Enterprise Security: No Endpoint Left Behind

Duncan McAlýnn
Chief Cyber Strategist
Operandis, LLC
PS: whoami

- 20+ Years Enterprise Mgmt & InfoSec
- 6x MVP, CISSP, Security+, MCSE, MCSA
- Co-Founder, Original SMS User Conf ’98
- FBI InfraGard
- Columnist, CSO Online
- Heavy Twitter User @infosecwar (#WeHackBack)
- Connect on LinkedIn
Agenda

Protecting & Defending the Enterprise

- Cybersecurity Threat Briefing
- CIS Top 5 Security Controls: 80/20 Rule
- Threat Mitigation Features of Windows 10 CU
- System Center ConfigMgr as a Security Screwdriver
- Windows 10/Server 2016 Hardening Made Easy
- Cybersecurity Hygiene & Best Practices
- Malware/Ransomware Detection & Removal
Trigger Warning
2017 Cyberthreat Year in Review

- Cloudbeed, OKCupid/Fitbit PII
- Wikileaks CIA Vault 7, Espionage Tools
- Shadow Brokers, NSA Tools; incl. EternalBlue, DoublePulsar
- WannaCry, 250-300K Infected Systems Worldwide
- Petya/NotPetya/GoldenEye, Ukraine (ManageEngine/LogMeIn)
- Macron Campaign Hack, 9GB Trove of Leaked Emails
- DeepRoot, 198M Voter Records PII Exposed Publicly
- Equi***, Uber... Need I Say More?
Center for Internet Security Top 5
Security Controls: 80/20
CIS Top Five Controls

Put simply, the CIS Controls were developed to answer the frequent question:

“Where should I start when I want to improve my cyber defenses?”
CIS Controls

First 5 CIS Controls
Eliminate the vast majority of your organization's vulnerabilities

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software
4: Continuous Vulnerability Assessment and Remediation
5: Controlled Use of Administrative Privileges

All 20 CIS Controls
Secure your entire organization against today's most pervasive threats

6: Maintenance, Monitoring, and Analysis of Audit Logs
7: Email and Web Browser Protections
8: Malware Defenses
9: Limitation and Control of Network Ports
10: Data Recovery Capability
11: Secure Configurations for Network Devices
12: Boundary Defense
13: Data Protection
14: Controlled Access Based on the Need to Know
15: Wireless Access Control
16: Account Monitoring and Control
17: Security Skills Assessment and Appropriate Training to Fill Gaps
18: Application Software Security
19: Incident Response and Management
20: Penetration Tests and Red Team Exercises

CIS SecureSuite Membership
Become a member
Learn More

Download the First 5 CIS Controls
Download All 20 CIS Controls
The First 5 CIS Controls

CIS, US-CERT, ASD, & other authorities prioritize these five elements of cyber hygiene to significantly reduce security threats.

<table>
<thead>
<tr>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory of authorized and unauthorized devices</td>
</tr>
<tr>
<td>Inventory of authorized and unauthorized software</td>
</tr>
<tr>
<td>Secure configuration for hardware and software</td>
</tr>
<tr>
<td>Controlled use of administration privileges</td>
</tr>
<tr>
<td>Continuous vulnerability assessment and remediation</td>
</tr>
</tbody>
</table>
# The First 5 CIS Controls

CIS, US-CERT, ASD, & other authorities prioritize these five elements of cyber hygiene to significantly reduce security threats.

## Inventory of authorized and unauthorized devices

<table>
<thead>
<tr>
<th>Key Principle:</th>
<th>Main Points:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.</td>
<td>Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization’s public and private network(s).</td>
</tr>
</tbody>
</table>
The First 5 CIS Controls
CIS, US-CERT, ASD, & other authorities prioritize these five elements of cyber hygiene to significantly reduce security threats

<table>
<thead>
<tr>
<th>Inventory of authorized and unauthorized software</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Principle:</strong></td>
</tr>
<tr>
<td>Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.</td>
</tr>
<tr>
<td><strong>Main Points:</strong></td>
</tr>
<tr>
<td>Devise a list of authorized software and version that is required in the enterprise for each type of system. Deploy application whitelisting that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system.</td>
</tr>
</tbody>
</table>
The First 5 CIS Controls
CIS, US-CERT, ASD, & other authorities prioritize these five elements of cyber hygiene to significantly reduce security threats

<table>
<thead>
<tr>
<th>Secure configuration for hardware and software</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Principle:</strong></td>
</tr>
<tr>
<td>Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.</td>
</tr>
<tr>
<td><strong>Main Points:</strong></td>
</tr>
<tr>
<td>Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications. Follow strict configuration management, building a secure image.</td>
</tr>
</tbody>
</table>
The First 5 CIS Controls
CIS, US-CERT, ASD, & other authorities prioritize these five elements of cyber hygiene to significantly reduce security threats

### Continuous vulnerability assessment and remediation

**Key Principle:**
Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

**Main Points:**
Run automated vulnerability scanning tools against all systems on the network regularly. Deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator. Correlate event logs with information from vulnerability scans to determine if an exploit has been used.
The First 5 CIS Controls
CIS, US-CERT, ASD, & other authorities prioritize these five elements of cyber hygiene to significantly reduce security threats

Key Principle:
The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Main Points:
Minimize administrative privileges & only use administrative accounts when they are required. Implement auditing on the use of administrative privileged functions & monitor for anomalous behavior.

Use automated tools to inventory all administrative accounts.
Windows 10 FCU

Threat Mitigation Features
Pre-breach Threat Mitigation

• Windows Defender System Guard  
  • TPMv2-based boot-to-use integrity guardian
• Windows Defender Application Guard  
  • EMET Mitigations Built-in (ASLR, ASR, Cert Pinning, etc.)
• Windows Defender Exploit Guard  
  • ASR Rules, Controlled Folders, Exploit Protection
• Windows Defender Antivirus  
  • Common anti-malware solution
• Windows Defender Application Control  
  • Controlled use of applications that can/cannot be run by end-users
Post-breach Detection w WD-ATP

• Detect attacks and zero-day exploits
• Visually investigate forensic evidence
• Interactively hunt with historical data
• Respond to contain the attack & prevent future exploits of the same vector
• Exploration with Office 365 ATP Graph Subscription
System Center ConfigMgr as a Security Screwdriver
Security Screwdriver

Don’t underestimate the power of SCCM

• Hardware & Software Inventory
• Software Update Management
• Windows Defender Client Deployment & Management
• Windows Firewall Settings
• Compliance Baseline Management
Windows 10 & Server 2016
Hardening Made Easy
Hardening Made Easy

Hardening is a process of limiting potential weaknesses that make systems vulnerable to cyber attacks. Benefits include:

• Reduce attack surfaces;
• Remove unneeded services, applications, features;
• Known-good image, approved by change mgmt.;
• Monitored for compliance drift.
DEMO
Creating & Importing Security Compliance Baselines
Cybersecurity Hygiene & Best Practices from the Field
Ransomware Vulnerabilities

- Understand the attack vectors of known threats;
- Inventory/scan environment to assess risk;
- Standardize prioritization of patching/remediation to mitigate risks (NIST);
- Isolate systems that can’t be fixed.
Phishing & Watering Hole Attacks

• Leverage anti-spam, phishing, and web control tools for employee protection;
• Encourage the human firewall;
• Don’t blame the victims; instead, give them the right tools and reward good behaviour.
• PhishMe Free (<500)
Malverstisements & Downloaders

- Go beyond traditional blacklist-based endpoint security for maximum protection;
- Focus on attack surface reduction;
- Detect and block malicious behavior;
- Re-associate malicious filetypes;
Filetype Re-Association

Consider re-associating the following with notepad:

- **Programs**: PIF, .COM, .SCR, .HTA, .CPL, .MSC, .JAR
- **Scripts**: .BAT, .CMD, .VB, .VBS, .VBE, .JS, .JSE, .WS, .WSF, .WSC, .WSH, .PS1, .PS1XML, .PS2, .PS2XML, .PSC1, .PSC2, .MSH, .MSH1, .MSH2, .MSHXML, .MSH1XML, .MSH2XML
- **Office Macros**: .DOC, .XLS, .PPT, .DOCM, .DOTM, .XLSM, .XLTM, .XLAM, .PPTM, .POTM, .PPAM, .PPSM, .SLDM
- **Others**: .REG, .INF, .LNK, .SCF, .PDF

Deploy with ConfigMgr:
Bulletproof Your Backup & Recovery Practices

• 3-2-1 Rule;
• Focus on frequent and clean backups;
• Schedule frequent backups;
• Watch backups for malware;
• Don’t forget Hypervisor backups.
Protecting Against Fileless Malware*

- Block activity, not just file signatures;
- Beware macros, stricter controls;
- Disable system admin tools you don’t use;
- Patch what you can, isolate what you can’t;
- “Do” the principle of least privilege;
- Protect RDP (Gateway/Ports), SMB (Disable SMB v1);
- Block common malicious file attachments;
- Conduct user awareness training (human firewall);
- Blocked fixed port for Remote WMI; and
- Monitor scheduled task creation & process spawning with CREATE_SUSPENDED flag (process hollowing)

*Condensed content from Barkly - https://www.barkly.com/2017-cybersecurity-checklist
<table>
<thead>
<tr>
<th>Time</th>
<th>Speaker</th>
<th>Room</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/8: 10:30</td>
<td>Mowrer</td>
<td>Sterling Ridge</td>
<td>Architect a Post-Breach Cyber-Defense Strategy</td>
</tr>
<tr>
<td>2/8: 11:45</td>
<td>Rangama</td>
<td>College Park</td>
<td>Azure Governance: Lessons from the Field</td>
</tr>
<tr>
<td>2/9: 10:30</td>
<td>Zerger</td>
<td>Sterling Ridge</td>
<td>Mapping Microsoft Cybersecurity to the Cyber Kill-Chain</td>
</tr>
<tr>
<td>2/9: 11:45</td>
<td>Mowrer</td>
<td>Alden Bridge</td>
<td>Securing BYOD Mobility with EMS &amp; Intune MAM</td>
</tr>
<tr>
<td>2/9: 2:00</td>
<td>McAlynn</td>
<td>Alden Bridge</td>
<td>Enterprise Cybersecurity: No Endpoint Left Behind</td>
</tr>
<tr>
<td>2/9: 3:30</td>
<td>Kroesbergen</td>
<td>College Park</td>
<td>Modernizing Authentication: Eliminating Extranet Passwords</td>
</tr>
</tbody>
</table>
Take the Survey!

Your feedback is important! Please rate the session for a chance to win!

Survey is below session description at http://elus18.expertslive.us
Questions & Answers

Duncan McAlynn
dmc@operandis.net | @infosecwar