WitFoo Precinct Roadmap

Charles Herring
Co-Founder, CTO

Disclaimer

Product development at WitFoo is a programmatic learning experience with the mission of solving the craft challenges of SECOPS. Lessons prompt additional work, changes in features and changes in philosophies that will alter this roadmap.

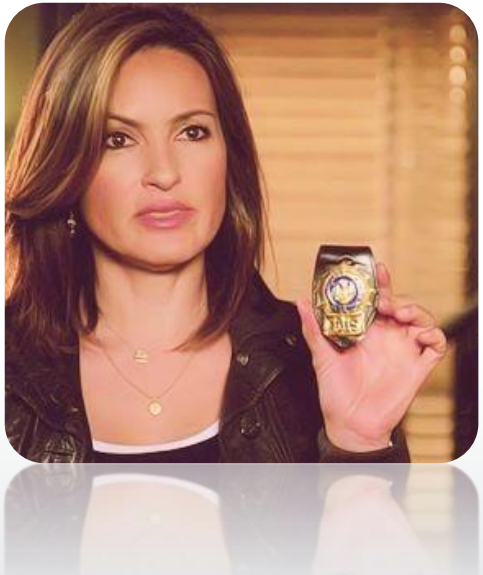
- These features are not guaranteed. Changes may occur.
- Timelines are not guaranteed. Changes may occur.

Development Timelines

	6.1	6.2	6.3
Investigative Engine	Partition Size Control	Streaming Processing, Campaigns, MO Editor	Machine Learning, Retro, MITRE ATT@CK
Streamer	Lead Processing		
Dispatch	Initial Release		
Aggregator	Initial Release	Campaigns	
Data Cluster	Datacenter Aware	Cassandra 4.0	
Artifacts		Streaming Data API	Custom Dashboards
Reports		Multi-Framework	Custom Dashboards, Emails
Assets		Initial Release	Custom Dashboards
Incidents	DoD Categories	• Campaigns • Attribute Filtering • Import • MITRE ATT@CK	• “Incident Viewer” Standalone • Modus Operandi Editor
Platform	Common Criteria	• i18n (multi-language) • Light Mode UI	• Health Reports • Configurable Modules • Custom Resource Allocation • Rolling Updates

Precinct 6.1 (Golden Benson) Highlights

- Simple, Sustainable API Integrations
- RBAC Response Actions
- Faster User Experience & Processing
- Federated Data & Workflows

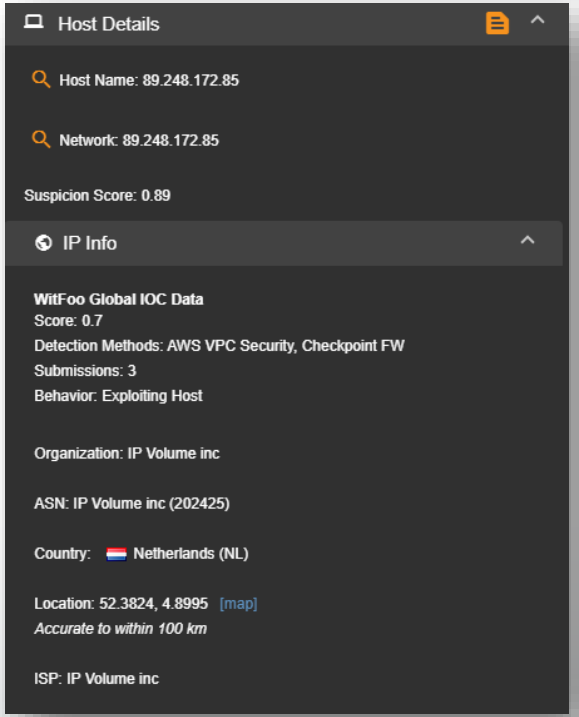


Streamer 2.0

- Lead Rule matches on Artifact
- Critical Security Control on Artifact
- Sending Product on Artifact
- Reduced IOPS and Cassandra load
- Streaming Lead Analysis (vs Micro-batch)
- Streamlined Streamer Code
- Leveraging Scala 2.13 improvements

Global Indicator of Compromise Feed

- Anonymous Customer Submission
- Includes detection method/product
- Includes nefarious behavior types
- Includes suspicion score
- Retro-analysis of IOC hits
- Geo-IP Resolution
- ASN Resolution

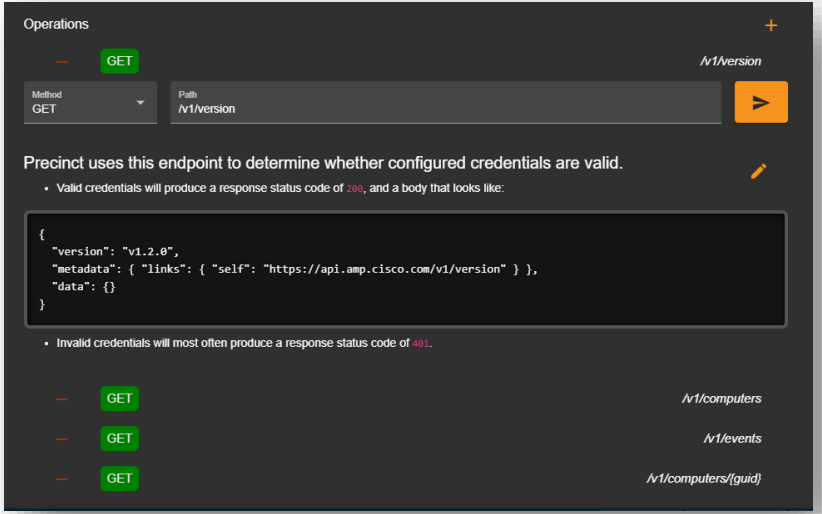


Dispatch : Codeless Integrations

- New Integrations delivered by meta signatures (vs Release)
- RBAC configurable actions
- Broader API data available to Precinct
- Quicker turn around of new API integrations & existing support
- Triggered/automatic actions
- Framework for advanced response workflows
- API Definitions based on OpenAPI Specifications
- Customer can import custom definitions (in addition OOTB)

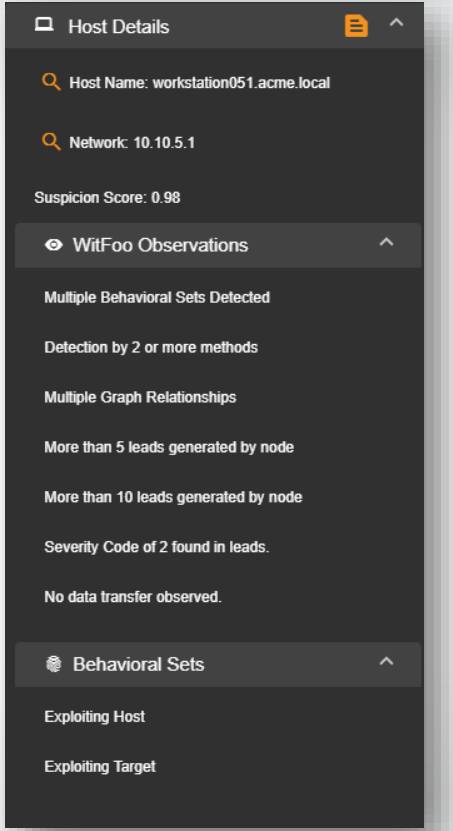
Codeless Integrations

- Import OpenAPI Specification
- Published in WitFoo Library
- Support for REST & SOAP
- Code not required
- Amazon States Language Support
  - Developed by Amazon
  - States-language.net
  - JSON definitions of States Engines
- Custom WitFoo Precinct States Engine



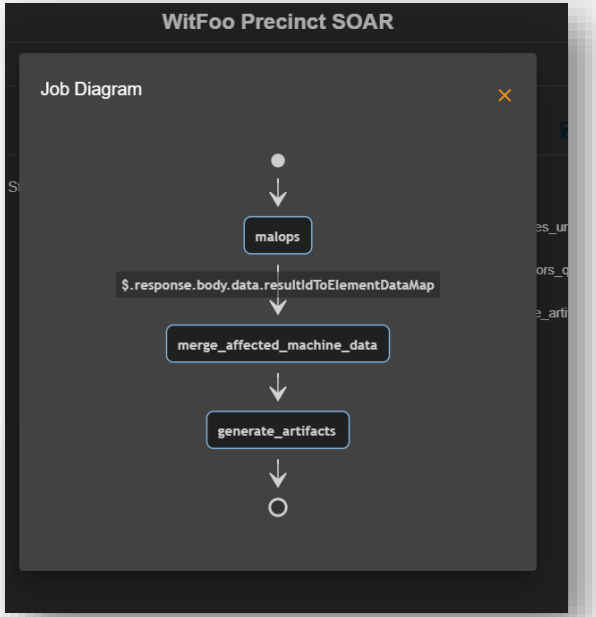
High-level SOAR

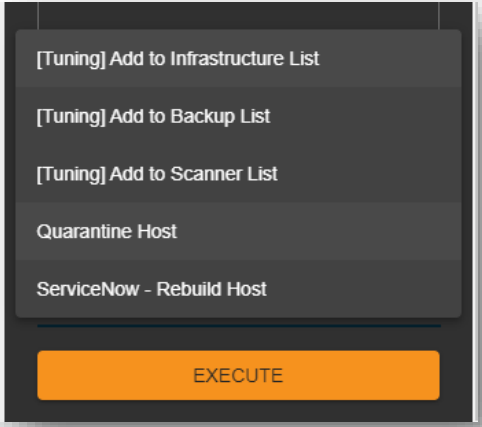
- Unit of Analysis: Incident
  - Context of Attack Type
  - State of all nodes & edges
  - All artifacts available
- Generalized Observations impact suspicion
- Suspicion approaches 1 when
  - Evidence Supports Modus Operandi Progression
  - Sufficient Evidence Exists
- Less Expensive to Maintain v. Linear SOAR
- More accurate than Linear SOAR



Codeless Response Jobs

- Collect External Data into Artifact
- Execute Playbooks
- Code not required
- Amazon States Language Support

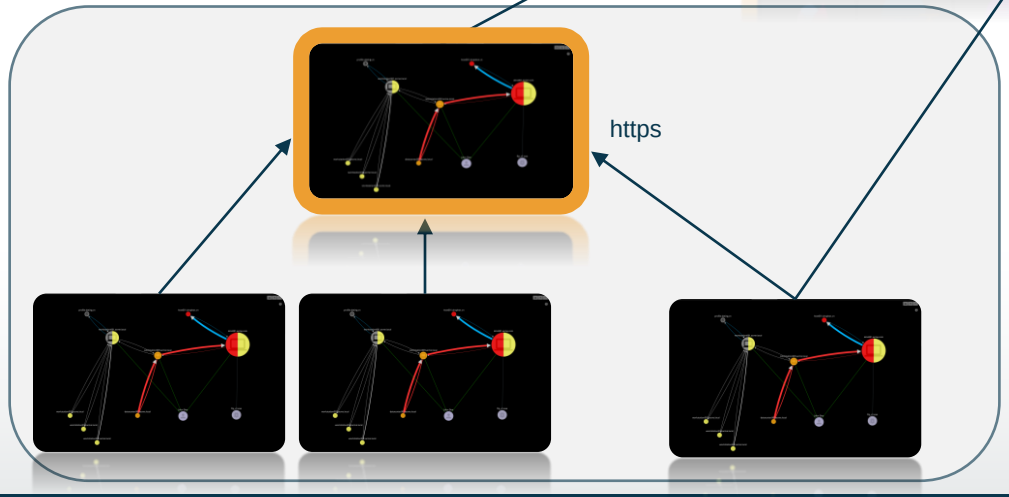




WitFoo Aggregation Mode

- Incidents, Reports, Rules
- Issue Search & SOAR Jobs
- One-way HTTPS Connection
- Queuing for poor Internet
- No limit on aggregators

https



https

Aggregate Reporting

- Cybersecurity Insurers
- Vendor Management
- Ongoing Audit
- Chain-of-Command

Aggregate Operations

- MSSP
- Military SOC
- Community SOC
- M&A
- Report to Law Enforcement

Aggregation

- Agg Node is Server (443/tcp) avoiding Firewall issues
- Agg Node Queues Jobs for Tenants
- Tenants Queue Results for Agg Nodes
- Result Types
  - Incidents
  - Reports
  - Search Results
- Job Types
  - Search Jobs
  - Dispatch Labs (Response Actions)
  - Lead Rules (Detection Signatures)
- Use-cases
  - MSSP / M&A / Subsidiaries / Military Chain-of-Command
  - Law Enforcement Reporting
  - Cybersecurity Insurers

Precinct 6.2 (Platinum Benson) Highlights

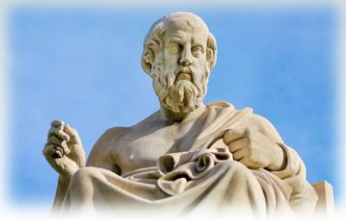
- Incidents and Artifacts Searchable by MITRE ATT@CK
- Compliance Reports against NIST and ISO Frameworks
- Autonomous Asset Searching
- Incidents Grouped into Campaigns (local and aggregator)
- Incident UI enhancements
- I18n localization (multi-language)
- “Light Mode” UI
- Cassandra 4.0 (speed & reduced IOPS)
- Streaming (real-time) Artifact filtering

MITRE

NIST

ISO

Platonic Engine



- Infinite Horizontal Processing (vs. Vertical)
- Built on Kafka and Scala for extensibility
- Fully streaming processing (vs. Micro-batch)
- Reduced IOPS and Cassandra load (better search experience)
- Framework for Machine Learning
- Enhanced Graph Relationship Handling

Scala API

- Extreme Improvement on Artifact Searches through threading
- Ability to filter artifacts as they are received
- Improve User Experience through Websockets

Precinct 6.3 (Titanium Benson) Highlights

- Machine Learning on Node & Edge Baselines
- Custom Dashboards
- Emailed PDF Reports
- “Incident Viewer” Standalone Application
- Deployment/Cluster Health Reports
- UI for tweaking/tuning modules and resources
- Rolling upgrades at module level
- UI Editor for Modus Operandi
- UI Editor for Incident Observations

Library 2.0

- Library 2.0 – Global Data Service
  - IOC Attribution Comments
  - Tool Effectiveness for purchasing decisions
  - Technology Partners monitor their product health in customer networks
  - Reselling Partners support infrastructure health
  - Community Collaboration & Training

	6.1	6.2	6.3
Investigative Engine	Partition Size Control	Streaming Processing, Campaigns, MO Editor	Machine Learning, Retro, MITRE ATT@CK
Streamer	Lead Processing		
Dispatch	Initial Release		
Aggregator	Initial Release	Campaigns	
Data Cluster	Datacenter Aware	Cassandra 4.0	
Artifacts		Streaming Data API	Custom Dashboards
Reports		Multi-Framework	Custom Dashboards, Emails
Assets		Initial Release	Custom Dashboards
Incidents	DoD Categories	• Campaigns • Attribute Filtering • Import • MITRE ATT@CK	• “Incident Viewer” Standalone • Modus Operandi Editor
Platform	Common Criteria	• i18n (multi-language) • Light Mode UI	• Health Reports • Configurable Modules • Custom Resource Allocation • Rolling Updates


witfoo
Security, Leveled Up.