
BLOX FEST
Infoblox

Sean Tierney

Enterprise Defender
Cyber Warfighter
Director of Cyber Intelligence

Framing the Conversation

- Often security teams ask the DDI administrators for access to data like IP addresses and DNS records. What do they typically do with that data
- What do security teams usually do when they receive an indicator of compromise

How do we Obtain Threat Data?

Observed – Indicators and data collected from direct observation or experimentation.

Response – Threat data collected during incident response or investigation.

Exchanged – Threat data and intelligence purchased or shared from another party.

PFM is the Cornerstone

Pivot – The practice of revealing new information by traversing from known indicators or initial seed data points to identify associated indicators or intelligence.

Farm – Organic creation of intelligence through investigation, experimentation, and deconstruction of active and historic threats to generate new data or insights.

Mine - Enrichment of threat data to create fused intelligence from existing data collections using transformation, quality assessments, and data analytics. Answer the unknown-knowns.

BLOX FEST

Malware

- Exploit Kits
- Banking Trojans
- Ransomware
- Destructive Attacks

DNS

- Tunneling
- DDoS
- Poisoning
- Hijacking

Data Breaches

- Point-of-sale Malware
- Financial Data Theft
- Personal Records
- Reputational (Anonymous, Lulzsec, Lizard Squad)