LegalSEC SUMMIT 2017

THREAT AUTOMATION

Curtis Davis – Fenwick & West LLP

Chris Fauerbach – Perch Security

WHAT IS SECURITY AUTOMATION?

Security automation: automatic handling of a task in an information or cyber security system

- You can automate multiple tasks within a single product or system, but…
  - Security orchestration is required in order to automate *many* tasks or security processes between *other products, tools, or systems*

WHAT IS SECURITY ORCHESTRATION?

Security orchestration: connecting security tools and integrating dissimilar security systems

- Leverage automation as necessary
- Get more value out of your people, processes, and tools
- Streamline detection, response, and remediation

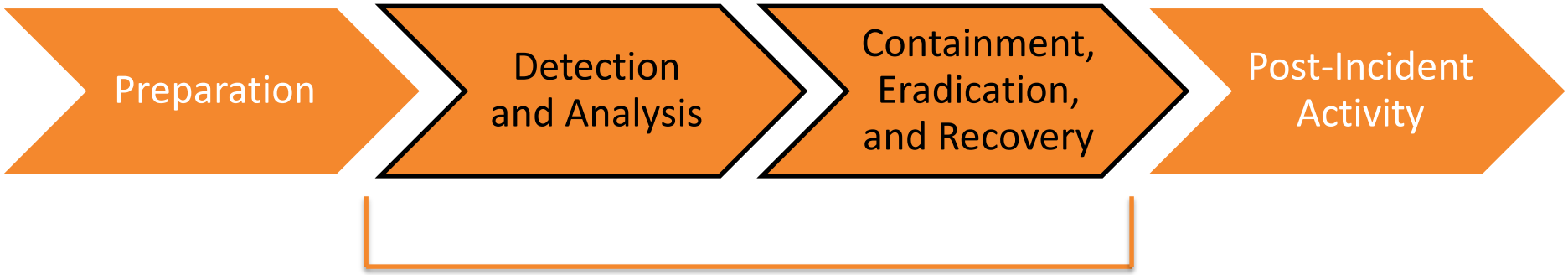
CURRENT CHALLENGES

- Managing multiple tools and processes manually
  - Time-to-response
  - Human error
  - Reactive
- “Best of breed” security systems do not integrate

AUTOMATING SECURITY-RELATED TASKS

- Querying logs
- Provisioning and deprovisioning users
- Malware and phishing investigations
- Vulnerability assessments
- IP scoring
- … and more

INCIDENT RESPONSE PLAN



THREAT INTELLIGENCE

- Maintain up to date intelligence
- High valued intelligence from communities
- Public and Private Sources
  - DHS AIS, Emerging Threats
  - ET Pro, ISAC, ISAO
  - Mailing Lists**
- ***Super Secret Communities*
- Your own intelligence

DETECTING THREAT INTELLIGENCE

- Threat Intelligence Sources
- STIX / TAXII
- Other protocols, custom code, etc
- Intelligence Normalization and Storage
- Install on network sensor/IDS
- Correlate alerts and other events

BIG ARCHITECTURAL COMPONENTS

- Intelligence to Network detection
- On premise, IDS
  - Rules based on intelligence
- Cloud detection engine
  - Things that can't easily be detected in an IDS such as Suricata
- Big data processing and storage
  - Buzz word!
  - It can get big, for sure.

STACK

- ELK (Elasticsearch, Logstash, Kibana)
- Suricata
- Django
- ReactJS

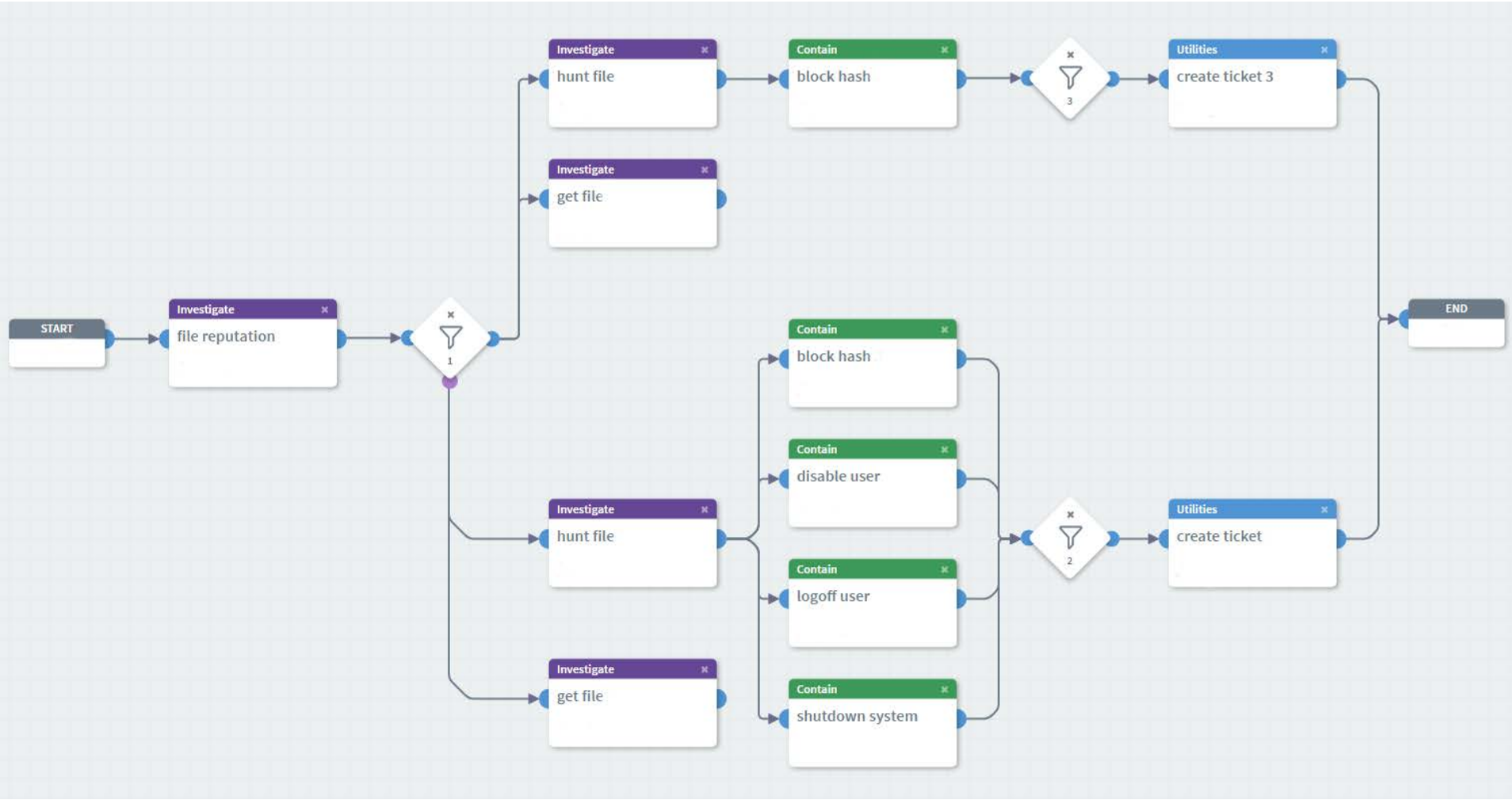
CLOUD

- If scale needs it
- AWS Provides infrastructure and application services
- Compute, data services, auto scaling - *oh my*
- ECS, SQS, ELB, Elastic Beanstalk, Route 53, VPC, ECS

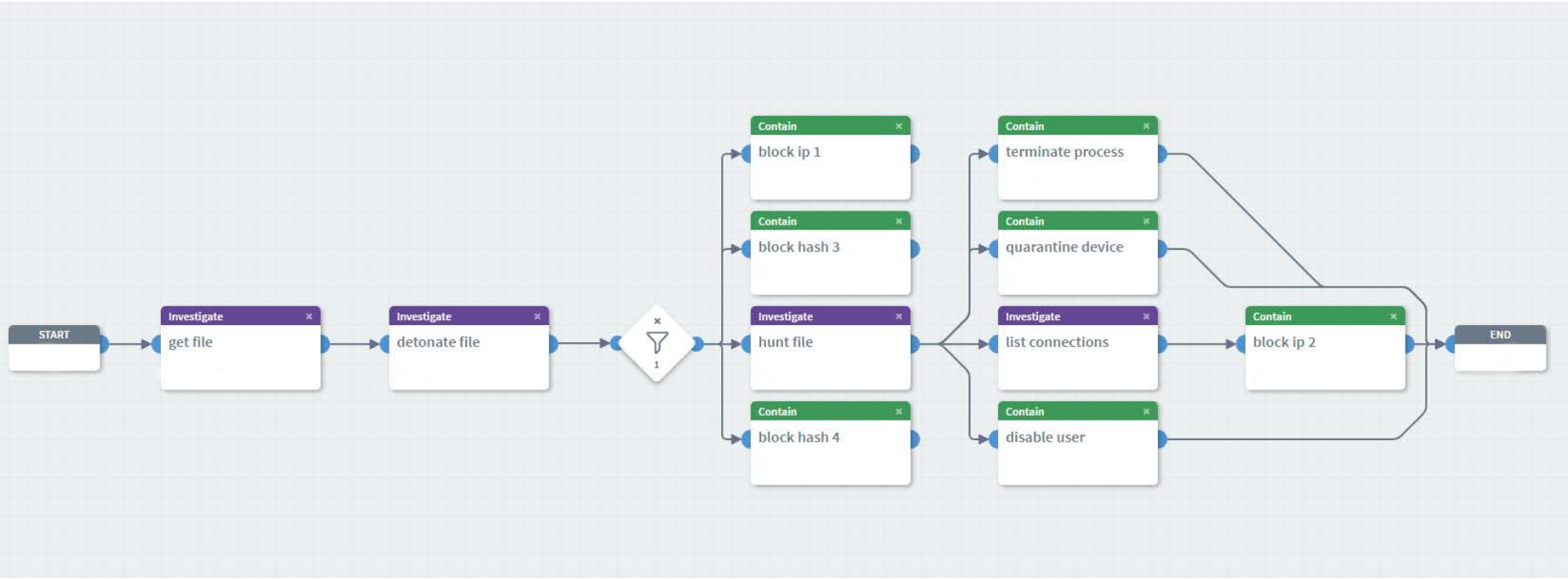
ALERTING

- IDS records flow through to Elasticsearch
- Use Logstash to tag and enhance
  - Geolocation
  - Data cleansing
- Kibana as user interface
  - Dashboards
  - Queries

MALWARE PLAYBOOK



RANSOMWARE PLAYBOOK



POST-INCIDENT ACTIVITY

- Share appropriate incident information with peers and industry
- Reporting requirements
  - Regulatory
  - Law enforcement
  - Legal department
- Lessons learned

LegalSEC SUMMIT 2017

THANK YOU!

Curtis Davis – Fenwick & West LLP
cdavis@fenwick.com

Chris Fauerbach – Perch Security
chris@perchsecurity.com