

# Lancope®

Threat Intelligence?



Gavin Reid - Lancope

# Presenter

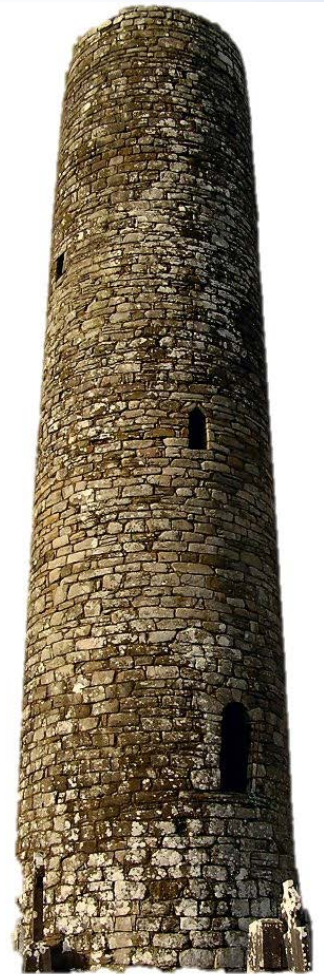
- Gavin Reid is Vice President of Threat Intelligence at Lancope, With over 25 years of experience in threat intelligence, Reid was a driving force behind the development of big data analytics and threat identification.
- While serving at Cisco Systems as director of threat research for Security Intelligence Operations, he led a team that developed new data analytics technologies to detect and remediate advanced cybersecurity threats.
- Reid also created and led Cisco's Computer Security Incident Response Team (CSIRT), a global organization of information security professionals responsible for monitoring, investigating and responding to cybersecurity incidents.
- In addition to his time at Cisco, Reid also served as the vice president of threat intelligence at Fidelity Investments and oversaw IT security at NASA's Johnson Space Center.



Where  
are we  
with  
security  
2015?



# State of the industry





# State of the industry



# What we need to do differently



# What is Threat?



# What is intelligence



## IP with no or invalid context

8.8.8.8

**Malware:** Dridex

**Analysis:**

**Attachment File Name:** RZZA3440.doc

**Attachment MD5s:**

[b4fe7224da594703e78d62d9cb85c5f4c3a00c36ea51040c3a10c557154bc7b15b9acbcd65555398a7e3fd0f0a389cf9582b75b4f8855dbe555bff080c57808abe699ba4855340adf5c9d7092e9df08b](#)

**Payload URLs:**

[http://internetz1\[.\]com/03/39.exe](http://internetz1[.]com/03/39.exe)  
[http://gggrp\[.\]com/03/59.exe](http://gggrp[.]com/03/59.exe)  
[http://fefg\[.\]com/03/39.exe](http://fefg[.]com/03/39.exe)  
[http://woofe\[.\]com/03/39.exe](http://woofe[.]com/03/39.exe)  
[http://contestswin\[.\]net/03/39.exe](http://contestswin[.]net/03/39.exe)

**Payload MD5:**

[5e91af2e44c17de55134ff935c0f30f1](#)

**C2:**

[130.0.133\[.\]135](#)

# Can you protect what you can't see?









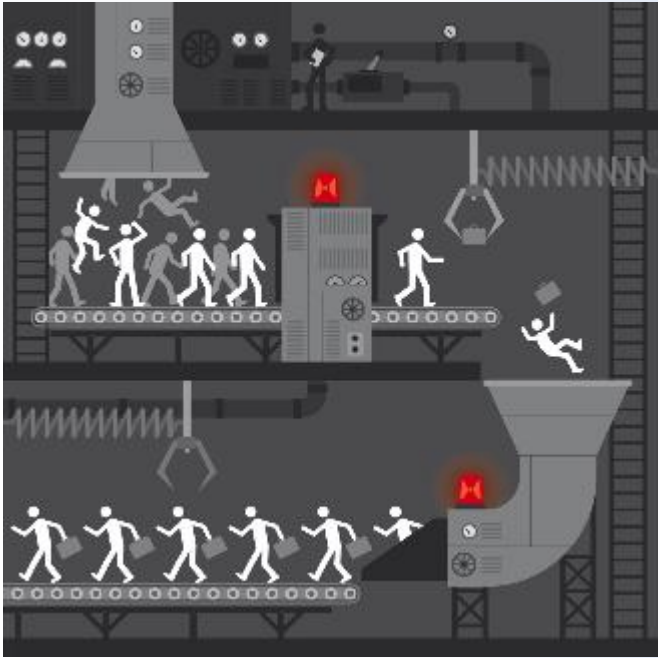
Data Jockey

Getting data ready

vs

Working on data

# Concerns





Make Sure you have deliverables beyond needle and haystack





Thanks!

