RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

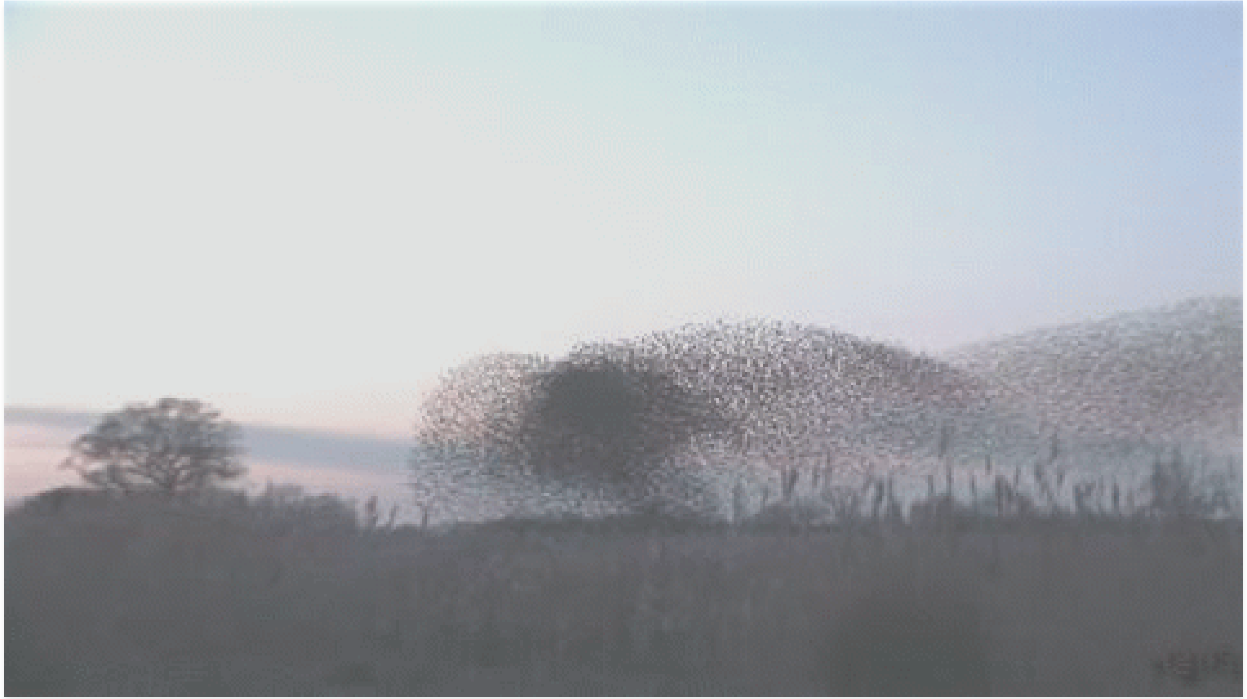
SESSION ID: MLN-R02

EVOLUTION OF AI BOTS FOR REAL-TIME ADAPTIVE SECURITY

Thomas Caldwell

Senior Director Engineering
Webroot
Twitter: @cybersdtom

Swarms

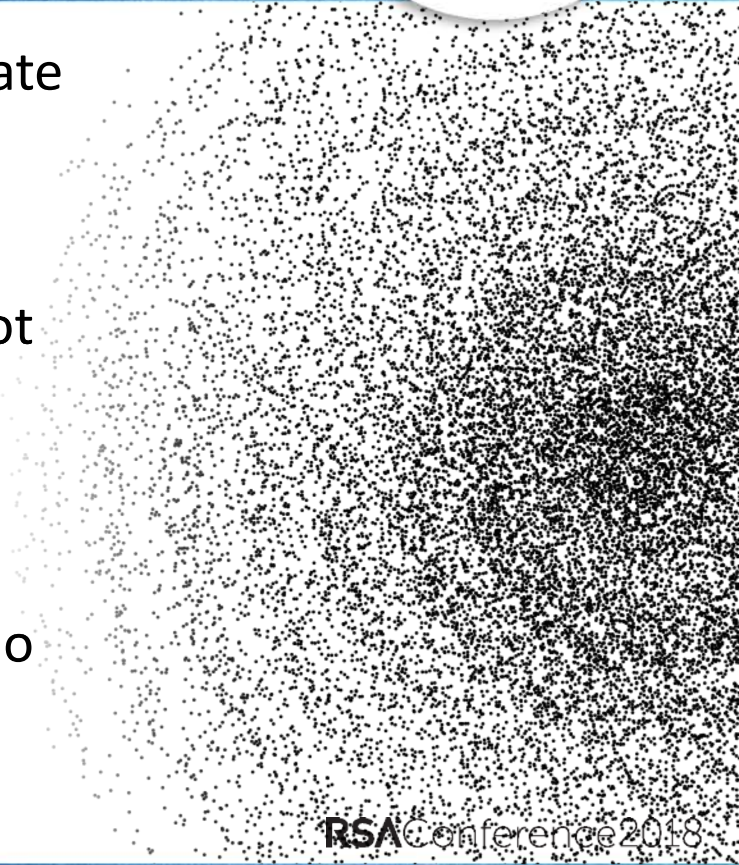


BotNets – The Dark Side

- **2018 could be the year we see the first battle of the AI bots…**
- **Cyber-Criminals build systems that can 'learn' and adapt to defenses…**
  - Nachi Worm – RPC vulnerability, Blaster removal and installed patches
  - Mirai - a zombie malware strain that enslaved "Internet of Things" (IoT)
  - Reaper and IoTroop - computer worms; built to spread automatically, still to be unleashed…
  - Artificial intelligence researchers warn re: internet-connected robots, with hundreds calling on governments to ban weaponized robots.
- **Bots are becoming one of the fastest growing trends with intelligent reasoning, messaging and conversational interfaces**

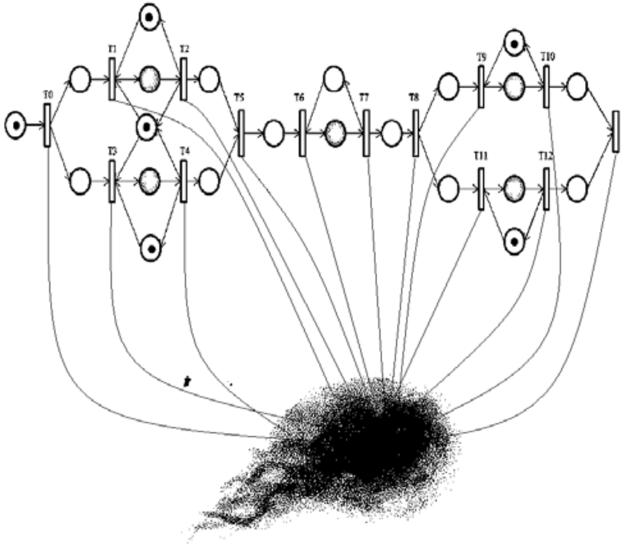
Distributed BotNet Swarming

- AI-Bots acting independently can’t coordinate
- Require Command and Control from a centralized source
- Individual decisions are not coordinated, not cooperative, and don’t result in consensus
- AI-Bots need to interact so consensus is an emergent property
- This is an example of the fusion problem. No fusion, no consensus.



AI-Bot Swarming

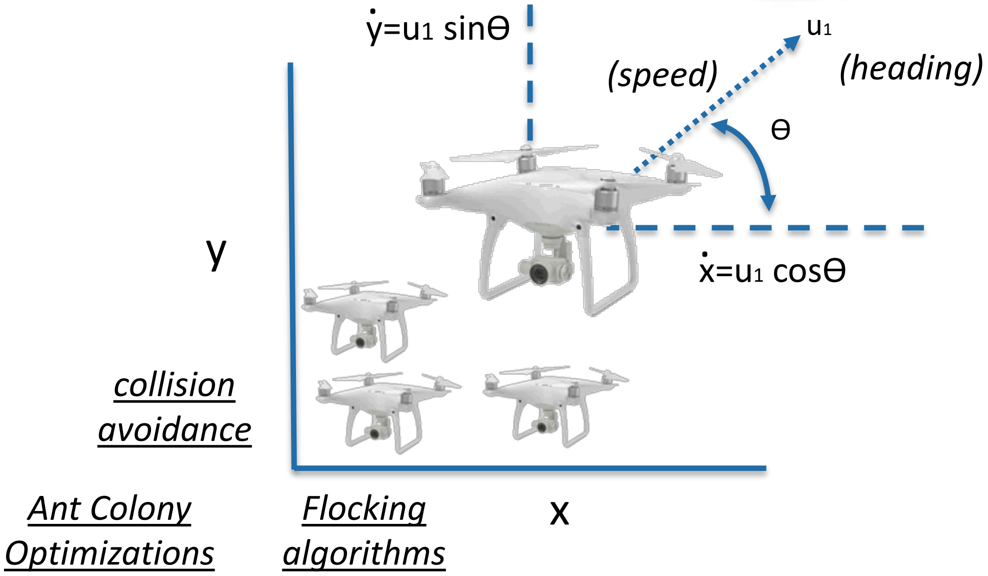
- The AI-BotNet Swarm is a network facilitating Communication, Collaboration, Cooperation, and Consensus
- Cognitive Contextual Awareness
- Suspicious patterns of activity and behaviors detected through ML models
- Determines whether an intrusion is beginning, present, active, or not.
- Replaces legacy Rule-Based system



Infections spread faster than humans can stop them

Swarming Algorithms: The Next Frontier

- Vector = spatial heading and velocity of robots
- Swarms: Collective, Collaborative, Cooperative
- Can Vectors represent cognitive behaviors and discovered opinions?
- Could Blockchain be used for de-centralized sharing and voting in swarms?



collision avoidance

Ant Colony Optimizations

Flocking algorithms

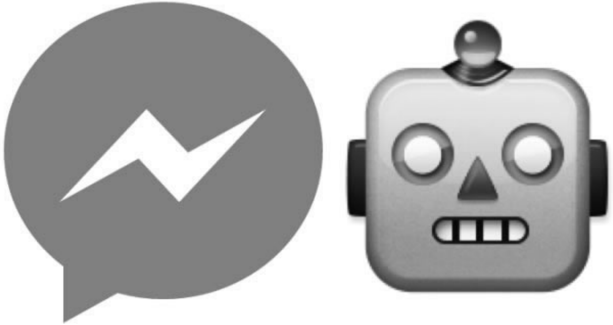
Today's robot Swarming Algorithms are focused on physical spatial aspects of swarming

What is an AI-Bot?

- **AI-Bot Capabilities**
  - Machine Learning
  - Cyber Intelligence
  - Behavioral Analysis
  - Ontology
  - Understands Entity State (Posture)
  - Orchestration and Deception Tactics
- **Reactive AI-Bots**
- **Reasoning AI-Bots**

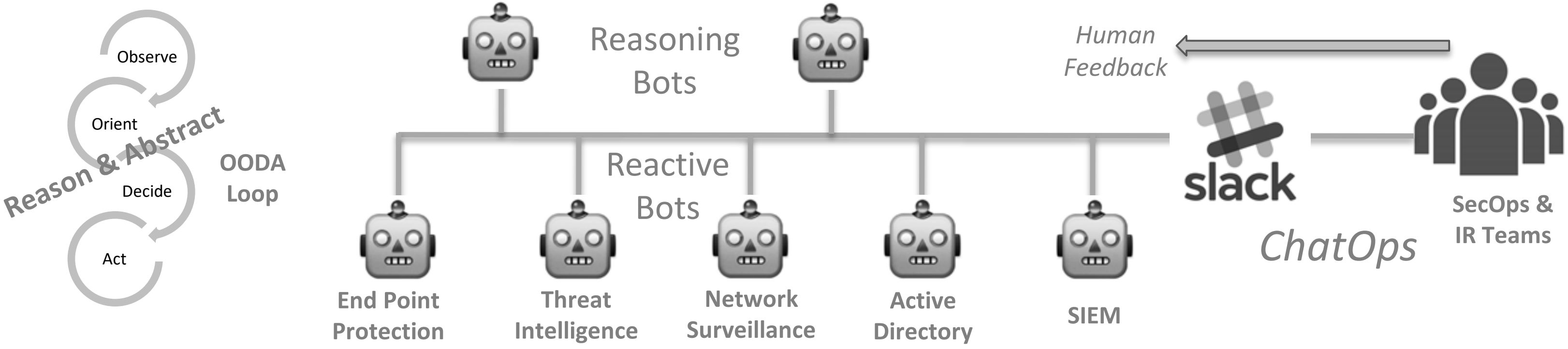
ChatOps: Talk to your Software!

- Imagine if “Alexa” is the talking knowledge base on your 3am Incident Response calls!!
- Enable Increased Accuracy:
  - Type 1 Error - False Positive
  - Type 2 Error - False Negative
  - “Active Learning” Machine Learning asks for help
- Unifies remotely distributed teams
- Streamlined collaboration
- Faster remediation times
- Operational efficiencies
- Underlying AI-Bots “Intelligently Automate”



AI-Bot Specialists

- Specialists required to build house: Electricians, Plumbers, Framers, Roofers…
- Organized into squads (e.g. Navy Seal team) or police organizations
- AI-Bot tools: Machine Learning, APIs to Threat Intelligence, Command & Control, Cooperative Communication, Dialog with Human Experts
- AI-Bots can use OODA loops for Contextualization (Observe, Orient, ***Understand***, Decide, Act)



AI-Bot Demo

ChatOps: Security Automation

Lifecycle of an Alert Automation:

1. Your monitoring system notices something suspicious
2. A bot sends the employee a message in Slack:
3. “**Did you do this $thing?**” (2-factor auth)
4. Employee confirms – Alert resolved
5. Employee denies or does not answer – escalate the Alert!
6. If alert requires action, contact employee & investigate

Automation Example 2:

1. Alice’s ssh key has been stolen
2. Attacker logs into **supportserver01**, runs ***flurb-export***
3. Monitoring system alerts Bot and asks Alice:
4. **“Hi there, I see you ran a sensitive command, Please acknowledge”**
5. The attacker cannot verify the message without Alice’s phone – Alert escalates to Security Team
6. The security team takes action to disable Alice’s accounts globally

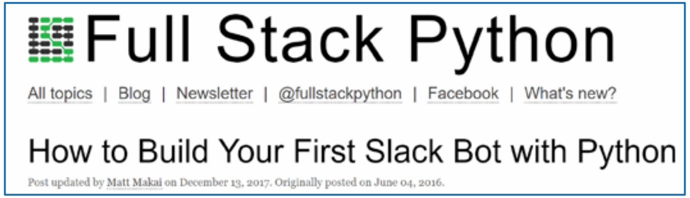
Source: Distributed Security Alerting, Ryan Huber, 2016

How to Implement your own ChatOps

1. Set up a Slack Chat Room

2. Set up integration between Slack and Python apps:
   - Create a Webhook in Slack for simple posting
   - Create a “Slack App” for reading/writing to Slack chat room

3. Many open source Python examples for posting/reading in Slack Chat Rooms



Full Stack Python

All topics | Blog | Newsletter | @fullstackpython | Facebook | What's new?

How to Build Your First Slack Bot with Python

Post updated by Matt Makai on December 13, 2017. Originally posted on June 04, 2016.

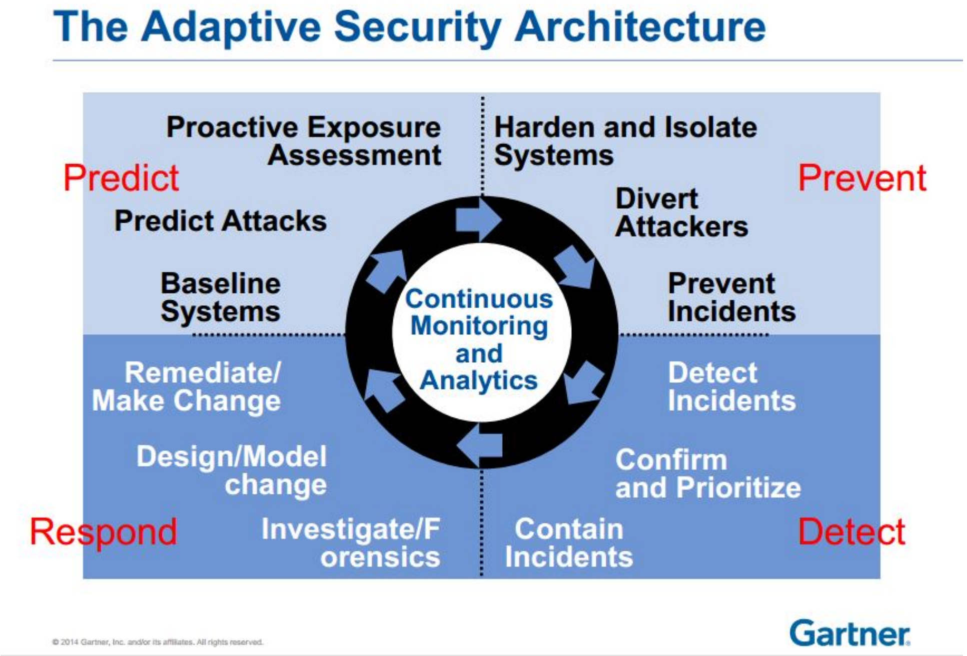
1. For Alexa Skill, modify Python Color Expert Example, add slack hooks

2. Use your Python apps as “specialists” to integrate your security applications via API with Slack

How do Bots fit into Adaptive Security?

- Traditional "prevent and detect" obsolete
- From "Incident Response" to "Continuous Response"
- Humans work on more complex incidents
- Enormous volume of data for advanced analytics
- By 2020, 40% of large organizations will have a "Security Intelligence Warehouse"
- Machine Learning will drive Adaptive Security

Source: Gartner



The Adaptive Security Architecture

Predict

Proactive Exposure Assessment

Predict Attacks

Baseline Systems

Prevent

Harden and Isolate Systems

Divert Attackers

Prevent Incidents

Continuous Monitoring and Analytics

Respond

Remediate/ Make Change

Design/Model change

Investigate/F orensics

Detect

Detect Incidents

Confirm and Prioritize

Contain Incidents

Gartner

Cyber Threat Intelligence (CTI)

- Distributed Intelligence Model
- Privacy and Legal implications (GDPR)
- Actionable-Contextualized
- Consumable via APIs
- Visibility on Bad Actors/Victims
- For ML it is all about the data!

DRM
People
Strategic
Assets
Tactical
Devices
Intelligence
Data
Operational
Process
Information

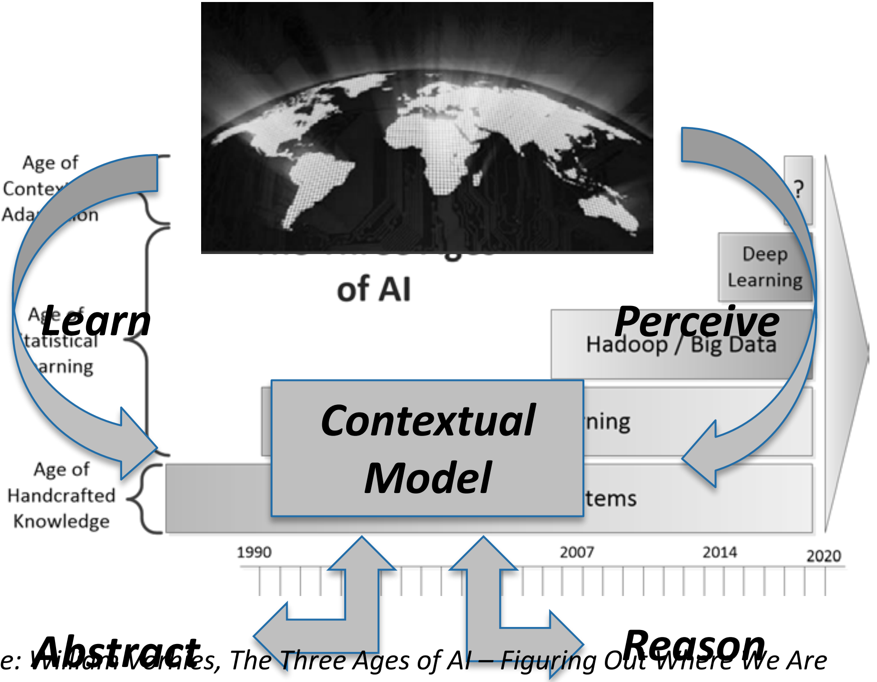
Adaptive Security Platform + CTI + AI/ML = Adaptive Response

AI drives Adaptive Security

- Artificial Intelligence:
  - Deep understanding of the context of the prediction (semantics)
  - Causal analysis of what was detected
  - Recommendation of best response in real-time
  - Digital visibility into bad actors

Growth of AI is on Fire!

- AI began in 1980’s stalled at End of Cold War
- Darpa: Three Ages of AI
  - Age of Handcrafted Knowledge
  - Age of Statistical Learning
  - Age of Contextual Adaptation
- Deep Learning pioneered as neural networks
- Back then… No ML Tools, Cloud, Lots of Data
- **<u>Massive AI Adoption Today</u>:**
  - Large Community & Culture for ML
  - Shared Methodologies of ML Tools
  - Knowledge in ML reaches critical mass



Source: William Vorhies, The Three Ages of AI – Figuring Out Where We Are

Darpa: 3^{rd} Wave of AI

Applying Bots to Cyber Security

- Leverage Adaptive Security combining AI/ML/CTI in your security stack – Come up the learning curve on AI and ML
- Identify specialized AI-Bots for false positive filtering and other post-ML automation and recommendations
- Evaluate ChatOps, realize the efficiency, create intelligent integrated AI-Bots to automate background tasks
- Look to the near future where **swarms** of AI-Bots **Collaborate**, **Coordinate** and connect with humans to reach the right decision in real-time (**Consensus**)

Resources

- How to get started with building your own Alexa ChatOps:
  - AWS Lambda: create function using blueprint “alexa-skills-kit-color-expert-python”
  - AWS Alexa Skills: Follow color picker instructions
  - Slack: create chat room and a webhook, embed python REST call using your webhook to slack
- “Google releases machine learning crash course, other educational AI resources” https://9to5google.com/2018/02/28/learn-with-google-ai-machine-learning-course/
- “Building Slack Apps” https://api.slack.com/slack-apps
- Topbots: https://www.topbots.com/
- https://www.darpa.mil/about-us/darpa-perspective-on-ai

Note: Appreciation to my colleague Dr. William Wright who has partnered with me in assembling this content and presentation.

QUESTIONS?

Tom Caldwell, Sr. Director Engineering, Webroot

tcaldwell@webroot.com

Twitter: @cybersdtom

LinkedIn: https://www.linkedin.com/in/tcaldwell/