IBM Security

Cyber Threat Hunting in the Middle East

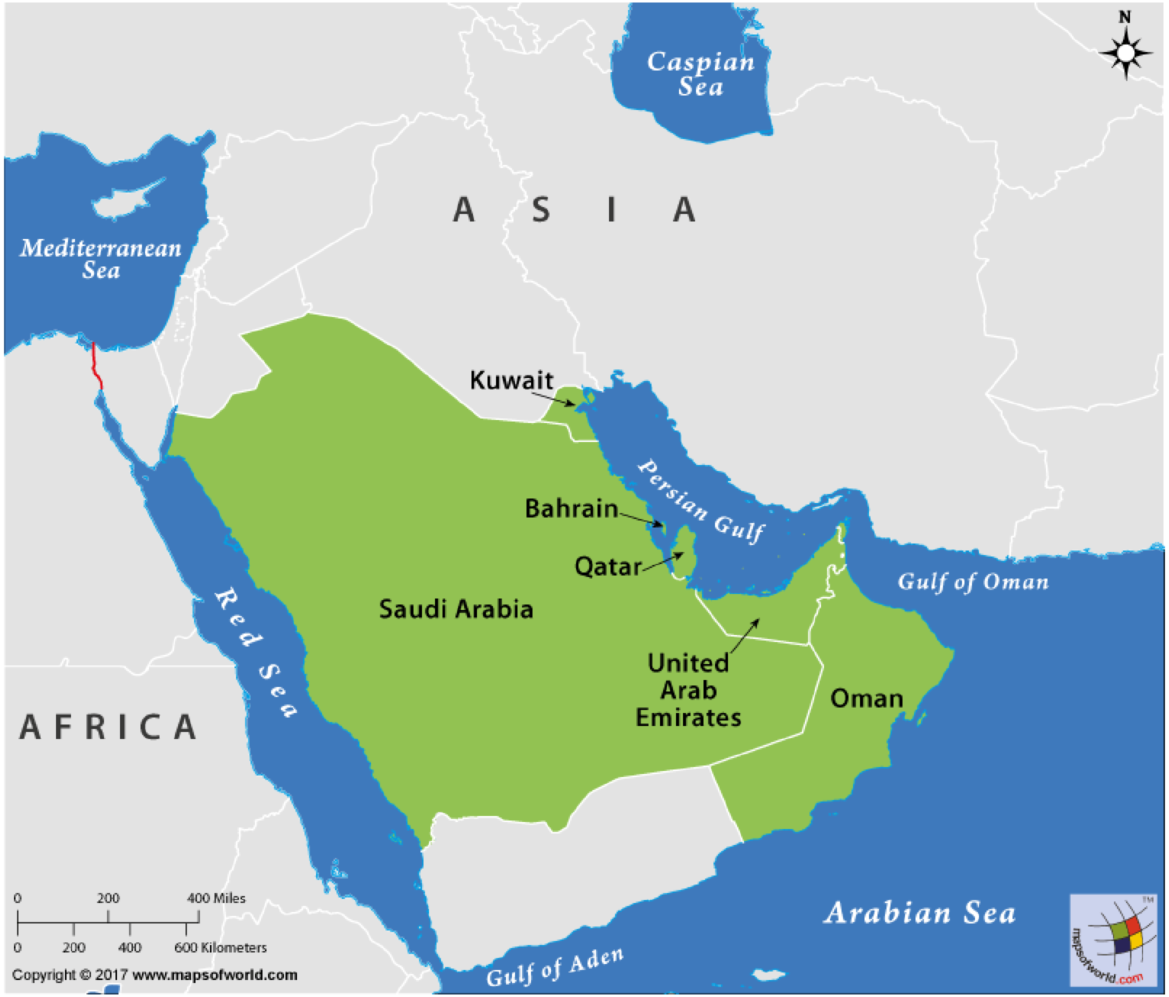
SEPTEMBER 2018

Kevin Albano
Global Threat Intelligence Lead

It’s just a little dusty…

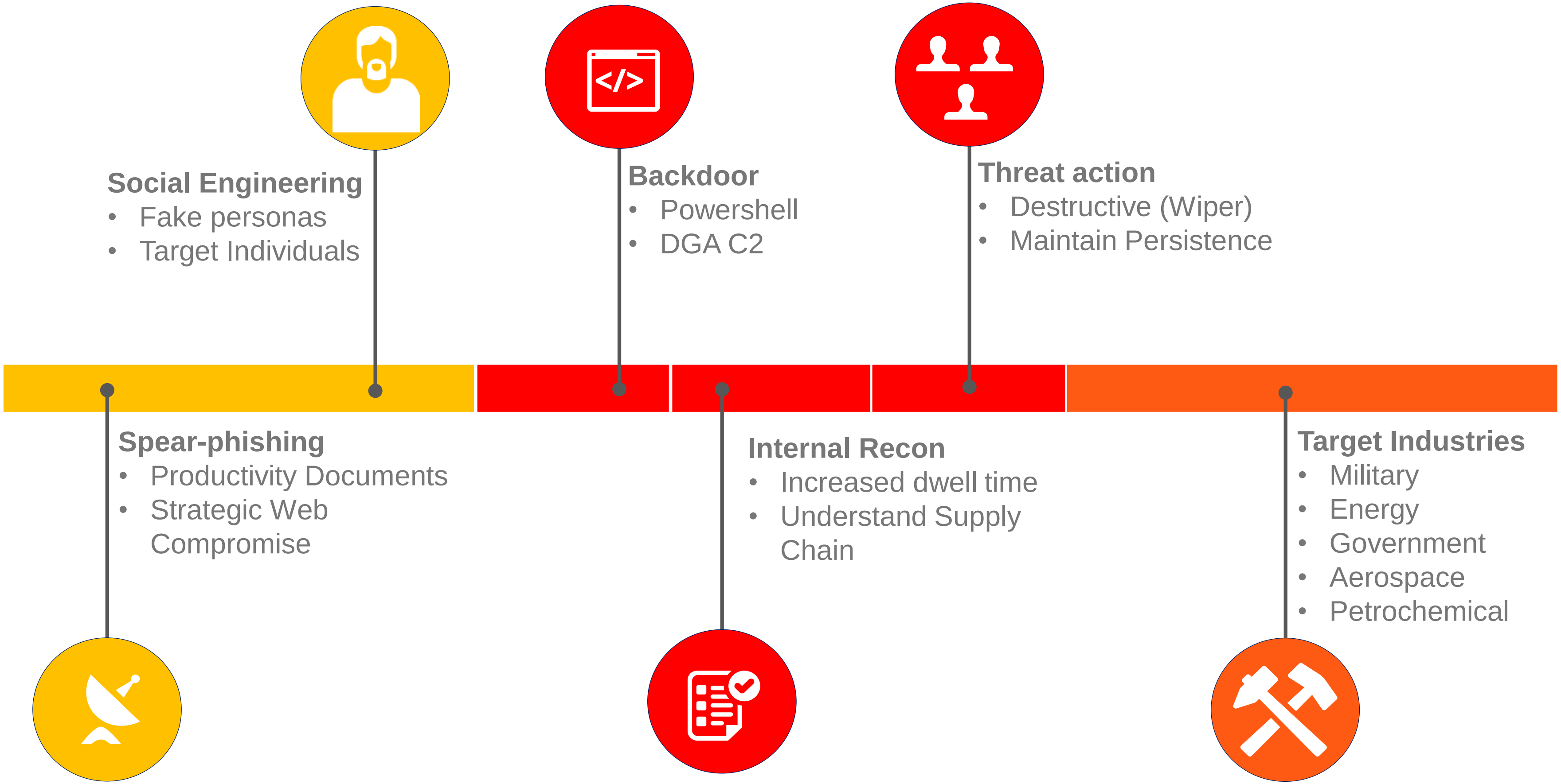
Gulf Cooperation Council Countries

- Kuwait
- Bahrain
- Qatar
- United Arab Emirates
- Oman
- Saudi Arabia



Copyright © 2017 www.mapsofworld.com

Iran Based Threats



Spear-phishing
- Productivity Documents
- Strategic Web Compromise

Social Engineering
- Fake personas
- Target Individuals

Backdoor
- Powershell
- DGA C2

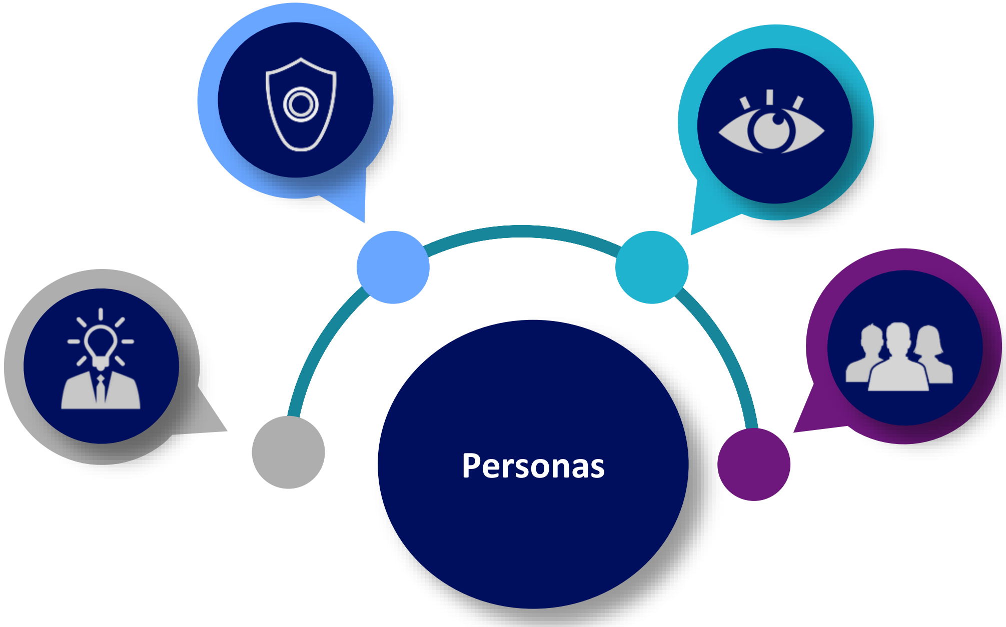
Internal Recon
- Increased dwell time
- Understand Supply Chain

Threat action
- Destructive (Wiper)
- Maintain Persistence

Target Industries
- Military
- Energy
- Government
- Aerospace
- Petrochemical

CTI Operations

THREAT INTEL PERSONAS



Doers

Doers **protect** their domain from relevant threats

Watchers

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

Experts

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

Decision Maker

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

Who are the Hunters?

Doers

Doers **protect** their domain from relevant threats

Watchers

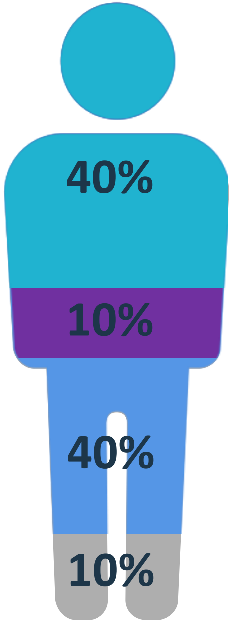
Watchers **communicate** key threats relevant to their domain

Decision Maker

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

Experts

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



IBM Security

THANK YOU

FOLLOW US ON:

ibm.com/security

securityintelligence.com

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

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.