FLOWER

	sTime	eTime	dur	fsIP	fdIP	sPort	dPort	pro	sPackets	dPackets
1	2016/02/15 14:16:01 -0800	2016/02/15 14:16:03 -0800	2.010699					58	3	3
2	2016/02/15 14:16:12 -0800	2016/02/15 14:16:12 -0800	0.019177	172031028230	172031000002	46725	53	17	1	1
3	2016/02/15 14:16:12 -0800	2016/02/15 14:16:12 -0800	0.086099			38832	80	6	8	6

	fsIP6	fdIP6	ICMP_ELF	TCP_ELF	tDepth	tsIP	tdIP	tpro
1	20010470000A08BE0000000000000002	20010470000A08BE0000000000000001	+8000-8100+8000-8100+8000-8100		1	172031028230	216218226238	41
2								
3	20010470000A08BE0000000000000002	2607F8B0400E0C04		+02-12+10+18-10-10-10+10+10-18+10+11-11+10	1	172031028230	216218226238	41