RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

Intelligent Application Security

Julian Cohen

@HockeyInJune

#RSAC

Julian Cohen | @HockeyInJune

- Product Security | Flatiron Health

Previously

- Application Security | Financial Services
- Vulnerability Researcher | Defense Industry
- Penetration Tester | Boutique Consultancy
- Adjunct Professor | New York University

Parallel Industry Anecdote

Tonsillectomies in 1930

"It is a little difficult to believe that among the mass of tonsillectomies performed to-day all subjects for operation are selected with true discrimination, and one cannot avoid the conclusion that there is a tendency for the operation to be performed as a routine prophylactic ritual for no particular reason and with no particular result."

http://ije.oxfordjournals.org/content/37/1/9.full

Mammary Artery Ligations in 1955

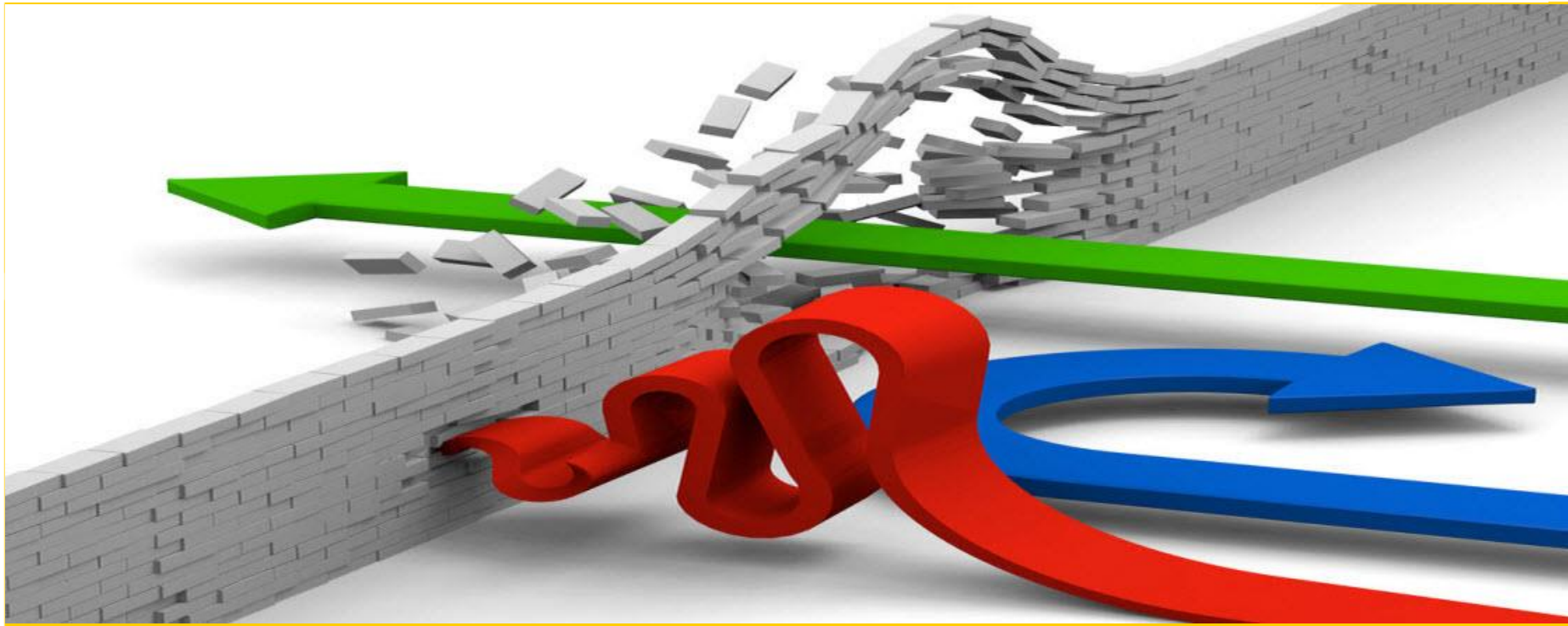
"Both the patients who did have their mammary arteries constricted and those who didn't reported immediate relief from their chest pain. In both groups the relief lasted about three months—and then complaints about chest pain returned. Meanwhile, electrocardiograms showed no difference between those who had undergone the real operation and those who got the placebo operation."

Predictably Irrational, Dan Ariely, 2009

Modern Security Medicine

Doctors were recommending the procedure and patients were having the procedure, regardless of its *effectiveness*

The expected results of the procedure did not match with the *actual results*, but no one noticed or changed anything



Penetration Testing

The Status Quo

- Penetration Testers are our experts
- Methodologies built from experience and intuition
- Application Security programs focused on fixing bugs
- Continuous loop of discovering and fixing issues
- Organizations continue to get owned

Penetration Testing Considered Harmful

- Haroon Meer, 2010, 44CON
- Limited Scope
- Bad Testers
- Poor OPSEC

- The penetration testing industry a market for lemons

http://blog.thinkst.com/p/penetration-testing-considered-harmful.html
http://www.econ.yale.edu/~dirkb/teach/pdf/akerlof/themarketforlemons.pdf

Penetration Testing Market Survey

Pre-engagement

'The quality of the marketing collateral of penetration testing companies leaves a lot to be desired. I think it's a marketplace that's shrouded in mystery and myth. It's very difficult as a person wishing to purchase penetration testing and IT Health Check services... to assess the marketplace and find out whether or not your potential vendors will satisfy what you require, other than them being able to say that they're CREST or CHECK registered... it almost feels like you need to be an expert yourself to buy an expert to come in and help you... Being able to come up with a framework with which you can engage these suppliers, and understand the nature of the different tests that they will do, and how they will treat that information in terms of reporting it back, and there being some consistency across the marketplace... I think that would be a very welcome development.'

A client of penetration tests

http://eprints.lancs.ac.uk/74275/1/Penetration_testing_online_2.pdf

Practical assessment

'Whatever's available.'

Providers on methodologies

Post-engagement

'I've never seen any "wow" reports, but a lot of bad ones.'

'Shocking.'

'Generally very hit and miss.'

'Appalling.'

Providers on the reports of other providers

'The quality varies immensely… the quality can be atrocious.'

'Often basically a Nessus output in PDF format.'

'Very impressed.'

'… great deal of variability.'

'Some are atrocious; others well thought out.'

'The quality of the document was high.'

'No significant quality variation.'

'Some are so shocking, it's hilarious.'

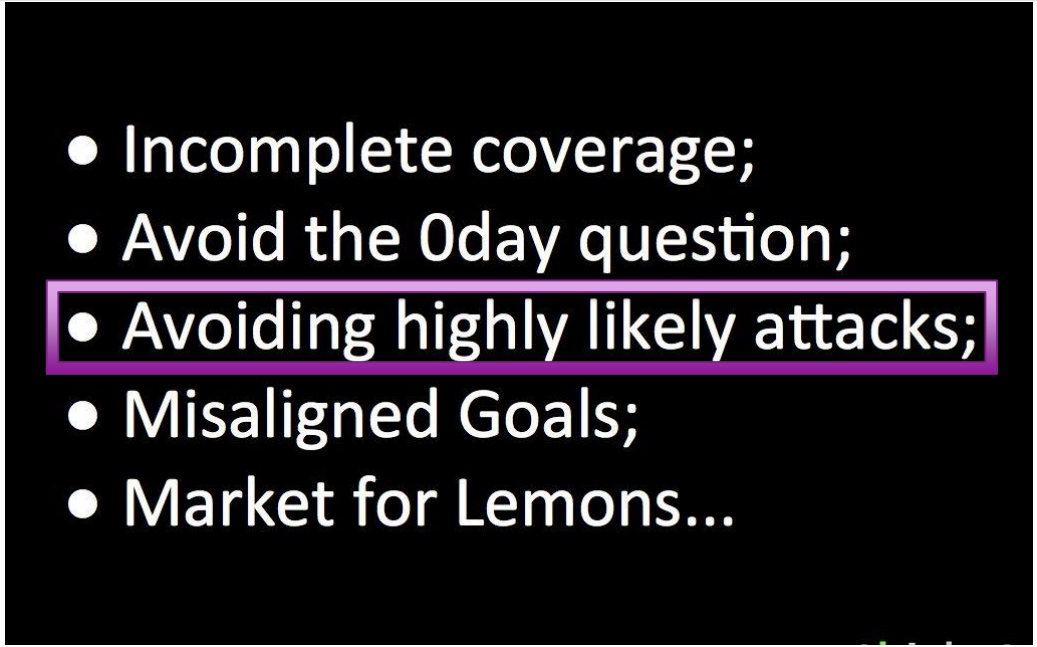
Clients on reporting quality

http://eprints.lancs.ac.uk/74275/1/Penetration_testing_online_2.pdf

Average Penetration Test

- Results depend on which testers are available
- Results depend on your tester's mood
- Results depend on your kick-off call
- Results depend on your scope
- Testers focused on writing a *"Nice Report"*
- Testers focused on discovering *cool* vulnerabilities

Pentests Avoid Highly Likely Attacks



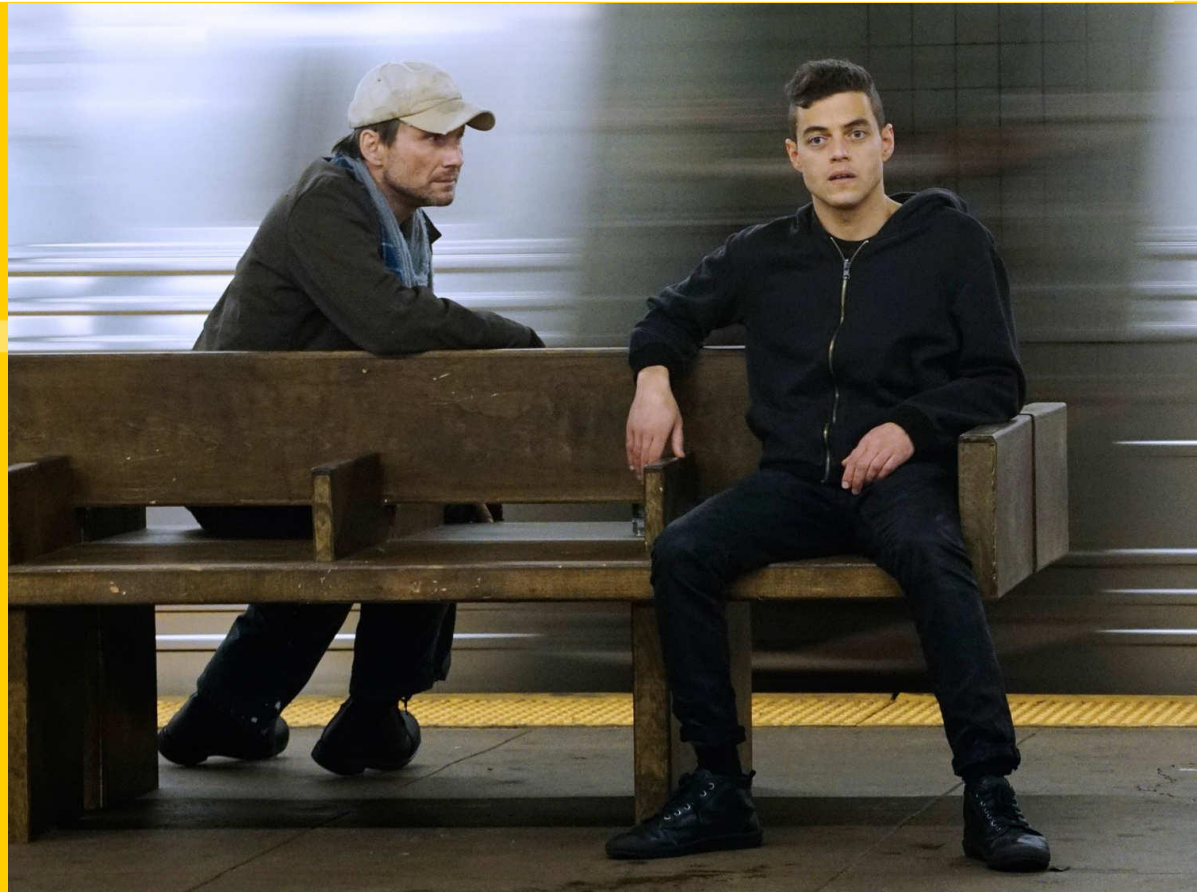
Penetration Testing Considered Harmful
Haroon Meer, 2010, 44CON

http://blog.thinkst.com/p/penetration-testing-considered-harmful.html

The Wrong Things In The Right Places

Penetration testing *avoids highly likely attacks* because the vulnerabilities that our penetration testers and our application security engineers find are *not* the vulnerabilities that real attackers find

Attackers



Everything You Know Is Wrong

- Defenders make bad assumptions about attackers
- Defenders do not understand attackers
- Defenders are not profiling attackers correctly
- And that’s why the attackers keep winning

Attacker Fallacies

Resourced Attackers

APT1 has a well-defined attack methodology, honed over years and designed to steal massive quantities of intellectual property. They begin with aggressive spear phishing, proceed to deploy custom digital weapons, and end by exporting compressed bundles of files to China – before beginning the cycle again. They employ good English — with acceptable

Intelligent Attackers

source of unreliable behavior. Nearly 50% of website visitors that should have been exploited were not due to the fragility of the replacement technique.

http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
http://blog.trailofbits.com/2013/05/20/writing-exploits-with-the-elderwood-kit-part-2/

Attacker Fallacies

Motivated Attackers

Indicators in APT28's malware suggest that the group consists of Russian speakers operating during business hours in Russia's major cities.

Dumb Attackers

The attack has been aimed at dozens of other organizations, of which Adobe Systems,[4] Juniper Networks[5] and Rackspace[6] have publicly confirmed that they were targeted. According to media reports, Yahoo, Symantec, Northrop Grumman, Morgan Stanley[7] and Dow Chemical[8] were also among the targets.

https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf
https://en.wikipedia.org/wiki/Operation_Aurora

Insight From Offense

All attackers are resource constrained

Resourced constrained attackers favor low-overhead attacks

Low-overhead requires good scalability

Attacker Playbooks

Attackers that have multiple targets care about *repeatability* and *scalability*

Operational Efficiency

Playbooks depend on:

- Who their targets are
- Intended success rate
- How fast they need to convert

Attackers operate like *efficient businesses*

- Experts at the top
- Employees are cheap and complete simple tasks
- Employees who don't meet their goals are fired
- Inefficient organizations fail quickly

Penetration testers operate like *hobbyists*

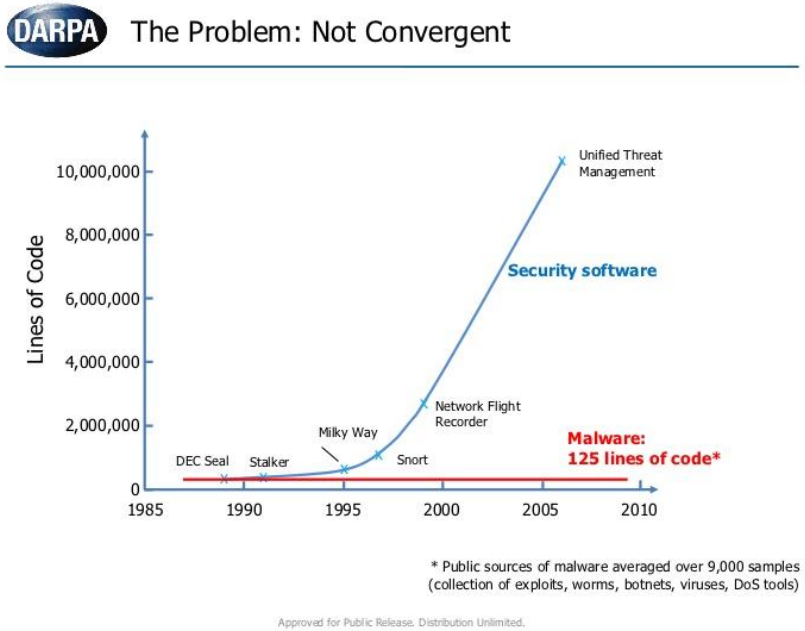
- All employees are experts
- Employees are expensive
- Employees who do not produce are hard to fire
- Organizations that do not produce do not fail
- Customers rarely care about output

Attackers

In defense, we mistake attacker *efficiency* for *inadequacy*

We are not being effective against certain attackers because we don't understand how they operate

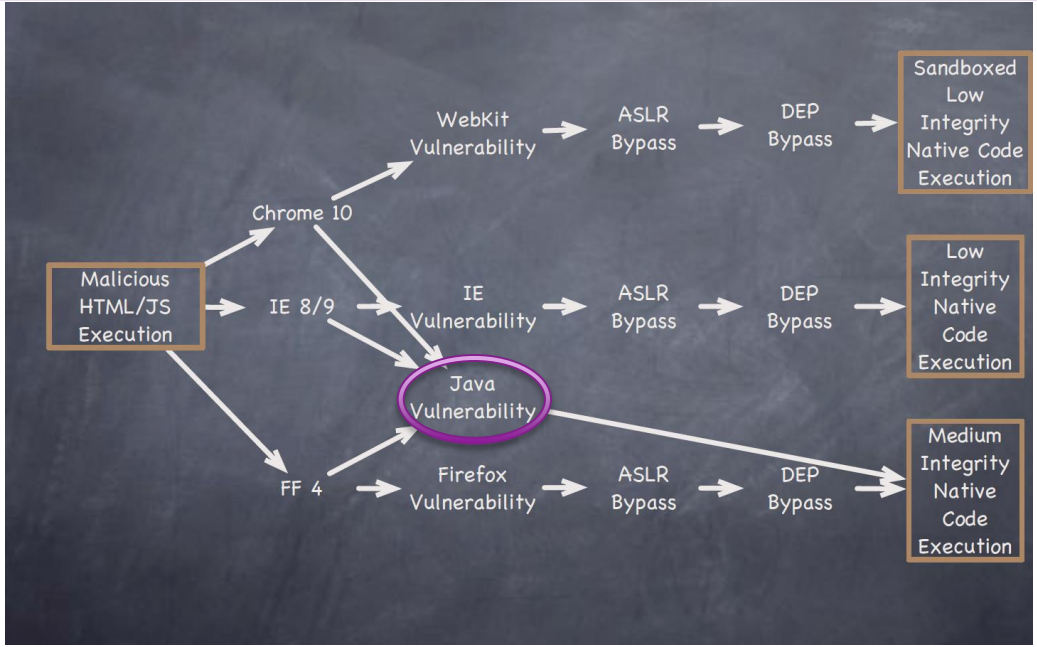
Complexity of Solution



If you don't like the game, hack the playbook…
Peiter “Mudge” Zatko, 2011, Everywhere

http://www.slideshare.net/scovetta/2011-11-07-cyber-colloquium-zatko

Attacker Cost Graph



Attacker "Math" 101
Dino Dai Zovi, 2011, SOURCE Boston, Summercon

https://www.trailofbits.com/resources/attacker_math_101_slides.pdf

Case Study: Syrian Electronic Army

- *Also: Lizard Squad and Anonymous*
- Politically-motivated, low-resourced attackers
- DNS hijacking by phishing DNS providers
- DDoS attacks with custom software
- Website defacing on shared hosting providers
- Conclusion: No web vulnerabilities used

http://news.harvard.edu/gazette/story/2013/08/hack-attacks-explained/
http://www.infowar-monitor.net/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/

Case Study: Elderwood

- *Also: PLA Unit 61398*
- State-sponsored, well-resourced attackers
- Mostly low reliability Internet Explorer bugs
- ASLR/DEP bypasses with Microsoft Office/Java
- Exploits delivered via phishing and watering holes
- Conclusion: Web vulnerabilities only when needed

http://blog.trailofbits.com/2013/05/14/writing-exploits-with-the-elderwood-kit-part-1/
http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

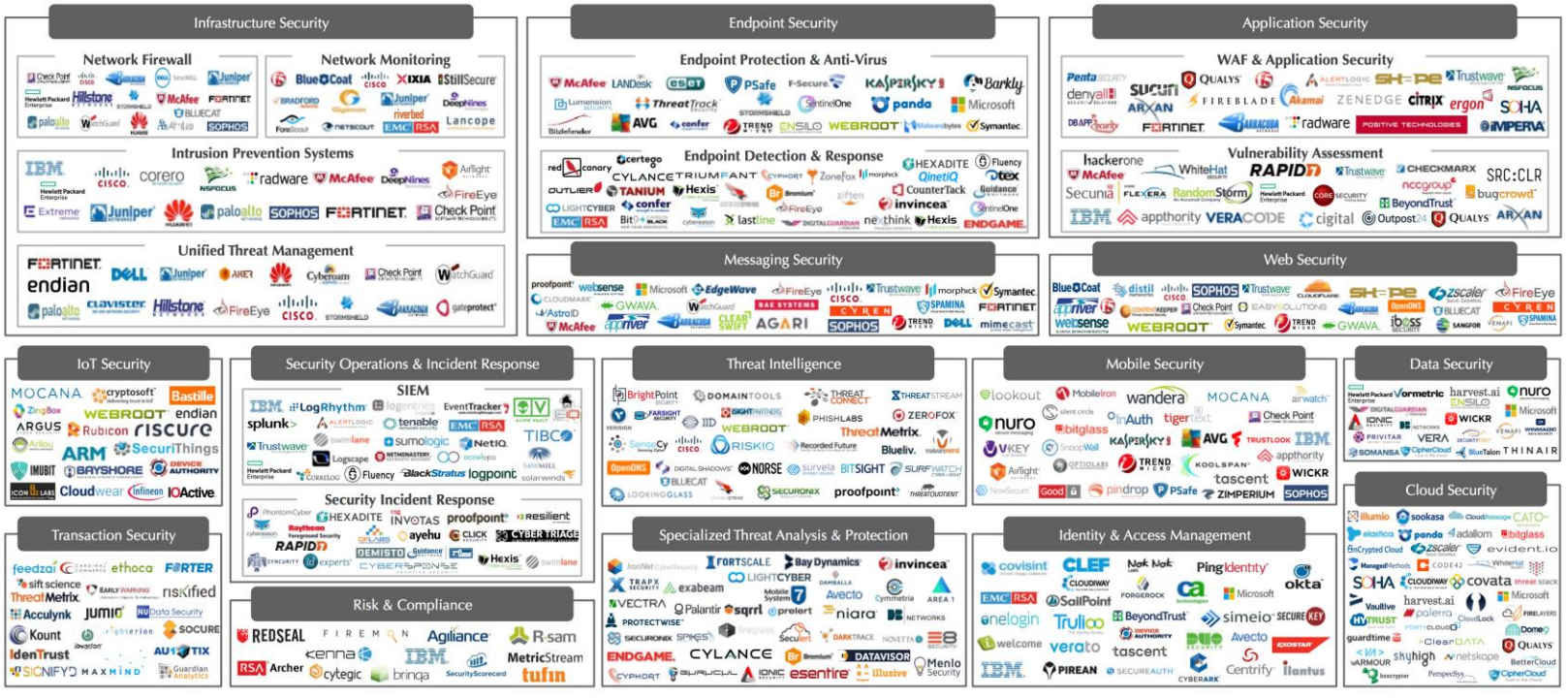
Case Study: ShadowCrew

- *Also: Other organized crime groups*
- Financially-motivated, well-resourced attackers
- Credit card data theft via SQL injection
- Typically targets one website at a time
- Scaled poorly with tools like sqlmap and havij
- Conclusion: One web vulnerability used at a time

http://www.wired.com/2010/03/tjx-sentencing/

Observations

- Real attackers don't attack web applications (*mostly*)
- These vulnerabilities are not *scalable* and *repeatable*
- Attackers focus on *inexpensive*, but *effective* methods
- The only application security threat is sqlmap
  - (sqlmap is not much of a threat)



New Security Strategy

http://momentum.partners/docs/Cybersecurity_Market_Review_Q4_2015.pdf

Lockheed Martin's Intrusion Kill Chain

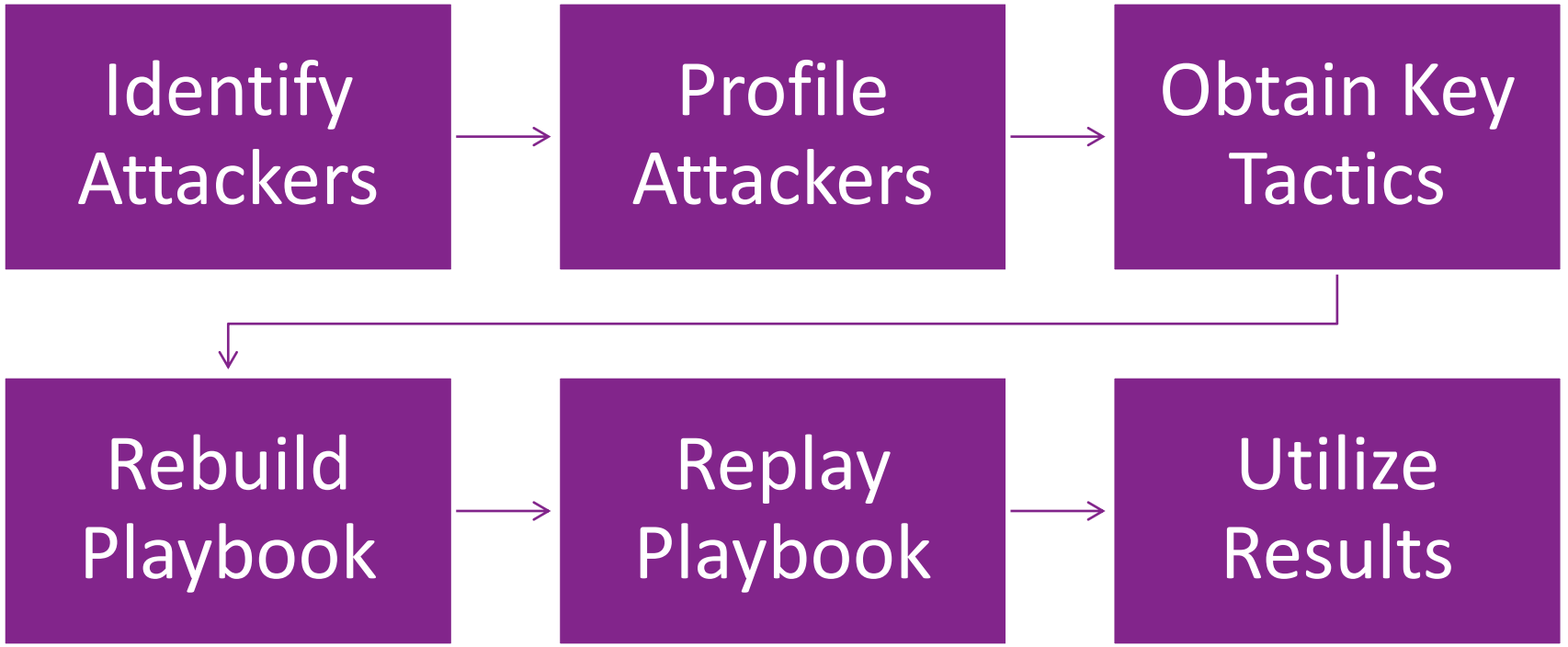
Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D.
6th International Conference Information Warfare and Security (ICIW 11)

http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Attacker Emulation



Step 4: Rebuild Playbook

Run sqlmap against your web applications

Results

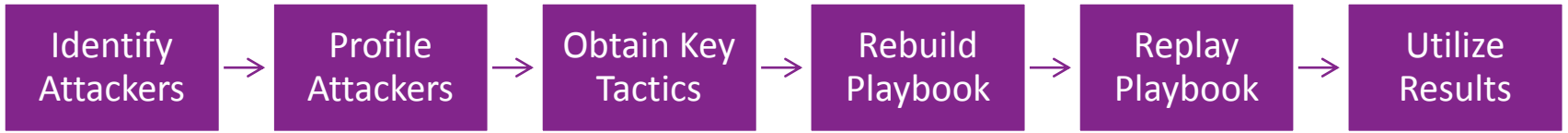
- Repeatable
- Precise
- Practical
- Effective

Threat “Intelligence”

Instead of *ephemeral* information like IP addresses, MD5 hashes, and other indicators of compromise, we should be collecting and sharing *indelible* information on *techniques* and *procedures*

Free Business Ideas

- Intelligence on attacker tactics and procedures
- Attack emulation service
- Which attacker groups I am vulnerable to



Conclusion

The security industry lacks a focus on accurate attacker methodologies during assessments

Future Work

- We are only discussing application security

The same techniques can be applied to:

- Infrastructure Security and Lateral Movement
- Client-Side Security and Endpoint Security
- Reconnaissance and Social Engineering (Phishing)

Attacker Emulation Example: RSA

Identify Attackers:
Economic Espionage
Strategic Espionage

→

Profile Attackers:
State-Sponsored
Well-Resourced

→

Obtain Key Tactics:
Phishing
Watering Hole
Client-Side Exploitation

↓

Rebuild Playbook:
Public Reconnaissance
Phishing Campaigns
Client-Side Exploitation

→

Replay Playbook:
Launch Attack

→

Utilize Results:
Exploit Mitigation
Sandboxing
Execution Tree Analysis

Thanks

- Justin Berman
- Nicholas Arvanitis
- Chris Sandulow
- Stuart Larsen
- Spencer Jackson
- Dino Dai Zovi
- Nick Freeman
- Brandon Edwards

We’re Hiring!

FLATIRON

security@flatiron.com