SLAIT Consulting

Threat Ops

End Point -

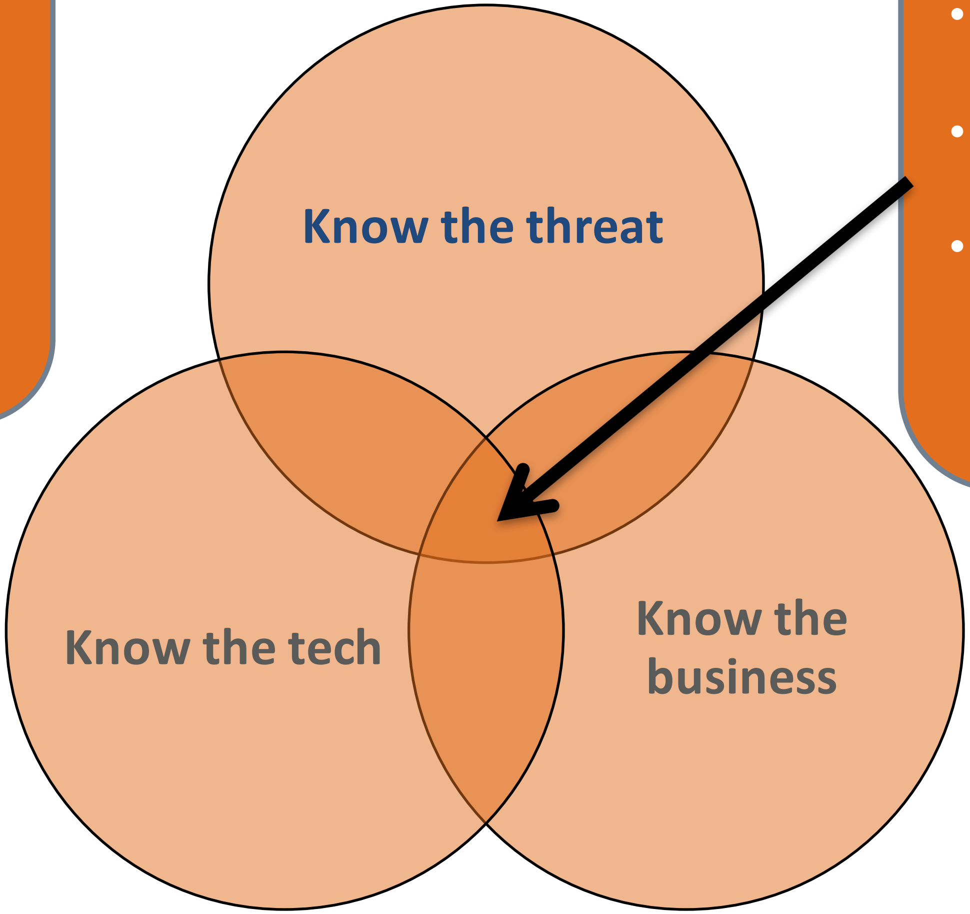
First line of defense

Why are the Good Guys losing?

- Evolving Threats (Bad guys are getting better)
- Program Maturity / Investment Challenges
- Security Staffing Challenges
- Over-reliance on security technologies
- Alert Fatigue (Information overload)

You are Special

Your business really is special
- Different threat landscape
- Different tech stack
- Different business processes



Hunting means:
- Understanding your business-specific threats and motivations
- Understanding your tech stack and blind spots
- Understands the business and what's "normal"

Lets face the facts

Attackers are well funded and sophisticated

91%

Increase in targeted attacks in 2013

Launching Zero-Day attacks are more accessible and common

78%

Of exploit kits utilize vulnerabilities less than two years old

Targeted attacks can only be solved on the endpoint

71%

Of Breaches involve a targeted user device

What do I mean when I think end point?

- Symantic
- Kaspersky
- Bitdefender
- Sophos
- McAfee

- SLAIT Security
- Crowdstrike
- FireEye (Mandiant)
- Fidelis

AntiVirus, White listing, AntiSpam, IPS, Patch management

Active hunting capable, No Blocking, DVR, Live response capable, includes threat intelligence, Sand box, Security analytics

Typical vulnerabilities on the Endpoint?

Endpoint = Desktop, Laptops, Servers, IoT (anything with an OS)

- Operating System (Windows, Linux, OSX)
- Browser
- Application

Why the endpoint?

- Visibility with off network activity
- Solves encryption problem
- Attack surface (endpoint is the preferred target)
- VPN to unauthorized networks (logging network connections)
- Data creation and transmission point

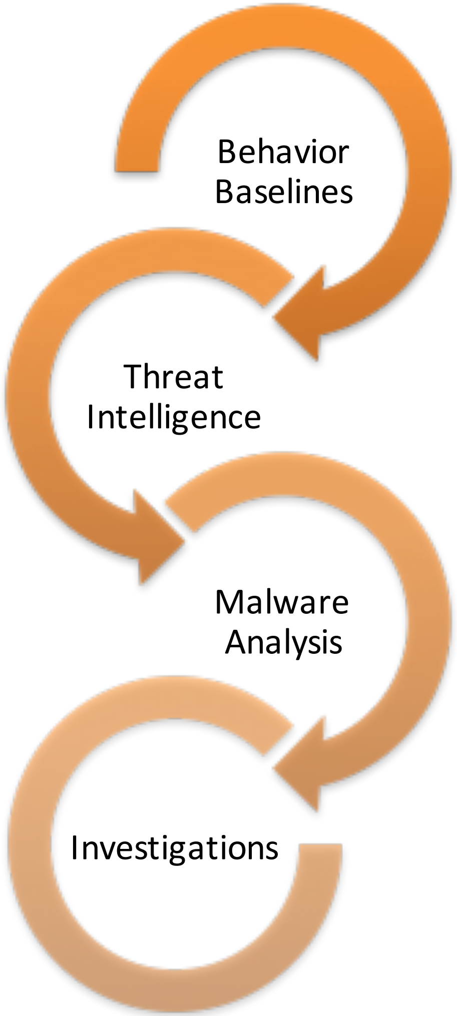
Why “Hunting at the endpoint”?

- Active hunting vs. passive alerting
- Search for adversaries without explicit warnings
- BYO Breach Notifications
- Reduce “Dwell Time”
- Control the messaging and response (First to know)
- Effective “off network”

How do you hunt for threats?

- Add Endpoint visibility
- Utilize the tools you have
  - SEIM/Splunk
  - Palo Alto Wildfire / FireEye
  - IDS/IPS/HIDS
  - Centralized A/V
- Find “context” in every alert
- Customize alerts for your environment

Hunting Methodology



Behavioral Baseline
Looking at Operating System activity to discover potential security incidents

Threat Intelligence
Determining if existing activity matches “known bad” indicators

Malware Analysis
Take every executed application within the enterprise and determining if the binary shows any potential high-risk behaviors

Investigations
All suspicious activities are put into the SLAIT investigation framework to determine potential impact to the client

Let's talk tech…

○ Endpoint Detection & Response

TANIUM™

Guidance® SOFTWARE The World Leader in Digital Investigations™

RESOLUTION1 SECURITY

FireEye®

CROWDSTRIKE

CARBON BLACK ARM YOUR ENDPOINTS

○ Advanced Prevention

CYLANCE

paloalto NETWORKS

CISCO™

cybereason

SOPHOS

○ Network

paloalto NETWORKS

FireEye®

SOPHOS

splunk®>

RSA®

CISCO™

○ Open Source

GRR RAPID RESPONSE

cuckoo

Windows Sysinternals

F.I.D.O. Fully Integrated Defense Operation

Top 10 places to look for Badness

- Processes
- Persistence
- User Account Behavior
- IP/Domain connections
- Admin Tool or Exfiltration files
- Geography of network connections
- Network Activity/Volume
- AV Logs
- Driver Stack
- Advance Malware logs

Bringing it home

- Figure out what's normal in your environment and build anomaly alerting – add context
- Start with tracking down alerts or events you already have – integrate threat intel
- Attacks usually start with endpoints
- Be proactive! Don't wait for someone else to notify you of a compromise - reduce "threat persistence / dwell time" window
- Integrate with defensible security program

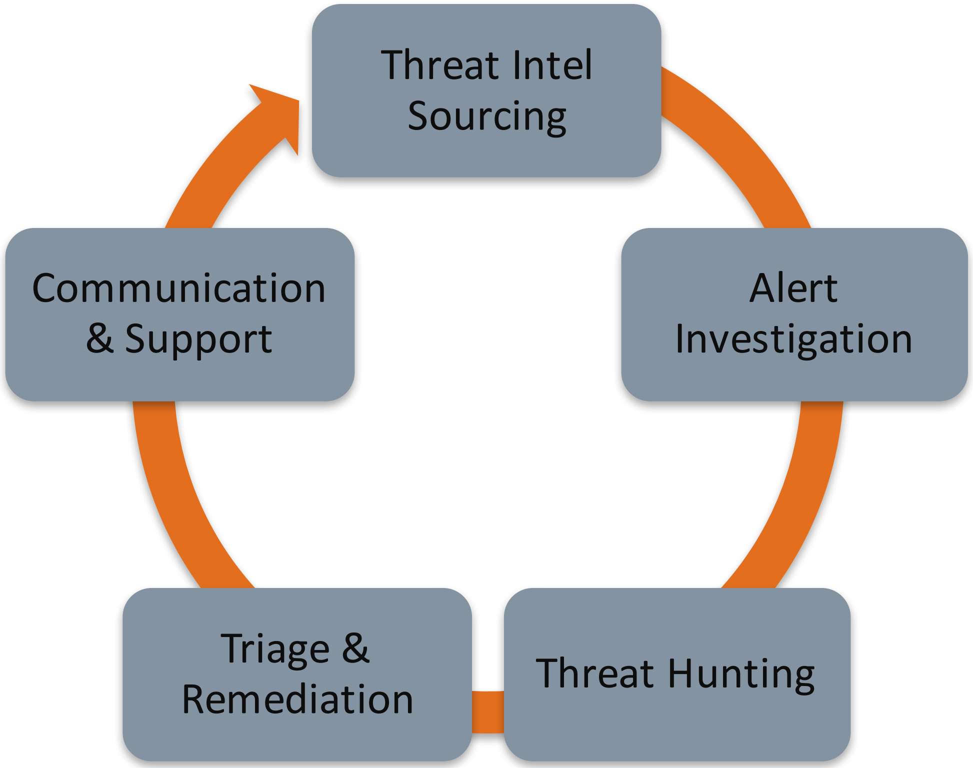
SLAIT ThreatManage

Managed Services – Incident Response

- Provides full management of Client IR and Security Operations solutions from the SLAIT Services team
- ***Includes Active Hunting & Passive Monitoring***
- Shared console and shared threat intelligence
- Scales easily – every dataset adds value to system
- Assumes day-to-day operations with focus on improvement
- Expert team of IR and Threat Hunting staff
- Utilizes “best-of-breed” endpoint technology

Secure, specialized, scalable

- ➢ Discover & hunt
- ➢ Detect & alert
- ➢ Volatile collection & analysis
- ➢ Stop, Triage, Destroy & Recover



Threat Intel Sourcing

Alert Investigation

Threat Hunting

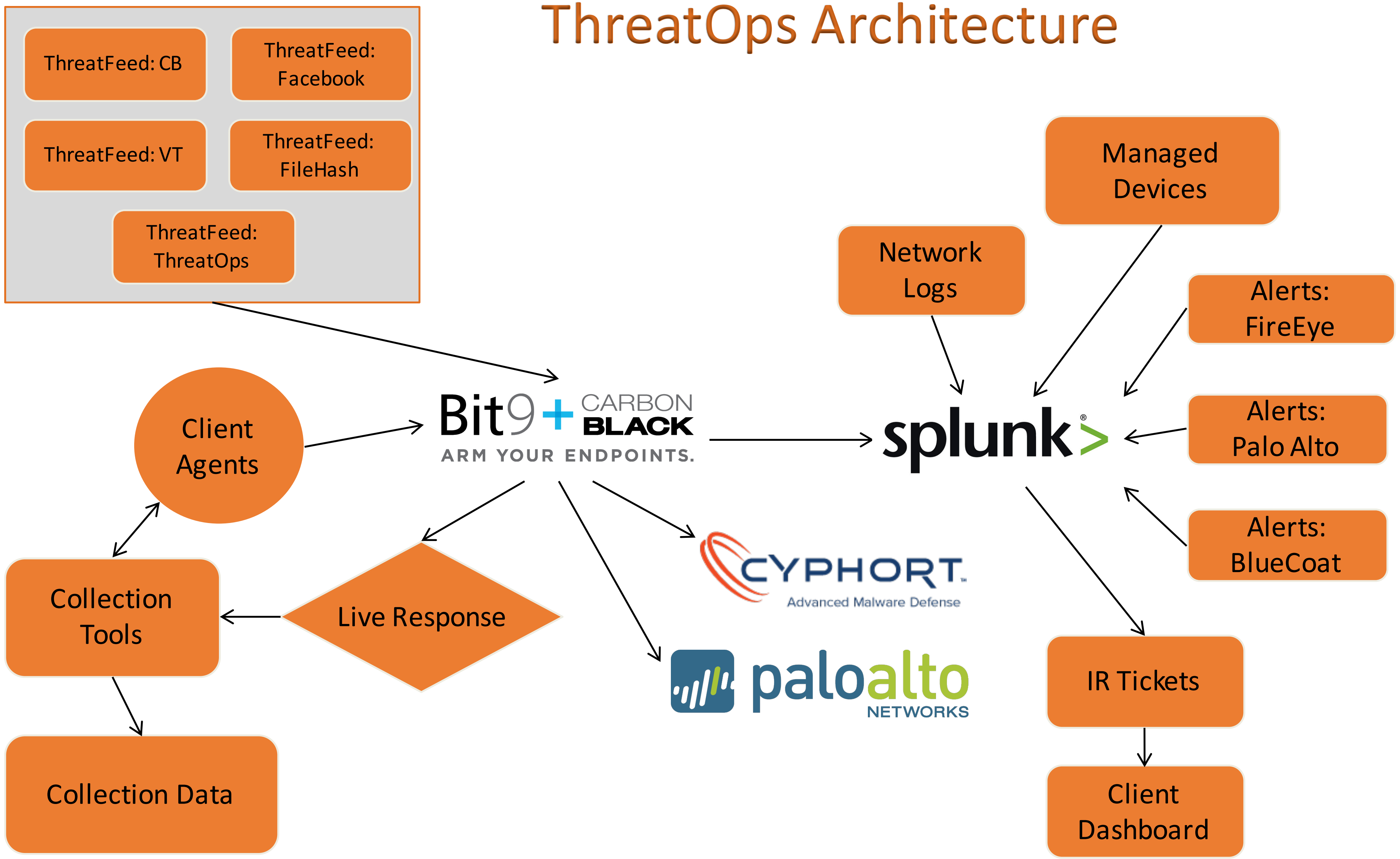
Triage & Remediation

Communication & Support

Let SLAIT assume the complexity, difficulty, and risk of an enterprise-level threat operations while providing advanced threat intelligence & expertise

True IR-as-a-Service

ThreatOps Architecture



Questions?

Arnold.bell@slaitconsulting.com