
BLOX FEST
Infoblox

Rod Rasmussen

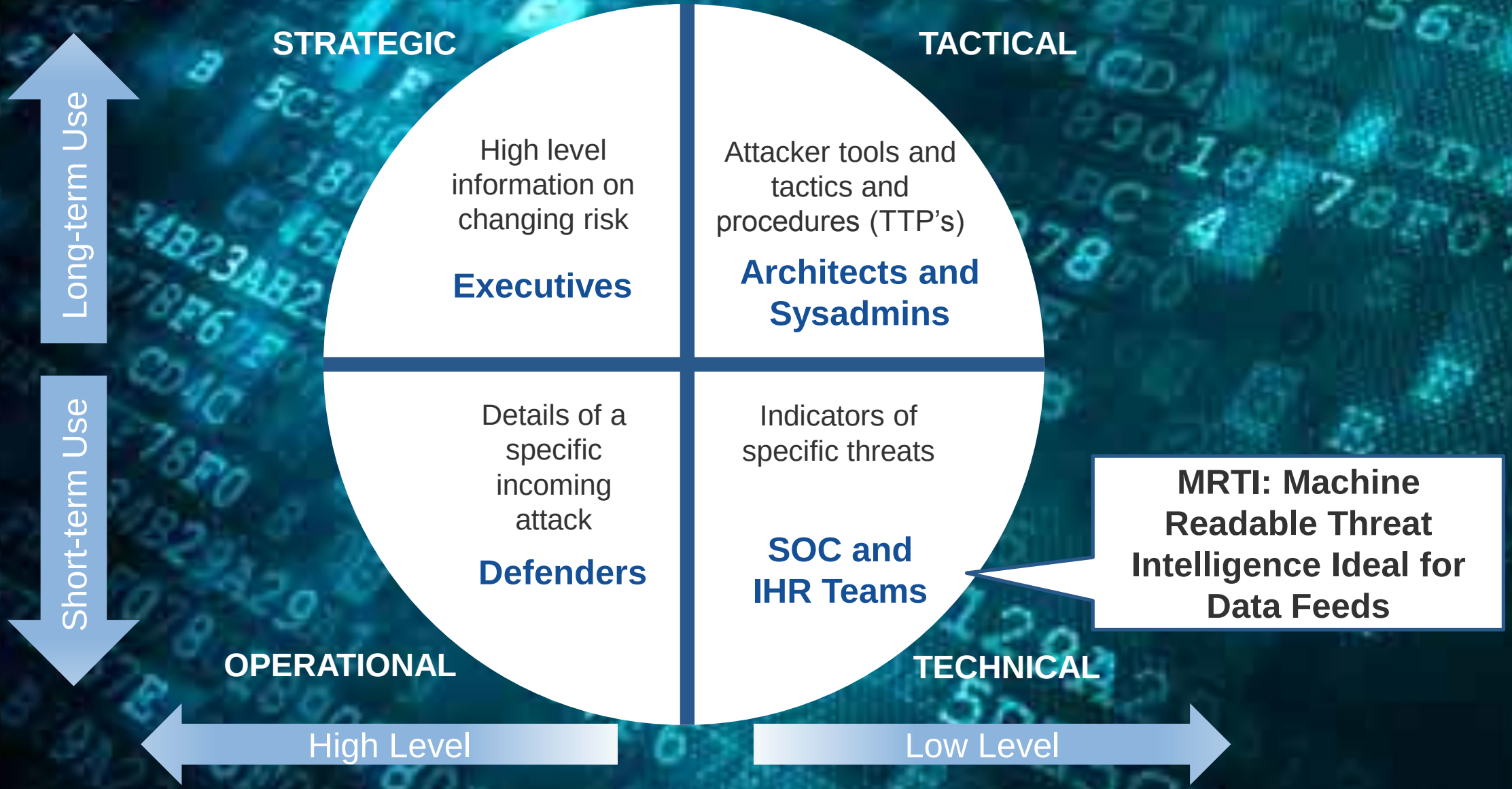
VP of Cybersecurity



They Are Out to Get You - Combatting Malware and APTs by Leveraging Threat Feeds

BLOX FEST

What is Threat Intelligence?



MRTI: Machine Readable Threat Intelligence Ideal for Data Feeds

Adapted from: *Threat Intelligence:Collecting, Analysing, Evaluating* by MWR Security, CPNI, CERT.UK, 23 March 2015

Where Do Most People Get MRTI?

VIPRE from SUNBELT SOFTWARE
TREND MICRO
pctools
McAfee
KASPERSKY lab
ca
eset
AVG
G DATA
PANDA SECURITY
AhnLab
avast!
Norton from symantec
F-Secure
Microsoft Security Essentials
webroot
Quick Heal
RISING
bitdefender

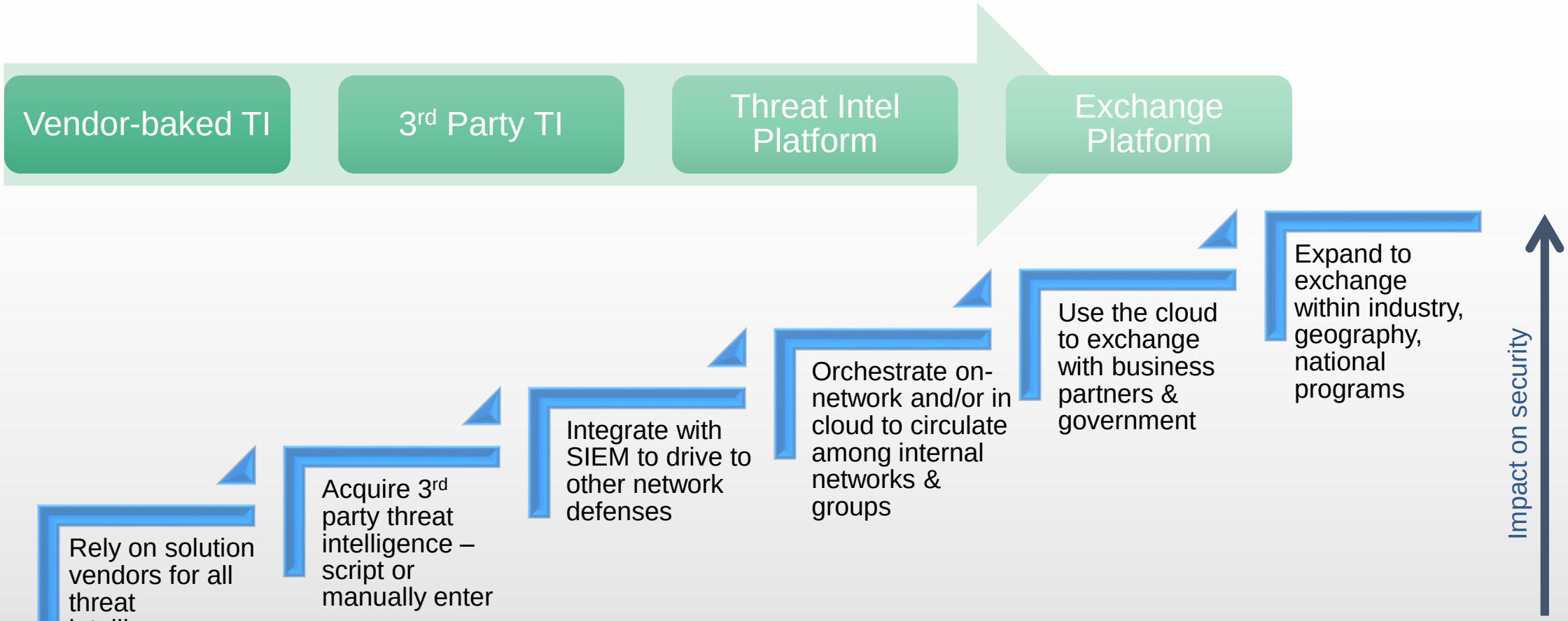
Problem:

These devices and software suites don't talk to each other to ensure full coverage of threats and they largely don't share the intel they do have directly with their users. They also don't have the full picture of everything evil – no one does!

BLOX FEST

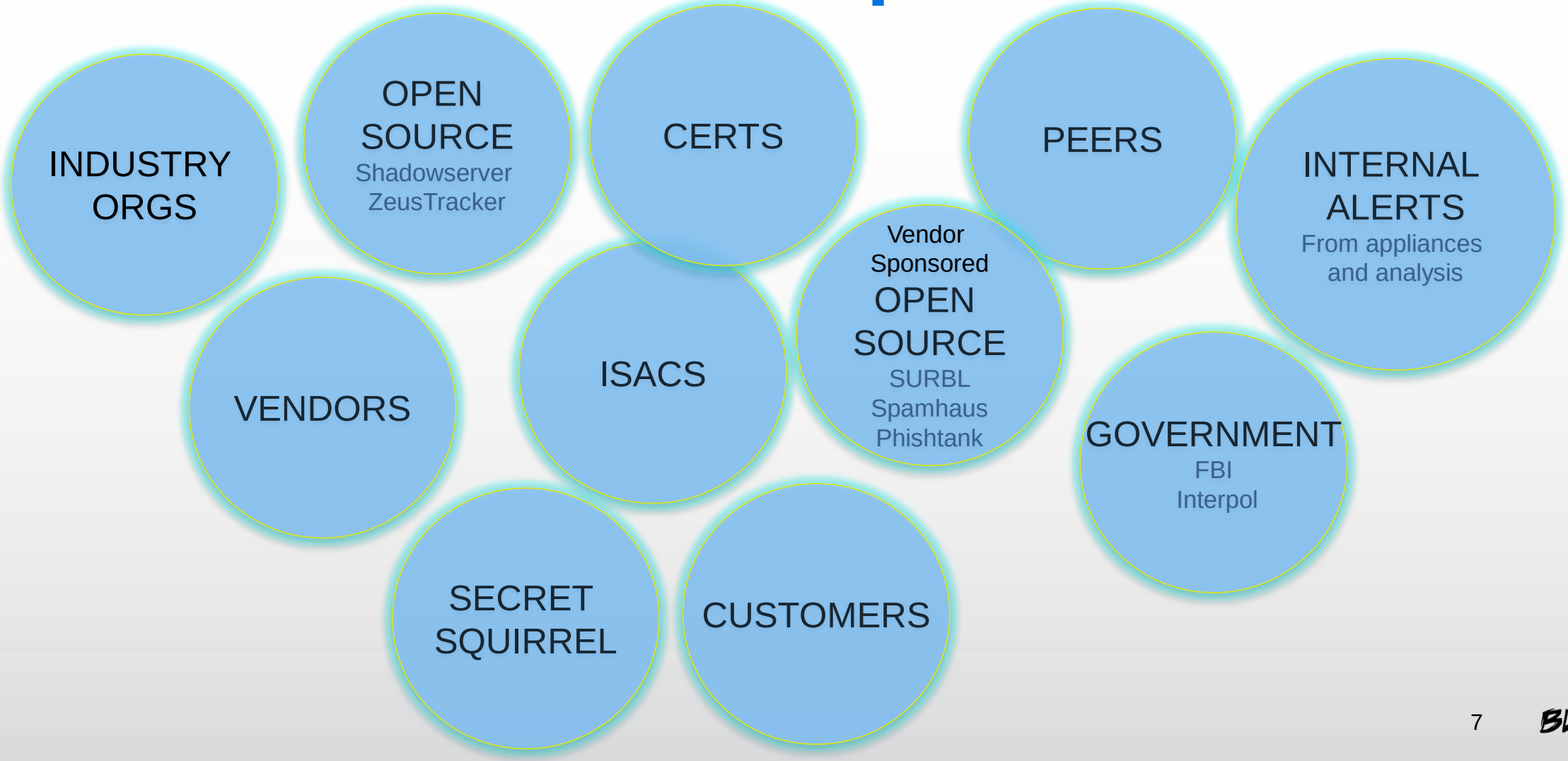
Leveraging Threat Intelligence

How to use Threat Intel as your security organization matures



BLOX FEST

Threat Intel Source Options

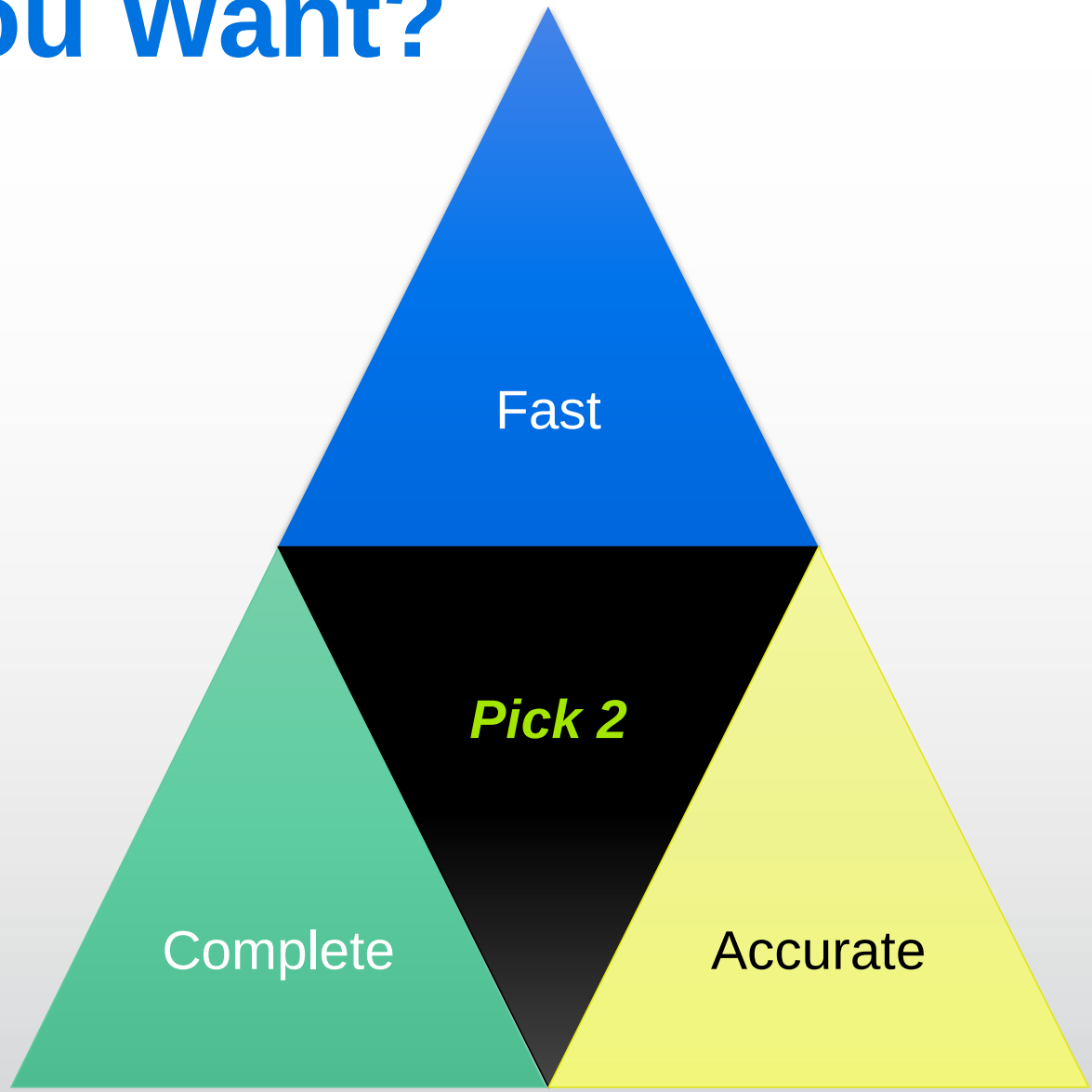


BLOX FEST

Sources Cover Many Important Things

- IPs, hosts, malware hashes, TTP's, e-mail, account info, etc.
- Recent CERTCC study showed amazing lack of overlap amongst most popular "open source" data feeds
  - Over 96% of hostnames were unique to one feed only (sample size >30 million hosts on 13 lists)
  - Over 82% of IP addresses were unique to one feed only (sample size >120 million IPs on 38 lists)
  - http://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_428614.pdf

What Do You Want?



BLOX FEST

Even Less Capacity to *Use* Data

Product	Rule/protection type	Max Entries
Firewall vendor 1	Security rules (IPs/ASNs)	40,000
Firewall vendor 2	Maximum Firewall Policies	100,000
Firewall vendor 3	Maximum Firewall Policies	40,000

- IDS systems have rule or practical performance limits that kick in depending on hardware
- RBL's, DNSBL's, web proxies, and other in-line products that match against known threats all run into capacity and performance problems eventually
- Flexible analysis tools (e.g. Splunk) have cost considerations

All Intel is Useful for Something—Use Case Matters MOST

- Life is shades of gray, not black and white
- Reputation and context are key for use
- Block | Alert | Inform scoring | “Fits a pattern” | “Kill Chain” point
  - For example, google.com
    - In an ISP blacklist = disaster.
    - In a malware analysis tool doing wireshark on a bare-metal honeypot = likely sign of malware activity
  - Fit the data to your purpose

DATA EXFIL | SPAM | VULN Scanning | VIRUS Scanning

Dangers of Threat Intel That's Just Noise

- False positives
- Incomplete or missing context
- No concept of TTL or useful life
- Lack of understanding good applications for data
- Not relevant to your risk situation (one size fits all data)

Noiseworthy vs. noise

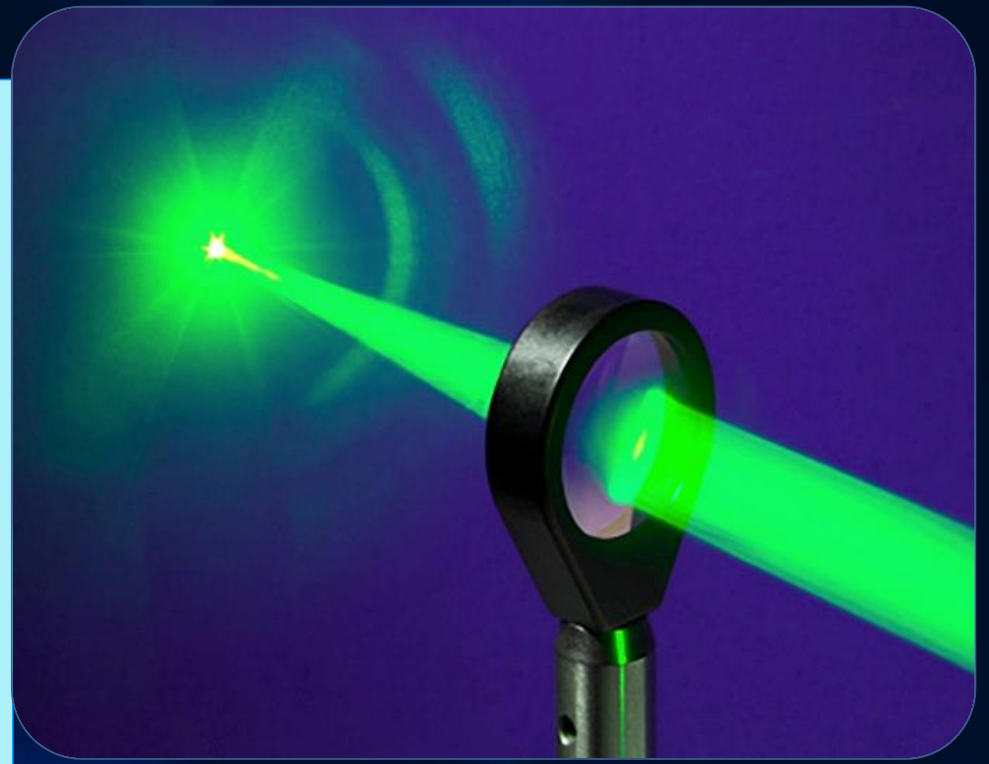
Determine trustworthiness of source

Use internal threat intel and reputation to determine false positives

Analyze metrics across all data

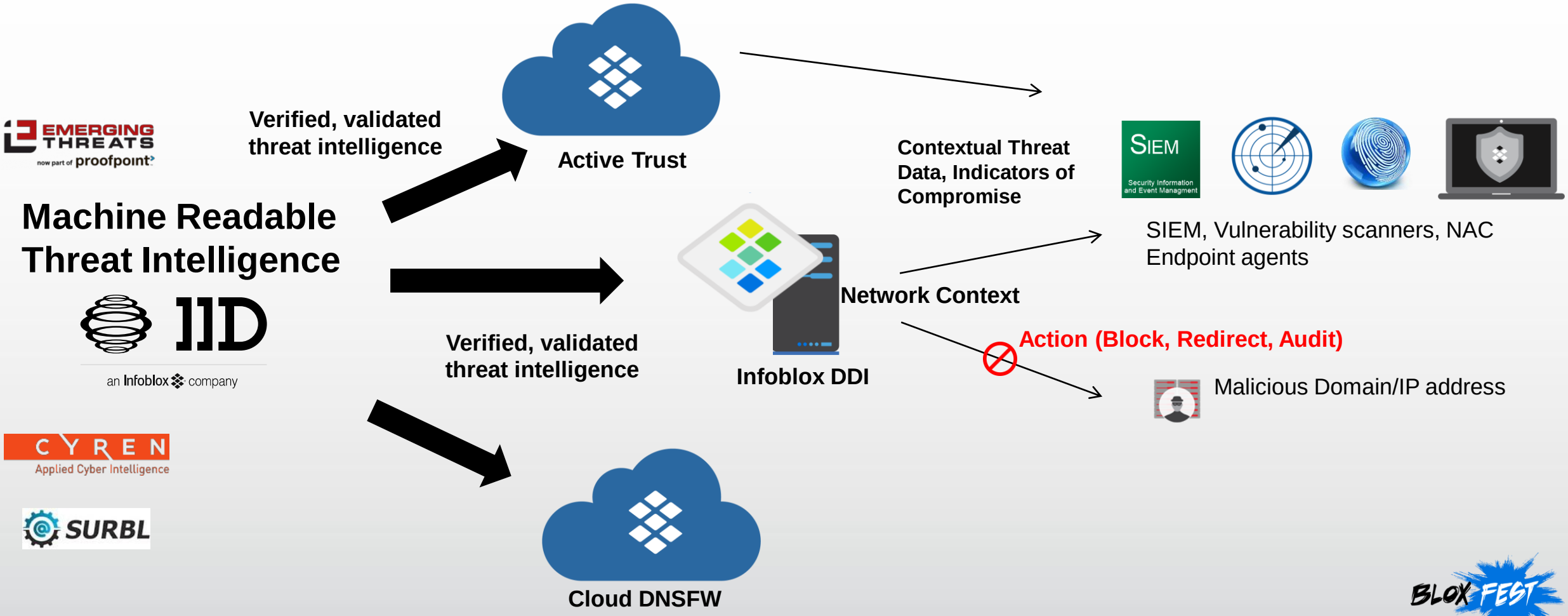
Increase confidence with correlation, frequency and source reputation

Expand context by linking related data points to previous unknowns



Infoblox Approach: Threat Intel Platform Ecosystem

Attend the Infoblox Security Strategy session for complete details!

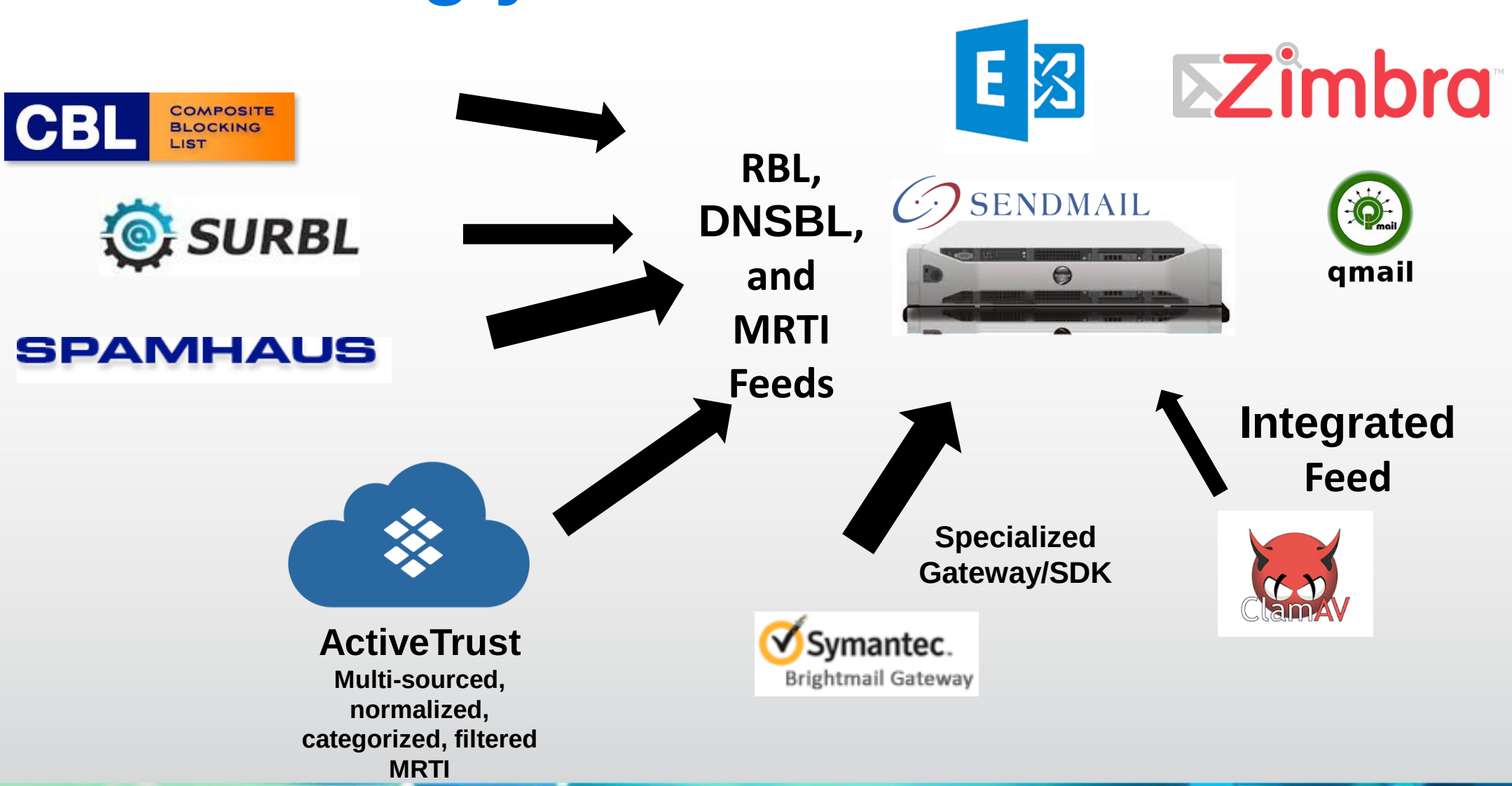


BLOX FEST

Use Case: E-mail Threat Prevention

- E-mail remains the primary entry point for nearly all types of major threats: APT, (spear) phishing, ransomware, banking trojans, etc.
- A 20+ year-old MRTI use case – a classic that is well baked!
- Supplement existing solution with solid MRTI data – typically RBL's for blocking known spam sources
  - SURBL, Spamhaus, CBL,ClamAV,
  - Infoblox providing high-quality data via ActiveTrust
- Add external threat feeds via custom plug-ins/integrations
- Content data to quarantine potential lure messages based on message bodies

Bolstering your MTA

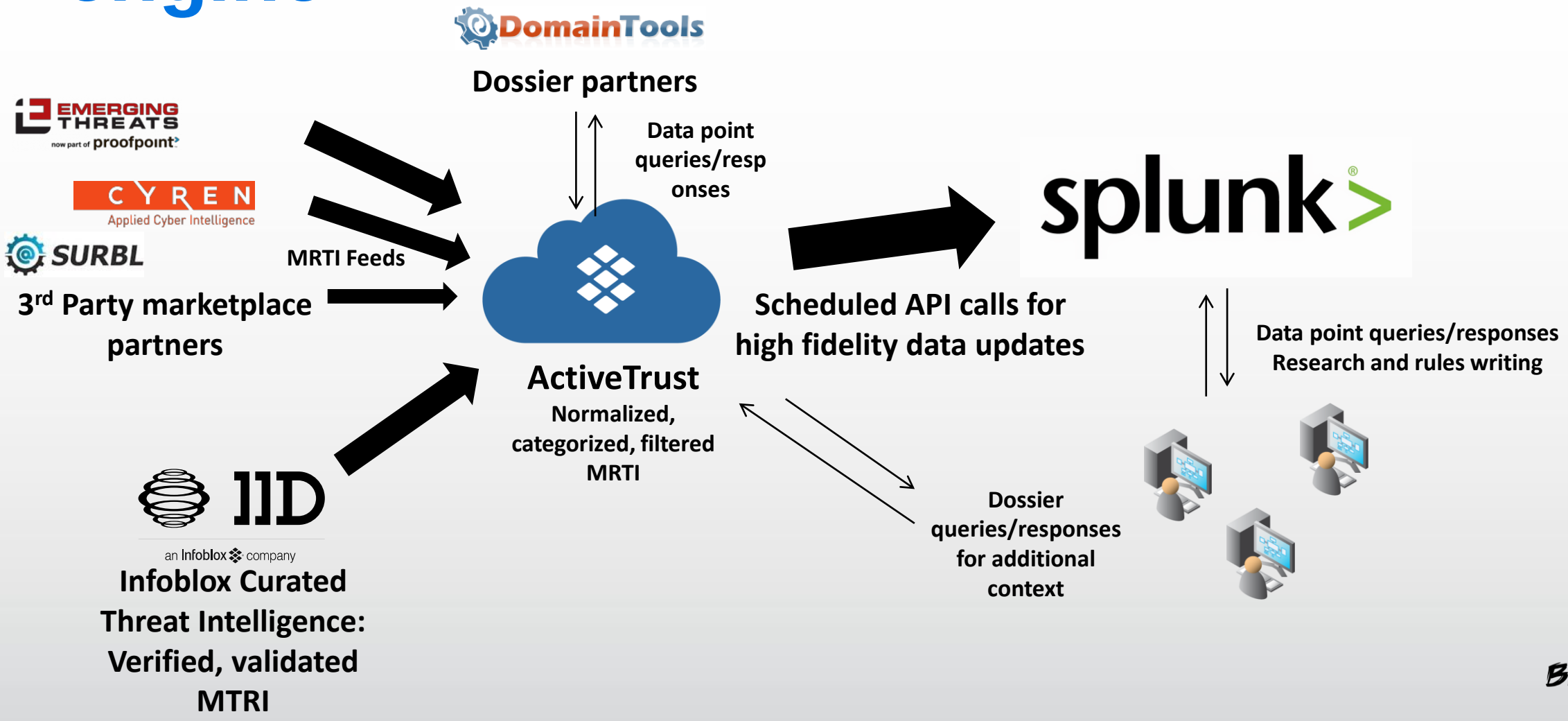


BLOX FEST

Use Case: Splunk as research repository

- Major enterprise with security team and many tools
- Needs TI data in central repository for current and historical assessments of alerts/potential issues
- Must have completely “clean” data with fullest context possible
- Does not want to have to source/manage all data themselves
- Putting everything into Splunk for ubiquitous access and efficiency in writing/using analysis applications and tools
- Fractional access via API to larger data sets to bring in more contextual data when needed

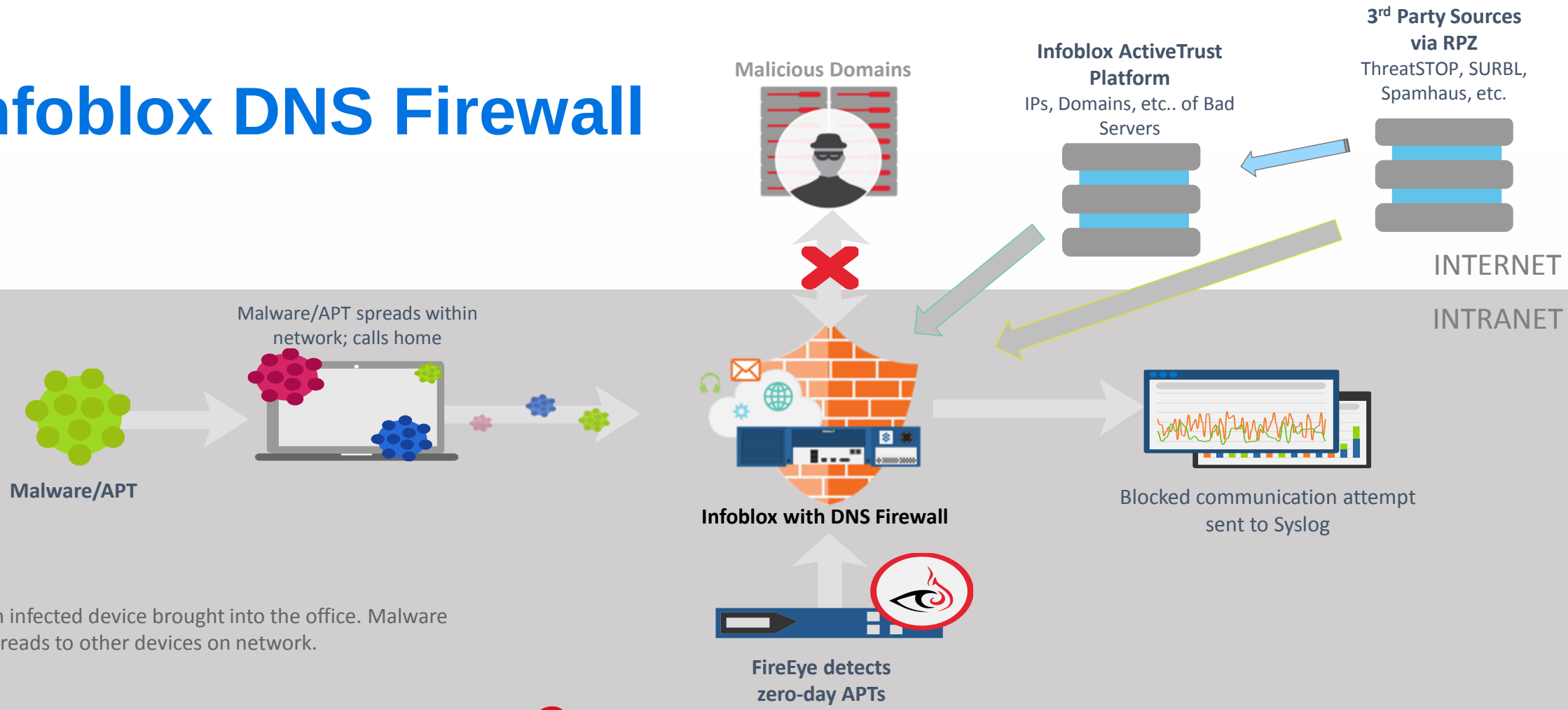
Splunk as a data repository analysis engine



Use Case: DNS Firewall

- We’re all using them right?
- Block, redirect or alert on requests for tagged domains/hosts/IP’s
- Highly effective and relatively cheap to implement vs. “yet another box on a spanning port” or an in-line traffic analysis/firewall system
- Combine with DDI data for full visibility
- Use of RPZ’s allows for multiple data sources and policies
- Bonus: analyze your DNS traffic to find tunnels, DGA’s, C2 comms and other suspicious activities

Infoblox DNS Firewall



1 An infected device brought into the office. Malware spreads to other devices on network.

2 Malware makes a DNS query to find "home" (botnet / C&C). DNS Firewall looks at the DNS response and takes admin-defined action (disallows communication to malware site or redirects traffic to a landing page or "walled garden" site).

3 **Pinpoint.** Infoblox Reporting lists DNS Firewall action as well as the:

- Device IP address
- Device MAC address
- Device type (DHCP fingerprint)
- Device host name
- Device lease history

4 Data updated regularly to add new threats and remove mitigated/non-applicable DNS locations.

5 Additional threat intelligence from sources outside Infoblox can also be used by DNS Firewall (e.g. FireEye, ThreatSTOP, SURBL)

LEVERAGING ACTIONABLE THREAT INTELLIGENCE IN PROVIDER NETWORKS

Because They Have Been Out To Get Us for A Long Time

Jay Tumas
Sr. Director
Cyber Security Architecture

FairPoint communications

WHAT A LONG STRANGE TRIP IT'S BEEN

- 9 Years at New England Telephone/NYNEX/Bell Atlantic/Verizon
- 16 Years Leading Network Operations and Cyber Security at Harvard University
  - Network Security and Incident Response Team in 1999
  - Digital Forensics Lab Operations in 2002
  - Operations Manager for the Northern Crossroads (NoX)
  - Longwood Medical Area Technical Subcommittee Chair
  - University CALEA Compliance Officer
  - New England Electronic Crime Task Force Member
  - Infragard BoD – New England Chapter
- Sr. Director at Fairpoint Communications focusing on Threat Mitigation
  - DNS Infrastructure Planning and Future Services
  - Threat Mitigation – Infrastructure Protection, DDoS Countermeasures, Malware Defense
- General Class Ham Operator (KC1FGW) and Motorcycle Enthusiast!
  - 73's to all you "Rag Chewers" out there!

FairPoint communications

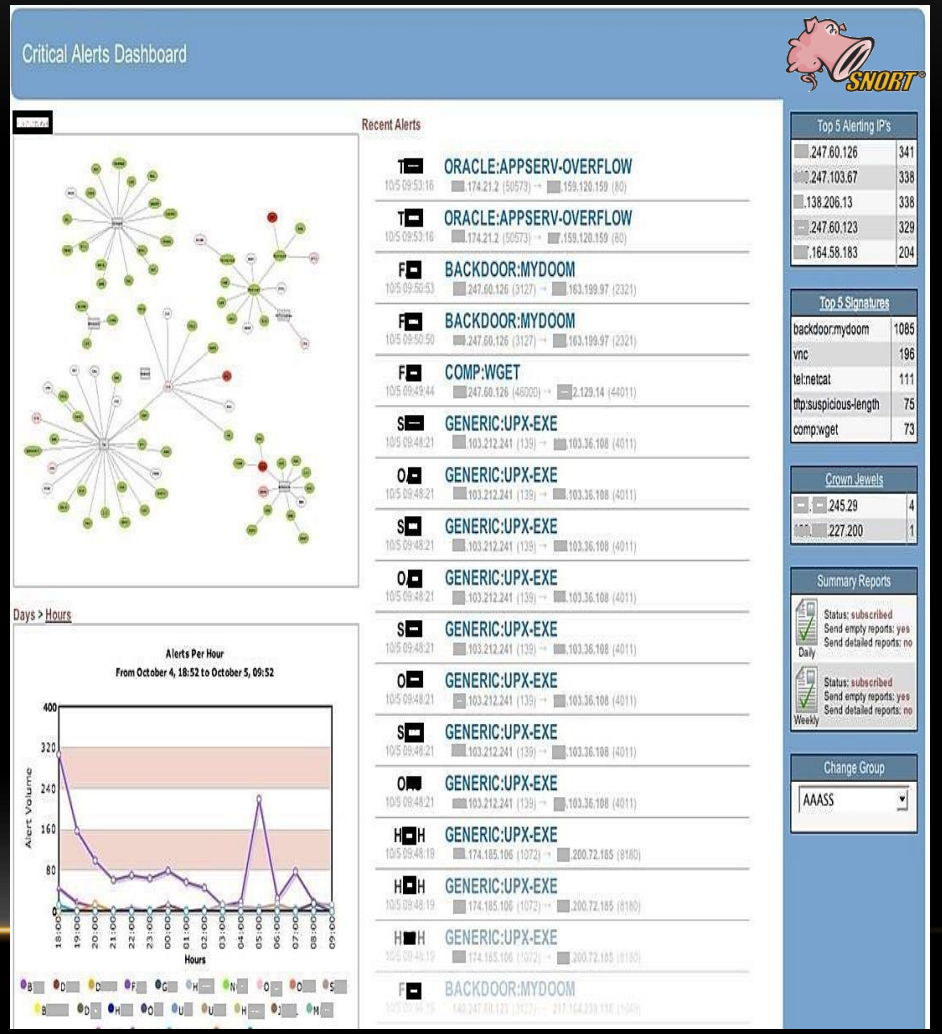
FAIRPOINT COMMUNICATIONS

- IT Services and Telecommunications Provider
  - Headquartered in Charlotte NC
  - Services delivered in 31 markets across 17 states (ILEC)
  - Largest holding is our NNE Property – Purchased from Verizon in 2008
  - POTS, CTBH, Digital Subscriber Line, Carrier Ethernet Services (10 Gbps)
  - HPBX, Managed Networking, EDC Colocation
- Focus on future Advanced and Managed Security Services development
  - DDoS Mitigation and Threat Management
  - Public Cloud Services
  - Hardened rDNS Services

FairPoint communications

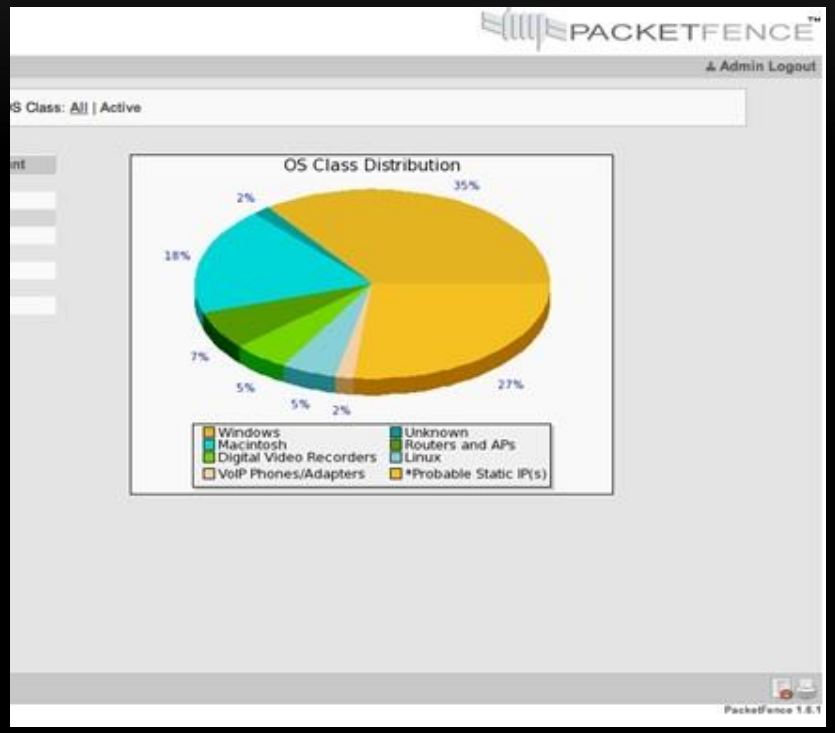
EARLY ADOPTION OF OPEN SOURCE MRTI

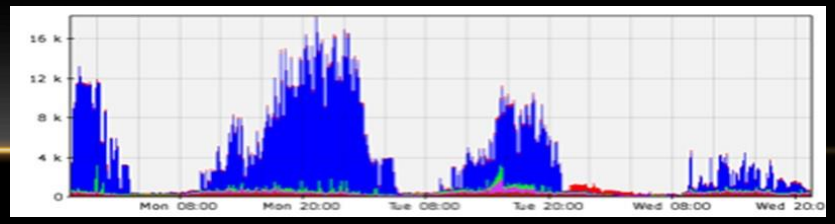
- SNORT – Open Source IDS/IPS (1998)
  - Leveraged for it's ability to apply sigs and analyze live traffic (1999)
  - Combined signature, protocol and anomaly based traffic inspection
  - Ability to "feed" MRTI (Rule Sets) to SNORT a priority for a small operation
  - ~20 High Confidence signatures triggered Auto-Alerting to the community
    - BOTnet and Trojan Activity, BF Attacks and behavioral sigs indicative of scanning activity
    - 0% False Positive Rate instilled community confidence and acceptance in the service
  - Interesting Rule Set Categories
    - protocol-scada, protocol-rpc, malware–cnc, malware-backdoor, malware-tools (LOIC)
  - First in the industry implementation
    - Production SNORT on NIC ASICS



THREAT AWARE NETWORK ACCESS CONTROL

- PacketFence Project initially developed to address secure NAC
  - Massive worms of the early 2000's birthed 1000's of infected systems on client and residential networks
  - Needed a NAC with the ability to detect infected systems, isolate and assist with remediation
  - Integrated Radius and DHCP with SNORT IDS and a Vulnerability Scanner
- SNORT MRTI enabled 0-Day detection of abnormal network activities
  - Now integrates with Suricata IDS
  - Can be combined with malware hash databases
- 2005 Zotob worm event not so much of an event!
  - Exploited MS05-039 vulnerability
  - Outbound flows of associated scanning by infected systems evident
- Packetfence.org

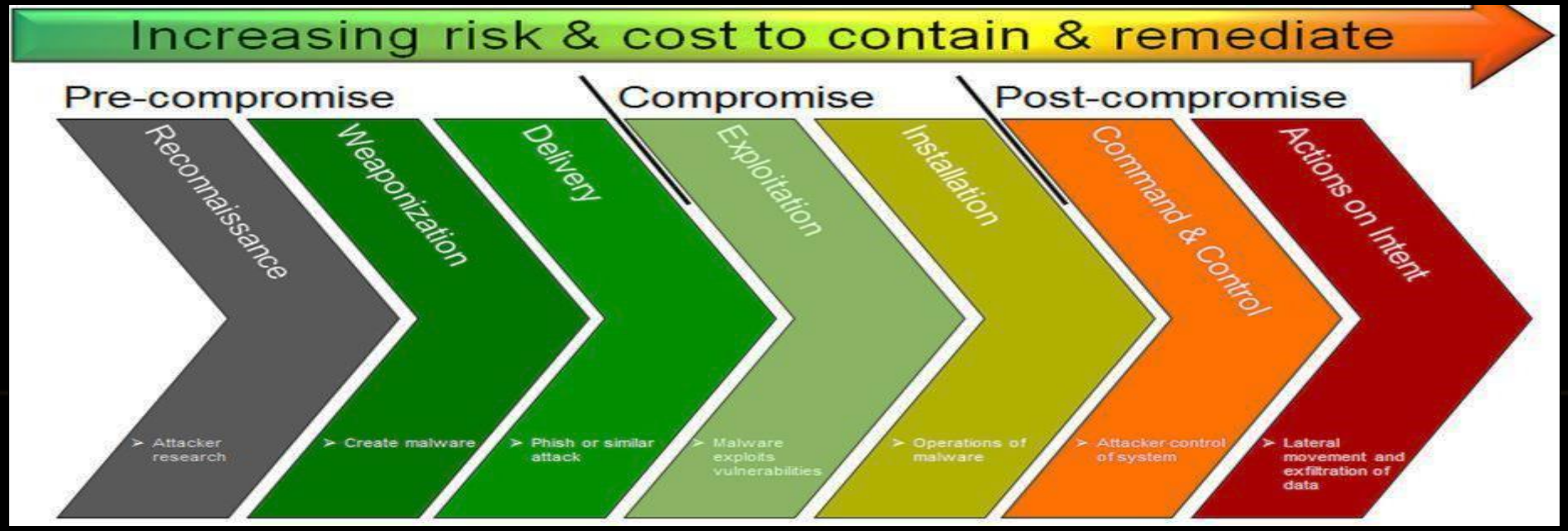




THE PACKETFENCE PROJECT LIVES!

ATTACKING THE CYBER KILL CHAIN

- Win the Battle before it begins!
- Threat Actors are innovating faster that defenders
- Commercialization of the Malware Market – Rent-a-botnet really cheap!
- Malware products adapt over time
  - Reuse of Malware, C&C Protocols, and Methods
- Machine Readable Threat Intelligence (MRTI) the only way to keep up
- Many attacks begin with successful DNS queries

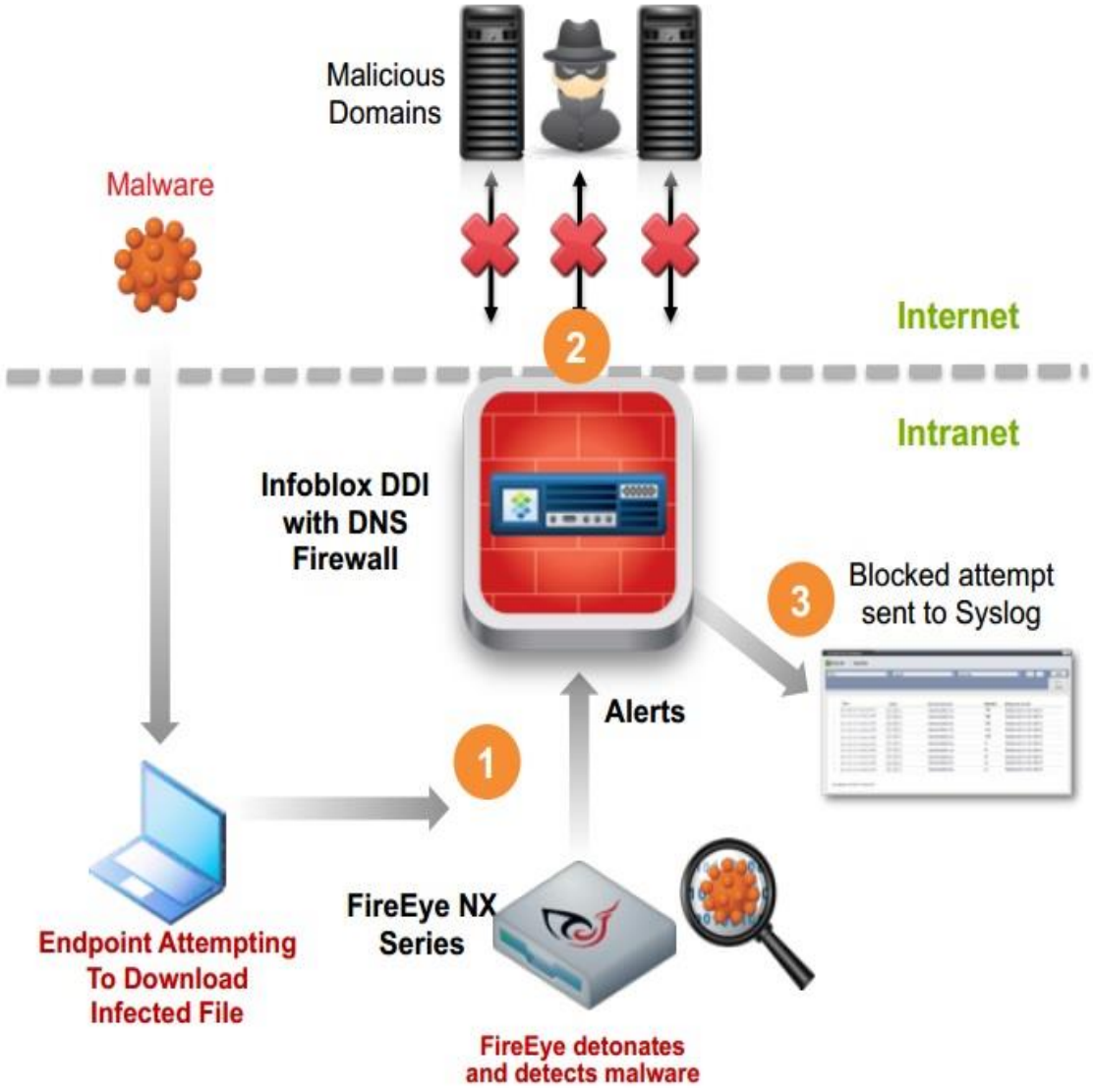


USEFUL SOURCES OF MRTI

- Multiple Threat Intelligence Resources Available for Splunk
  - Add-on for Cisco FireSIGHT (formerly Sourcefire) leverages data collected from eStreamer
    - Correlate Cisco NGIPD and NGFW log data with Advanced Malware Protection (AMP) reports
    - Cisco FireSIGHT and Snort IDS events through the Splunk Common Information Model (CIM)
  - ThreatStream, RiskIQs PassiveTotal, Novetta Cyber Analytics
- Atlas Intelligence Feed (AIF)
  - Product of Arbor Security Engineering and Response Team (ASERT)
  - Detection and mitigation of malware, botnets and DoS attacks
  - Provides analysis and countermeasures for volumetric, application and protocol anomalies
  - Advanced feed uncovers campaign style attack behaviors (scanners, APT, RAT, rootkits)
- FireEye Threat Intelligence
  - Dynamic Threat Intelligence (DTI) up to Advanced Threat Intelligence Plus (ATI+)
  - Integration Hub offering now aggregates alerts from FE and Non-FE tools
  - Combine the power of FireEye APT detection with Infoblox DNS level blocking and device fingerprinting
  - Disrupt APT malware communications and pinpoint infected devices quickly

Infoblox DNS Firewall - FireEye Adapter

Blocking APT



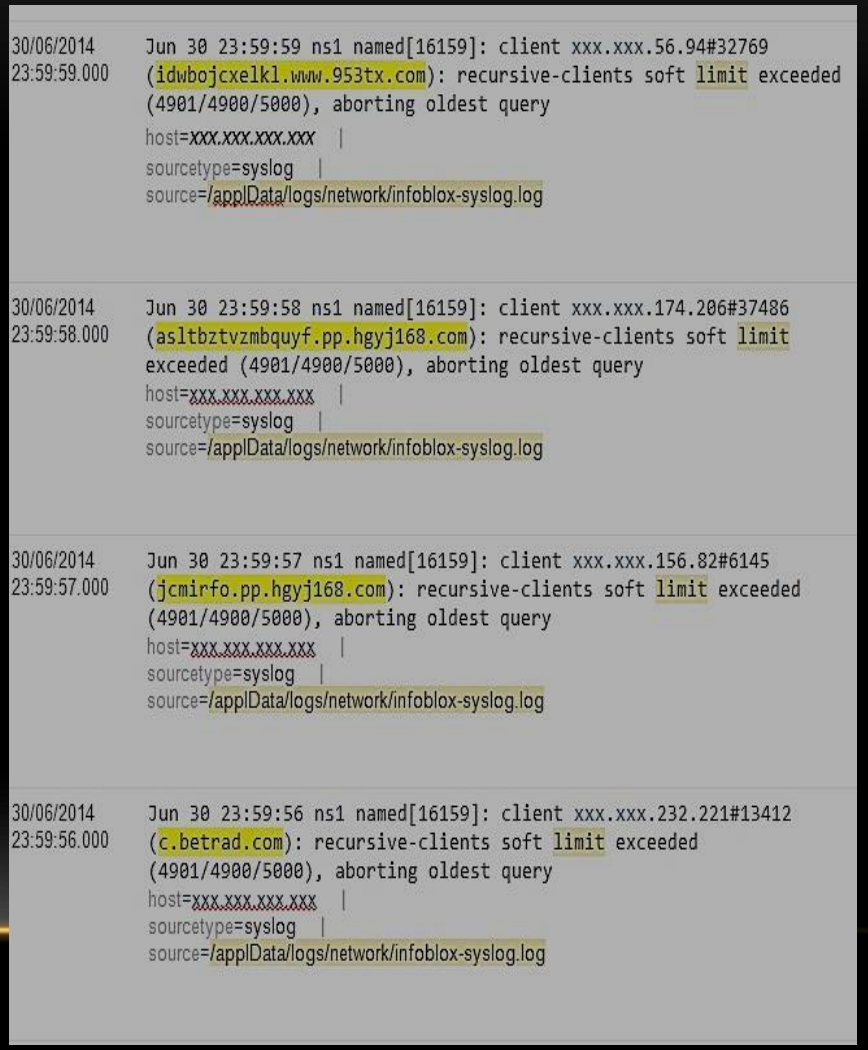
1. **Detect** - FireEye detects APT, alerts are sent to Infoblox.

2. **Disrupt** – Infoblox DNS Firewall disrupts malware DNS communication

3. **Pin Point** - Infoblox Reporting provides list of blocked attempts as well as the
   - IP address
   - MAC address
   - Device type (DHCP fingerprint)
   - DHCP Lease (on/off network)
   - Host Name

VULNERABLE CUSTOMER NETWORKS

- ISP and Customer networks under assault
- ISP's are uniquely positioned to provide visibility and assistance to targeted customer's
  - Basic Cache Poisoning attacks
  - Domain Lock-Up Attack
  - NXDOMAIN Attack
  - Phantom Domain Attack
  - Random Subdomain (Slow Drip) Attack
- Slow Drip Attack
  - Possibly start with infected client systems
    - Malware infections forming botnets
  - Randomly generated subdomain strings
  - Prefixed to a victim's domain
  - Thwarted with IB ADP/FW



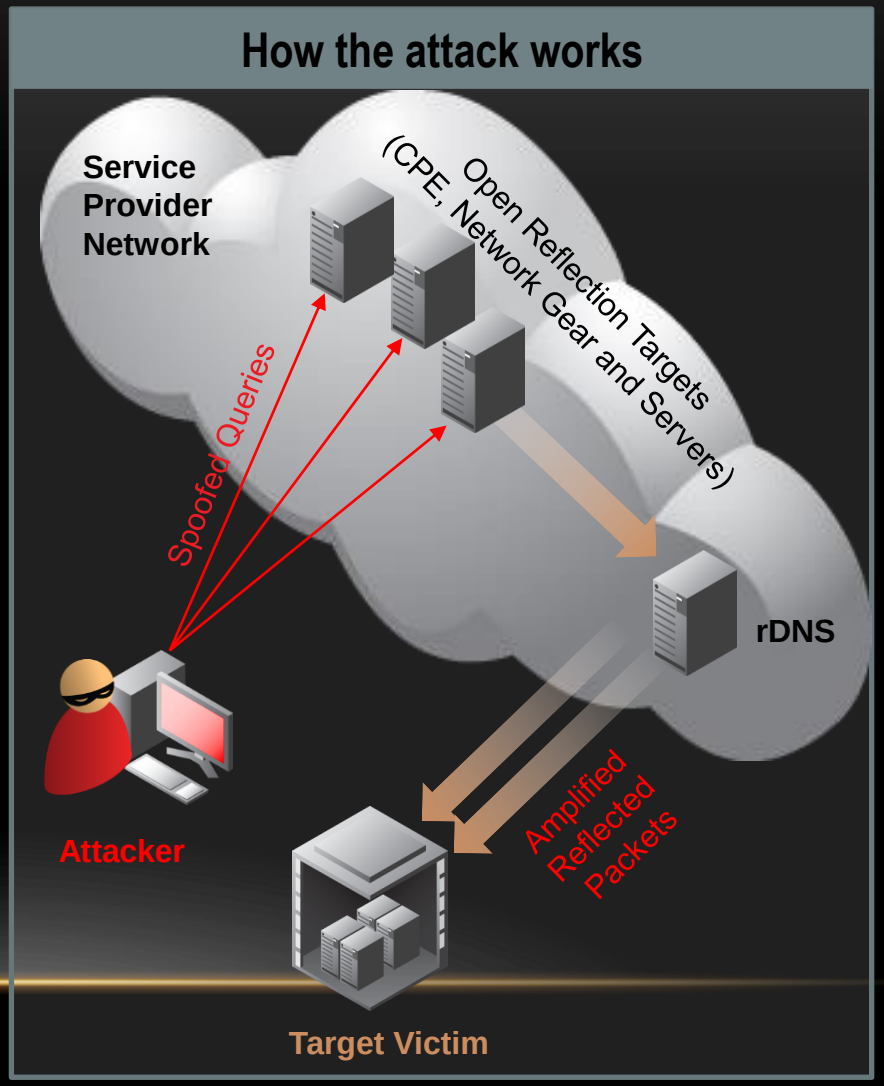
PROVIDING HARDENED DNS AS A MANAGED SERVICE

- Customer networks remain soft targets
  - Open Recursive DNS infrastructure
  - Misconfigured forwarder in external zones
  - Misconfigured network gear
    - Exposing UDP/53 externally
    - Any exposed services
    - Vulnerable systems and servers
- Soft targets are discovered quickly
- Upstream SP positioned to assist?
- Leverage Infoblox ADP infrastructure
  - Dedicated Hardware
  - ISP grade performance
    - Caching Acceleration
  - Immediate update to new security threats
- Whitelist Customer IP Addresses for access
- Provide additional value to customers
  - Identify compromised clients
  - Provide detailed reports

ISP RDNS AS COLLATERAL DAMAGE

Distributed Reflection DoS Attack (DrDoS)

- Possibly reflection and amplification
- Uses available open resolvers or targets that reflect specific traffic
- Attacker sends spoofed queries to the open reflection targets
- Reflection bounces queries to rDNS
- Shear volume of queries grinds the unprotected ISP's rDNS to a halt
- Causes DDoS on the victim's server as well as the ISP's rDNS servers



ISP NETWORKS UNDER CONSTANT ASSAULT

- Service Provider networks are target rich for Amp/Ref Attacks
- 1000's of misconfigured devices
- Don't require botnets or malware
- Vendor supported Broadband Modems demonstrated to be effective vectors
  - DNS (UDP/53)
  - NTP (UDP/123)
  - SNMP v2 (UDP/161)

- Attackers leverage any reflection target they can discover through reconnaissance
  - Unsolicited scanning of network infrastructure flags possible future attacks
  - SP infrastructure globally has been targeted
- Broadband modems found not to react well when flooded with DNS traffic
  - ~3000 queries in <3 minutes found to crash DNS process
  - Increased customer troubles – Negative customer experience!
  - Work with Vendors to harden network CPE through new firmware
- Block inbound UDP/53 where not required – Implement DNS Auth elsewhere

OPERATIONALIZE THREAT INTELLIGENCE

- Threat Intelligence vs. Vulnerability Intelligence
- Evaluate your unique “Attack Surface”
- Don’t forget about Open Source Threat Intelligence
- DNS leveraging MRTI clarifies attacks and reveals severity
  - Discover interesting patterns within your network
  - Correlate badly behaving IP addresses with other vulnerability data
- Select Threat Intelligence that best fits into your operation
  - Most secure operational platforms readily leverage Threat Intelligence
  - DNS is a common network service where MRTI is most valuable
    - Consider Internal and External DNS zones for defense in depth
    - ADP and FW continuously adapts to evolving threats without patching or downtime
    - Latest threat intelligence from research and analysis on new threats observed in client networks across the globe

MRTI AS A FORCE MULTIPLIER