Cyber Threat Hunting in the Middle East

SEPTEMBER 2018

Kevin Albano
Global Threat Intelligence Lead
It’s just a little dusty…
Gulf Cooperation Council Countries

- Kuwait
- Bahrain
- Qatar
- United Arab Emirates
- Oman
- Saudi Arabia
Iran Based Threats

Social Engineering
- Fake personas
- Target Individuals

Backdoor
- Powershell
- DGA C2

Threat action
- Destructive (Wiper)
- Maintain Persistence

Spear-phishing
- Productivity Documents
- Strategic Web Compromise

Internal Recon
- Increased dwell time
- Understand Supply Chain

Target Industries
- Military
- Energy
- Government
- Aerospace
- Petrochemical
CTI Operations
THREAT INTEL PERSONAS

Experts

- Identify and curate threat information from around the globe

Doers

- Protect their domain from relevant threats

Watchers

- Communicate key threats relevant to their domain

Decision Maker

- Decision makers / influencers affect resource management in response to relevant threats
Who are the Hunters?

Threat Intel Personas

**Doers**
Doers *protect* their domain from relevant threats

**Watchers**
Watchers *communicate* key threats relevant to their domain

**Decision Maker**
Decision makers / influencers *affect* resource management in response to relevant threats

**Experts**
Experts *identify* and *curate* threat information from around the globe

40% 10% 40% 10%
THANK YOU

FOLLOW US ON:

ibm.com/security
securityintelligence.com
xforce.ibmcloud.com
@ibmsecurity
youtube/user/ibmsecuritaysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.