
# Cyber Threat and Proactive Defenses

Curtis Dukes
Executive VP & General Manager,
Security Best Practices & Automation Group
November 4, 2021

# Today's Cyber Threats -- Summary

- Cyber Threats becoming Commoditized
- Level of Expertise required is Decreasing – *Internet tools become easier to use*
- Trend is Clear – *Disruption*
- Growing use of Information Operations leveraging Cyber Intrusions – *Nation States*

# Nation State Activity

- Top Tier Cyber Adversary
- Aggressive Behavior of Late – similar to Military Operations
- Integration with Physical and Information Operations

- Sensitive to International Political Events
- Volume – Government, Economic, Information
- Organization Defines Capability

- Growing in Capability
- Early DDoS [ineffective] and Destructive Tendencies
- Reactive to Political Events

- Effective Tool of State Power
- Primarily Used for Generation of Hard Currency for the Regime
- Mostly Targets Asian Countries

# Ransomware

- **High Business Impact –** *Extortion must impact business operations to motivate payment*
- **Profitable for Attackers –** *Economic incentive to continue growing*
- **Room to Grow –** *Attackers can monetize security maintenance gaps at most enterprises*
- **Key Takeaways**
  - Stakes have changed
  - No end in sight
  - Attacks have weaknesses

# The Defender's Dilemma

- What's the right thing to do, and how much do I need to do?
- How do I actually do it?
- And how can I demonstrate to others that I have done the right thing?

# Community Defense Model (v2.0)

- Top five attack types:
  - Malware,
  - Ransomware,
  - Web Application Hacking,
  - Insider Privilege and Misuse, and
  - Targeted Intrusions.
- IG1 Safeguards defends against 77% of ATT&CK techniques used across the top five attack types
- 91% if all CIS Safeguards are implemented

# Critical Security Controls v8


*Confidence in the Connected World*