sqrrl

Securely explore your data

IT'S HUNTING SEASON!

Tips for getting started with proactive detection

ABOUT ME

Security Architect at Sqrrl. Research areas include threat intelligence, security analytics and the art & science of hunting.

15 years of detection & response experience in government, research, educational and corporate arenas.

A founding member of a Fortune 5's CIRT. Spent 5 years helping to build a global detection & response capability (500+ sensors, 5PB PCAP, 4TB logs/day).

WHAT IS “HUNTING”?

The collective name for any manual or machine-assisted techniques used to detect security incidents.

HOW TO BUILD A HUNT CAPABILITY

Embrace Big Data

Get Your Data Science On

Always Have a Good Strategy

Ask Lots of Questions

Pivot… Then Pivot Again

Automation is the Key to Continuous Improvement

sqrrl

Securely explore your data

TIP #1: EMBRACE BIG DATA

THE THREE DATA DOMAINS

Keep as much as you can comfortably store

Network

- Authentication
- Session data
- Proxy Logs
- File transfers
- DNS resolution

Host

- Authentication
- Audit logs
- Process creation

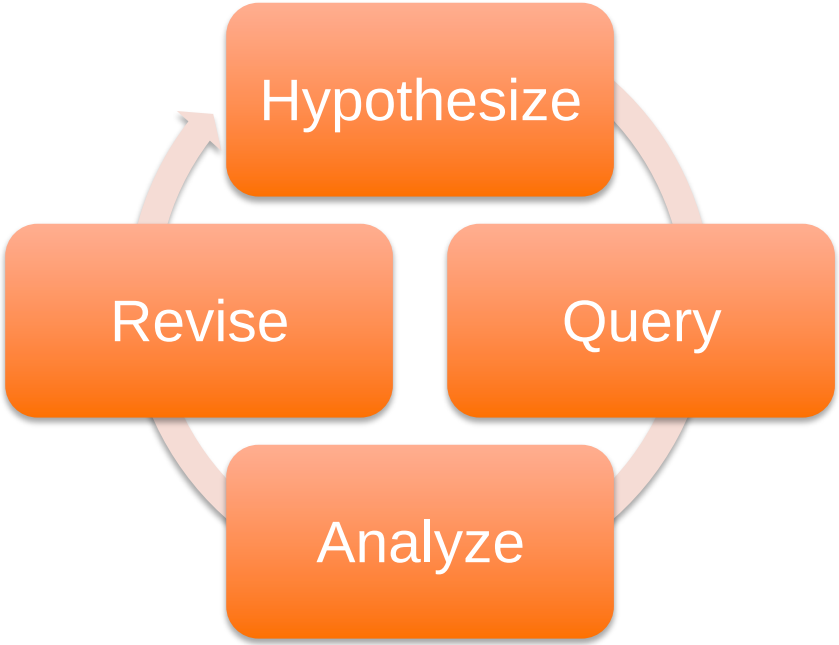
Application

- Authentication
- DB queries
- Audit & transaction logs
- Security alerts

THE HUNTING PROCESS

Successful hunting requires many iterations through this cycle.

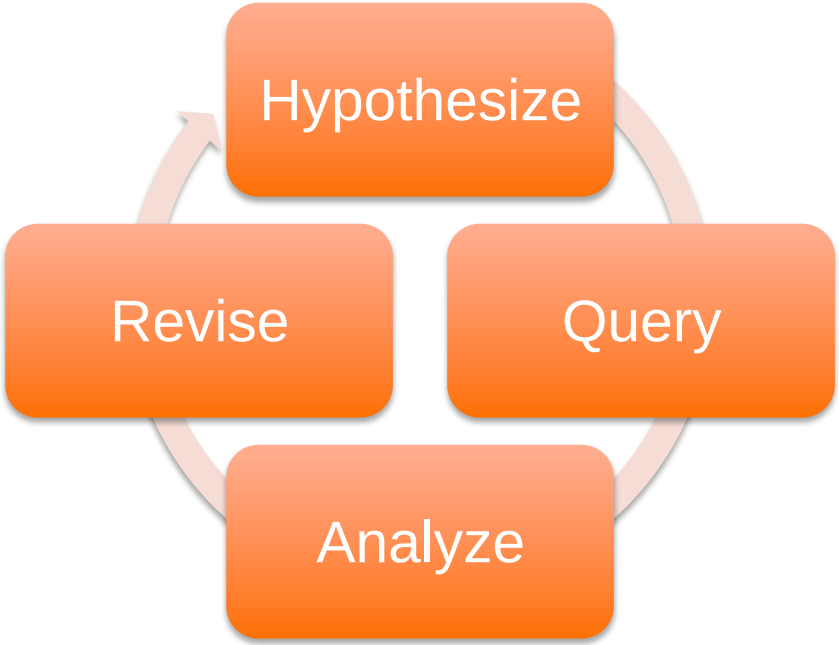
The faster your analysts get through this loop, the better.



Apache's Hadoop platform offers fast search and processing of huge amounts of data.

You will still need tooling on top of whatever platform you choose.

THE HUNTING PROCESS



Keep as much data as you can comfortably store…

…and work with!

sqrrl

Securely explore your data

TIP #2: GET YOUR DATA SCIENCE ON

WHEN'S THE LAST TIME YOU HEARD…?

"It is a Best Practice to review all your logs each day."

WHEN'S THE LAST TIME YOU HEARD…?

"It is a Best Practice to review all your logs each day."

BEST-ER PRACTICE

Parsing & Normalization

Data Deduplication & Reduction

Machine-Assisted Analysis

MACHINE-ASSISTED ANALYSIS

Computers

Bad at context and understanding

Good at repetition and drudgery

Algorithms work cheap!

People

Contextual analysis experts who love patterns

Posses curiosity & intuition

Business knowledge

Empowered Analysts

Process massive amounts of data

Agile investigations

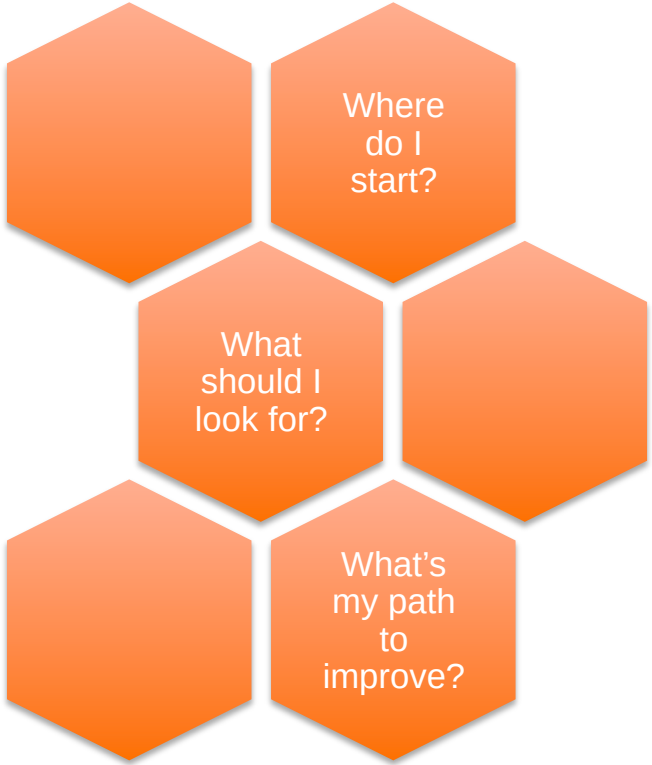
Quickly turn questions into insight

sqrrl

Securely explore your data

TIP #3: ALWAYS HAVE A GOOD STRATEGY

STRATEGY ENABLES RESULTS



Your strategy determines the quality of your results.

Choose a strategy that supports your detection goals.

Don't underestimate the importance of good planning!

STRATEGY #1

Make the most of what you already collect

Advantages	Disadvantages
You probably already collect at least some data. Someone is already familiar with its contents. You may already have some idea of the key questions you want answered.	Your ability to ask questions is limited by the available data. External forces have more influence over your results. May confuse “easy” with “effective”.

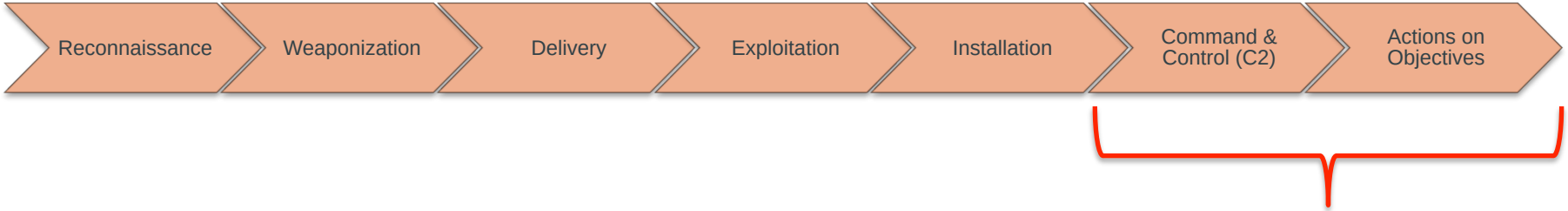
STRATEGY #2

Follow the Kill Chain

Source: *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"*, Hutchins, Cloppert, Amin, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf (Last checked April 29th,2015)

STRATEGY #2

Follow the Kill Chain



Find attacks already happening

Source: *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"*, Hutchins, Cloppert, Amin, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf (Last checked April 29th,2015)

STRATEGY #2

Follow the Kill Chain

Expand the stories you are able to tell

Find attacks already happening

Source: *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"*, Hutchins, Cloppert, Amin, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf (Last checked April 29th,2015)

STRATEGY #2

Follow the Kill Chain

Predict attacks before they happen

Expand the stories you are able to tell

Find attacks already happening

Source: *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"*, Hutchins, Cloppert, Amin, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf (Last checked April 29th,2015)

sqrrl

Securely explore your data

TIP #4: ASK LOTS OF QUESTIONS

ALL HUNTS START WITH QUESTIONS

What data do I have and what does it “look like”?

ALL HUNTS START WITH QUESTIONS

Is there any data exfiltration going on in my network?

What data do I have and what does it “look like”?

ALL HUNTS START WITH QUESTIONS

Is there any data exfiltration going on in my network?

What data do I have and what does it “look like”?

Are there any unauthorized users on my VPN?

ALL HUNTS START WITH QUESTIONS

Is there any data exfiltration going on in my network?

Have my users been spearphished?

What data do I have and what does it “look like”?

Are there any unauthorized users on my VPN?

ALL HUNTS START WITH QUESTIONS

Is there any data exfiltration going on in my network?

Have my users been spearphished?

What data do I have and what does it “look like”?

Are there any unauthorized users on my VPN?

Is anyone misusing their database credentials?

ALL HUNTS START WITH QUESTIONS

Is there any data exfiltration going on in my network?

Have my users been spearphished?

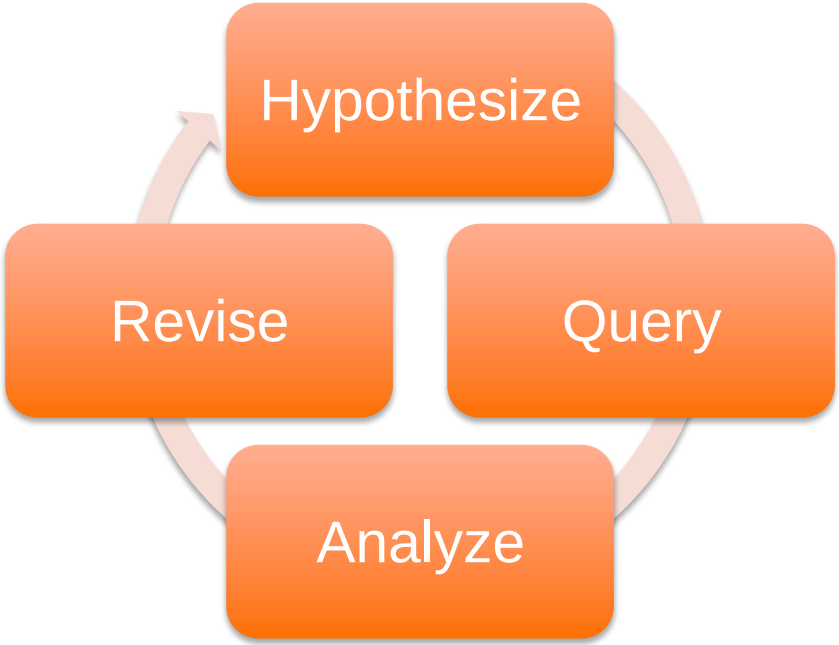
What data do I have and what does it “look like”?

Are there any unauthorized users on my VPN?

Is anyone misusing their database credentials?

Is there any lateral movement going on?

QUESTIONS BECOME HYPOTHESES



“If this activity is going on, it might look like…”

That’s your hypothesis!

If at first you don’t succeed, reimagine it.

sqrrl

Securely explore your data

TIP #5: PIVOT… THEN PIVOT AGAIN

ATTACKERS LEAVE TRAILS EVERYWHERE

Authentication records

HTTP proxy logs

Database query logs

Endpoint process accounting

Filesystem metadata

Email logs

Network session data

DATA DIVERSITY

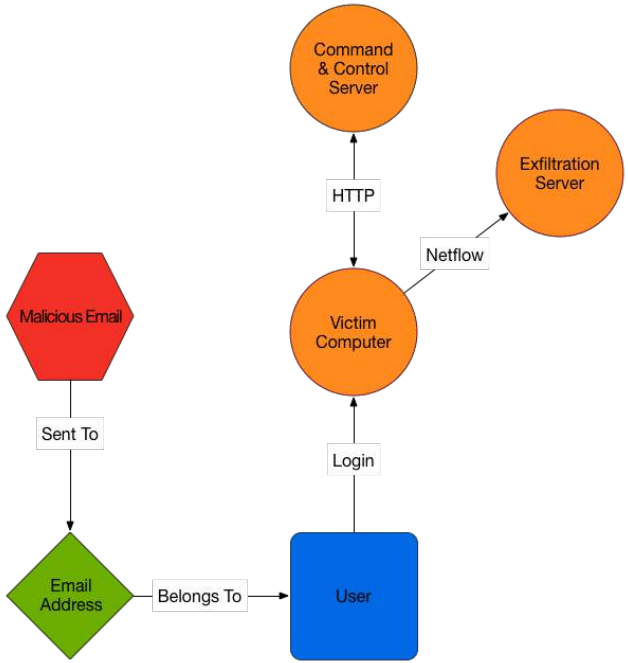
Leverage different types of data to…

- Reveal relationships
- Clarify the situation
- Highlight inconsistencies
- Tell a complete story

TOOLSET DIVERSITY

Different techniques, different perspectives

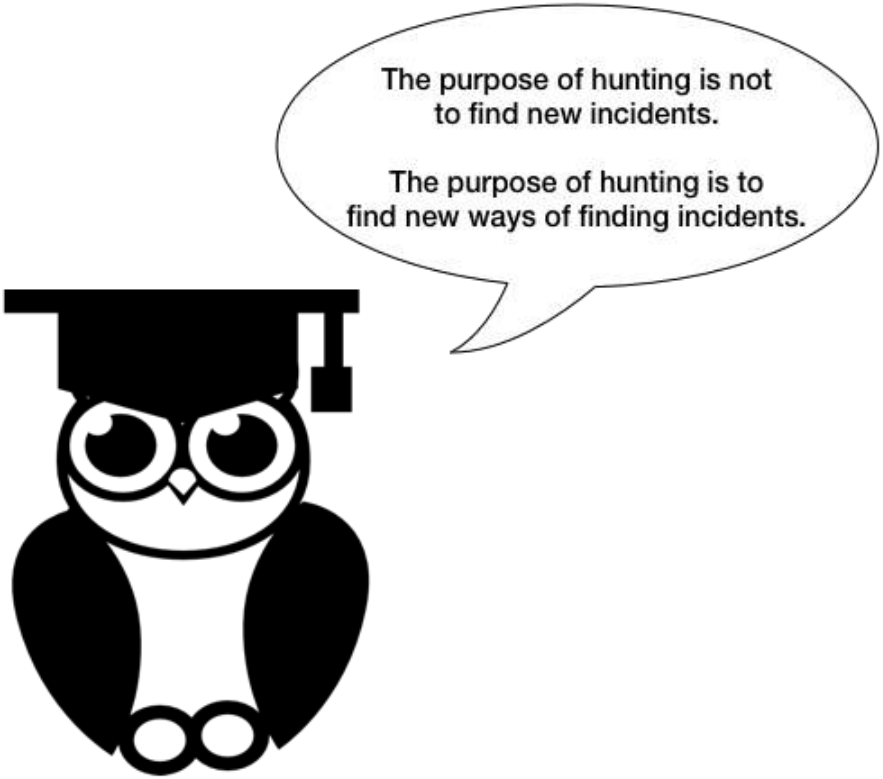
```
Terminal — tcsh — 80×24
Davids-MacBook-Pro-2:/Users/bianco/temp> cat conn.log | bro-cut -d | grep 172.16
.112.100 | head -7
1999-03-29T08:04:24-0500        CIraWsmNr6FfQnoN4       197.218.177.69  1207    1
72.16.112.100   25      tcp     smtp    0.079181        8789    243     SF      S
hAdDaFf 18      9513    14      807     (empty)
1999-03-29T08:06:03-0500        CJPYgv2yRihidyJfMj      197.182.91.233  1215    1
72.16.112.100   25      tcp     smtp    0.071476        876     244     SF      S
hAdDFaf 12      1360    11      688     (empty)
1999-03-29T08:10:07-0500        CZfV5S2A27ehEoAANk      197.218.177.69  1681    1
72.16.112.100   25      tcp     smtp    0.204133        1372    245     SF      S
hAdDaFf 13      1896    12      729     (empty)
1999-03-29T08:11:38-0500        CcEiS51qFZdVwo9Ch7      194.7.248.153   2100    1
72.16.112.100   25      tcp     smtp    0.226013        4357    243     SF      S
hAdDaFf 15      4961    13      767     (empty)
1999-03-29T08:12:10-0500        CH3KYt2602LaqpHSXj      196.227.33.189  2104    1
72.16.112.100   25      tcp     smtp    0.272825        4275    243     SF      S
hAdDaFf 15      4879    13      767     (empty)
1999-03-29T08:14:31-0500        Cyffo12ohJirmLxY7       195.115.218.108 2113    1
72.16.112.100   25      tcp     smtp    0.073653        2953    245     SF      S
hAdDaFf 14      3517    12      729     (empty)
1999-03-29T08:14:52-0500        CG5wlSu93zWh6PWy5       197.182.91.233  2120    1
72.16.112.100   25      tcp     smtp    0.086192        3633    247     SF      S
hAdDaFf 14      4197    12      731     (empty)
Davids-MacBook-Pro-2:/Users/bianco/temp>
```



sqrrl

Securely explore your data

BONUS TIP: AUTOMATION IS THE KEY TO IMPROVEMENT



sqrrl

Securely explore your data

CONCLUSION

LET'S REVIEW

- Embrace Big Data
- Get Your Data Science On
- Always Have a Good Strategy
- Ask Lots of Questions
- Pivot… Then Pivot Again
- Automation is the Key to Continuous Improvement

QUESTIONS?

David J. Bianco

dbianco@sqrrl.com

@DavidJBianco