Tactical Acceleration

https://news.nationalgeographic.com/content/dam/news/photos/000/683/68350.jpg

Doug Burks @dougburks
Crawl Before We Walk

Doug Burks @dougburks
Fundamentals

• Instrumentation
• Collection
• Ingestion
• Augmentation
• Pre-investigation automation

• Investigation
• Post-investigation automation
• Communication
• Meta-Acceleration

Doug Burks @dougburks
Accelerating Instrumentation

Doug Burks @dougburks
Accelerating Instrumentation

- Generate logs
- Network
- Infrastructure
- Endpoints

Doug Burks @dougburks
Instrumentation - Network

- NIDS alerts
- Comprehensive logs:
  - Connection logs
  - DNS logs
  - FTP logs
  - HTTP logs
  - SSL logs

Bonus: full packet capture

Of course, make sure network sensors aren’t dropping packets!

Doug Burks @dougburks
Instrumentation - Infrastructure

- Firewall logs
- Proxy logs
- Other network appliance logs
Instrumentation - Endpoints

• AV/HIDS alerts

• Comprehensive logging:
  – OS
  – Applications
  – Powershell
  – Persistence Mechanisms (Example: Autoruns)
  – Process Auditing (Example: Sysmon)
Instrumentation Automation

• Still rolling network sensors by hand?

• Spending more time being a sysadmin than catching bad guys?
Instrumentation Automation

• Endpoint visibility may require agents

• Can we automate installation/upgrade?
Accelerating Collection

Doug Burks @dougburks
Collection - Speed

• Sending across network?
• Network speed?
• What happens if network goes down?
Collection - Cost
• JSON vs good ole syslog
• JSON is easier to parse
• Syslog more compact
• Beware bandwidth cost

Doug Burks @dougburks
Collection - Cost

• Commercial SIEM may be cost prohibitive and may be limiting your capabilities

• Consider augmenting or replacing with open source to have better capabilities

Doug Burks @dougburks
Accelerating Ingestion

Doug Burks @dougburks
Accelerating Ingestion

• Store those logs in a searchable database

• Example: Logstash → Elasticsearch

• Review your ingestion pipeline for errors, timeouts, delays, failures

• Logstash 6.0 supports Multiple Pipelines
Sidebar: Timestamps

• If timestamps aren’t consistent, this will slow you down
• Ideally, timestamps should be stored in UTC
• Avoids time zone issues
• Also avoids time warp twice a year for daylight savings time
Acceleration via Augmentation

Doug Burks @dougburks
Augmentation: IP addresses

- Reverse DNS lookups
- geoip
- Threat Intel matching
Augmentation: Hostnames

• Threat Intel matching

• Use Frequency Analysis to identify DGAs (Ex: FreqServer)

• Whois - Baby Domains (Ex: DomainStats)

Doug Burks @dougburks
Augmentation: Alerts

• Include the rule that generated the alert at the time the alert was generated

• Include a hyperlink to view the current version of rule

• This can help determine if we’re dealing with a false positive that has already been resolved
Pre-Investigation Automation

Doug Burks @dougburks
Pre-Investigation Automation

• Perform an action automatically before human intervention

• Find that task that you do 10-100 times per day and automate it so you never have to do it again

• Time savings add up quickly

• Example: Create an ElastAlert rule that searches for phishing domains similar to Top Sites and sends email (and maybe that email generates a ticket in some other system)
Accelerating Investigation

Doug Burks @dougburks
Accelerating Investigation

• Goal: Identify Outliers with Group By

• Example: Show me a list of all DNS lookups on the network, grouped by FQDN

• Behavior like beaconing may bubble up to the top
Accelerating Investigation

• Goal: Long Tail Analysis

• Example: Show me a list of all processes executed on all Windows boxes, grouped by process name, but let’s start looking at the least frequent occurrence
Accelerating Investigation

• Goal: Streamline workflow

• Pre-build queries so that they’re just a click away

• Example: Save a query that shows downloaded Windows EXEs and grouped by the site they were downloaded from

Doug Burks @dougburks
Accelerating Investigation

• Goal: Reduce friction

• Pivot between different data types and different interfaces (bonus: pivot to pcap!)

• Never underestimate the value of a hyperlink (ex: click right into GRR for endpoint memory analysis)
Accelerating Investigation

• Goal: Define a subset of events which MUST be reviewed on a daily basis

• How many IDS alerts in your queue today vs how many can you actually handle in a day?

• Tune mercilessly until you reach that goal

• Keep non-essential alerts in a separate queue for additional analysis

Doug Burks @dougburks
Accelerating Investigation

• Goal: Search all the databases!

• Example: Elasticsearch 6.0 includes Cross Cluster Search
Accelerating Investigation

• Goal: Avoid slow rodents!

• Example: Kibana 6.0 includes improved keyboard navigation!
Post-Investigation Automation

Doug Burks @dougburks
Post-Investigation Automation

• Leaves you with more mental energy to do more advanced tasks

• CLI FTW
Acceleration via Communication

• Share information

• Makes your team better and therefore faster

• Sharing outside organization may return valuable intel

Doug Burks @dougburks
Meta Acceleration

• What percentage of your day is spent on meetings,administrivia, and water cooler talk?

• What percentage of your day are you finding evil?

• What percentage of that time is passively reacting to IDS alerts vs proactively hunting?
Time

• Map out YOUR ideal day and break out by percentage different tasks:
  – 30% review IDS alerts
  – 30% proactive hunting
  – 20% automate
  – 10% administrative

• Try to adhere to schedule on daily basis and build muscle memory

Doug Burks @dougburks
Accelerate your wheels, don’t spin your wheels

- Don’t mistake the urgent for the important (see Stephen Covey)
- Go for a walk
Accelerate your wheels, avoid the ludic loop

Doug Burks @dougburks
Accelerate your wheels, don’t reinvent the wheel

Doug Burks @dougburks
Accelerate your wheels, don’t reinvent the wheel

- Sigma - “Generic Signature Format for SIEM Systems”

- “Sigma is for log files what Snort is for network traffic and YARA is for files”

- https://github.com/Neo23x0/sigma
Nitrous

GOOD HEAVENS, THIS GASEOUS COMPOUND

SURE AUGMENTS MY AUTOMOBILE’S PERFORMANCE!

Doug Burks @dougburks
Learn Something New Every Day

• Your brain is a muscle
• It must be exercised
• Scripting, protocols, forensics, reverse engineering

Obligatory Machine Learning Reference

• Take advantage of it where it makes sense

Doug Burks @dougburks
Forest or Trees?

Doug Burks @dougburks
What can you do today to make yourself faster tomorrow?
What can you do today to make your organization faster tomorrow?
What can you do today to make our community faster tomorrow?