



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*

CIS. 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?



CIS 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



CIS Critical Security Controls v8

<p>CONTROL 01 Inventory and Control of Enterprise Assets</p> <p>5 Subparts EC 2.5 CC 4.5 HC 5.5</p>	<p>CONTROL 02 Inventory and Control of Software Assets</p> <p>7 Subparts EC 3.7 CC 6.7 HC 7.7</p>	<p>CONTROL 03 Data Protection</p> <p>14 Subparts EC 6.14 CC 12.14 HC 14.14</p>
<p>CONTROL 04 Secure Configuration of Enterprise Assets and Software</p> <p>12 Subparts EC 7.12 CC 11.12 HC 12.12</p>	<p>CONTROL 05 Account Management</p> <p>6 Subparts EC 4.6 CC 6.6 HC 6.6</p>	<p>CONTROL 06 Access Control Management</p> <p>8 Subparts EC 5.8 CC 7.8 HC 8.8</p>
<p>CONTROL 07 Continuous Vulnerability Management</p> <p>7 Subparts EC 4.7 CC 7.7 HC 7.7</p>	<p>CONTROL 08 Audit Log Management</p> <p>12 Subparts EC 3.12 CC 11.12 HC 12.12</p>	<p>CONTROL 09 Email and Web Browser Protection</p> <p>7 Subparts EC 2.7 CC 6.7 HC 7.7</p>
<p>CONTROL 10 Malware Defenses</p> <p>7 Subparts EC 3.7 CC 7.7 HC 7.7</p>	<p>CONTROL 11 Data Recovery</p> <p>5 Subparts EC 4.5 CC 5.5 HC 5.5</p>	<p>CONTROL 12 Network Infrastructure</p> <p>8 Subparts EC 1.8 CC 7.8 HC 8.8</p>
<p>CONTROL 13 Network Monitoring and Defense</p> <p>11 Subparts EC 0.11 CC 6.11 HC 11.11</p>	<p>CONTROL 14 Security Awareness and Skills Training</p> <p>9 Subparts EC 8.9 CC 9.9 HC 9.9</p>	<p>CONTROL 15 Service Provider Management</p> <p>7 Subparts EC 1.7 CC 4.7 HC 7.7</p>
<p>CONTROL 16 Applications Software Security</p> <p>14 Subparts EC 0.14 CC 11.14 HC 14.14</p>	<p>CONTROL 17 Incident Response Management</p> <p>9 Subparts EC 3.9 CC 8.9 HC 9.9</p>	<p>CONTROL 18 Penetration Testing</p> <p>5 Subparts EC 0.5 CC 3.5 HC 5.5</p>



Confidence in the Connected World