Maltego Kung-Fu
Exploiting Open Source Threat Intelligence

Matt Kodama
VP Product
matt@recordedfuture.com
OSINT finds are out there!

http://mmqb.si.com
https://twitter.com/mattyglesias/status/303994450605142018
Selected challenges
Iterative investigation

- Private Collections
- Open Sources
- Tips from Trusted Peers
- Research Subscriptions
Frictionless access to intel info

Probe a collection
Expand set of observables
Pivot investigation focus
Prune to indicators

Why Maltego?

Available and affordable

“Analyst owned and operated”

Got data? Just paste.

Extensible and connectable
What we’ve learned

Tips for linking your data to Maltego in a live demo form factor 😊
Conclusion: the takeaways

• Turnkey TDS access  Optimized for “I’m too busy”
• Keep transforms atomic  Enable creative mashups
• Transparent results  Good analysts are skeptics
• What & When  Time will matter
• Expect mystery meat  If you knew, you wouldn’t ask
• Keep your ears open!  Acknowledgements