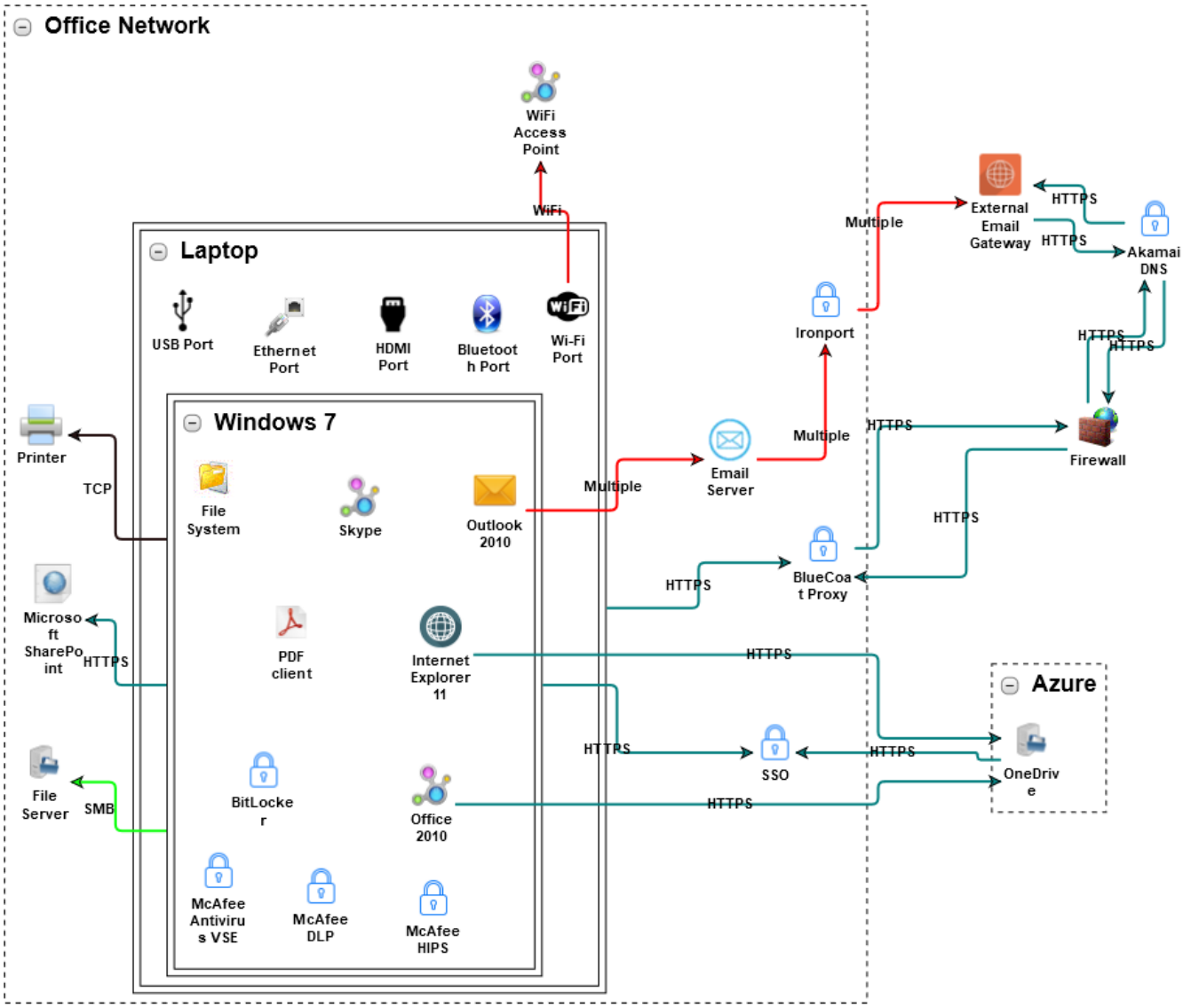
ThreatModeler
Identify • Classify • Prioritize • Mitigate

Endpoint Security - what-if analysis 1

07/23/2017

Threat Model



Threats

Threat	Source	Risk	Status	Date Created
File Manipulation	File System	Medium	Mitigated	07/23/2017
Accessing, Modifying or Executing Executable Files	File System	Very	Mitigated	07/23/2017

		High		
Create files with the same name as files protected with a higher classification	File System	Very High	Mitigated	07/23/2017
Force Use of Corrupted Files	File System	Medium	Mitigated	07/23/2017
Leveraging and or Manipulating Configuration File Search Paths	File System	Very High	Mitigated	07/23/2017
User-Controlled Filename	File System	High	Mitigated	07/23/2017
Manipulating Input to File System Calls	File System	Very High	Mitigated	07/23/2017
Buffer Overflow	File Server	Very High	Mitigated	07/23/2017
Explore For Predictable Temporary File Names	File Server	Medium	Mitigated	07/23/2017
Screen Temporary Files for Sensitive Information	File Server	Medium	Mitigated	07/23/2017
File Manipulation	File Server	Medium	Mitigated	07/23/2017
Accessing, Modifying or Executing Executable Files	File Server	Very High	Mitigated	07/23/2017
Create files with the same name as files protected with a higher classification	File Server	Very High	Mitigated	07/23/2017
Manipulating Input to File System Calls	File Server	Very High	Mitigated	07/23/2017
Physical Theft	Laptop	Very High	Mitigated	07/23/2017
Man in the Middle Attack	Wi-Fi Port	Very High	Mitigated	07/23/2017
Rogue Wi-Fi Access Point	Wi-Fi Port	Very High	Open	07/23/2017
Bluejacking	Bluetooth Port	Very High	Open	07/23/2017
Bluesnarfing	Bluetooth Port	Very High	Open	07/23/2017
Bluebugging	Bluetooth Port	Very High	Open	07/23/2017
Buffer Overflow	HDMI Port	Very High	Mitigated	07/23/2017
Malware Propagation via USB Stick	USB Port	Very High	Mitigated	07/23/2017
Malware Propagation via USB U3 Autorun	USB Port	High	Mitigated	07/23/2017
Malware Propagation via Infected Peripheral Device	USB Port	High	Mitigated	07/23/2017
Man in the browser	Internet Explorer 11	Very High	Mitigated	07/23/2017
Targeted Malware	Internet Explorer 11	Very High	Mitigated	07/23/2017
Account Footprinting	Internet Explorer 11	Very High	Open	07/23/2017
Automation Attack	Internet	Very	Mitigated	07/23/2017

	Explorer 11	High		
Buffer Overflow	Skype	Very High	Mitigated	07/23/2017
Identity Spoofing - Impersonation	Skype	Medium	Mitigated	07/23/2017
Sniffing Attacks	Skype	Medium	Mitigated	07/23/2017
Action Spoofing	Skype	Very High	Mitigated	07/23/2017
Hijacking a Privileged Thread of Execution	Skype	Very High	Mitigated	07/23/2017
Target Programs with Elevated Privileges	Skype	Very High	Mitigated	07/23/2017
Manipulating Input to File System Calls	Skype	Very High	Mitigated	07/23/2017
Privilege Abuse	Skype	Very High	Mitigated	07/23/2017
Privilege Escalation	Skype	Very High	Mitigated	07/23/2017
Weak Identity, Credential and Access Management	Skype	Very High	Mitigated	07/23/2017
Pharming	Outlook 2010	Very High	Open	07/23/2017
Phishing	Outlook 2010	Very High	Mitigated	07/23/2017
Targeted Malware	Outlook 2010	Very High	Mitigated	07/23/2017
Spam	Outlook 2010	Very High	Mitigated	07/23/2017
Buffer Overflow	Office 2010	Very High	Mitigated	07/23/2017
Identity Spoofing - Impersonation	Office 2010	Medium	Mitigated	07/23/2017
Sniffing Attacks	Office 2010	Medium	Mitigated	07/23/2017
Action Spoofing	Office 2010	Very High	Mitigated	07/23/2017
Hijacking a Privileged Thread of Execution	Office 2010	Very High	Mitigated	07/23/2017
Target Programs with Elevated Privileges	Office 2010	Very High	Mitigated	07/23/2017
Manipulating Input to File System Calls	Office 2010	Very High	Mitigated	07/23/2017
Privilege Abuse	Office 2010	Very High	Mitigated	07/23/2017
Privilege Escalation	Office 2010	Very High	Mitigated	07/23/2017
Weak Identity, Credential and Access Management	Office 2010	Very High	Mitigated	07/23/2017

Buffer Overflow	WiFi Access Point	Very High	Mitigated	07/23/2017
Identity Spoofing - Impersonation	WiFi Access Point	Medium	Mitigated	07/23/2017
Sniffing Attacks	WiFi Access Point	Medium	Mitigated	07/23/2017
Action Spoofing	WiFi Access Point	Very High	Mitigated	07/23/2017
Hijacking a Privileged Thread of Execution	WiFi Access Point	Very High	Mitigated	07/23/2017
Target Programs with Elevated Privileges	WiFi Access Point	Very High	Mitigated	07/23/2017
Manipulating Input to File System Calls	WiFi Access Point	Very High	Mitigated	07/23/2017
Privilege Abuse	WiFi Access Point	Very High	Mitigated	07/23/2017
Privilege Escalation	WiFi Access Point	Very High	Mitigated	07/23/2017
Weak Identity, Credential and Access Management	WiFi Access Point	Very High	Mitigated	07/23/2017
Email Injection	Email Server	Medium	Open	07/23/2017
DNS Cache Poisoning	Email Server	Very High	Mitigated	07/23/2017
Phishing	Email Server	Very High	Mitigated	07/23/2017
Targeted Malware	Email Server	Very High	Mitigated	07/23/2017
Spam	Email Server	Very High	Mitigated	07/23/2017
Buffer Overflow	OneDrive	Very High	Mitigated	07/23/2017
Explore For Predictable Temporary File Names	OneDrive	Medium	Mitigated	07/23/2017
Screen Temporary Files for Sensitive Information	OneDrive	Medium	Mitigated	07/23/2017
File Manipulation	OneDrive	Medium	Mitigated	07/23/2017
Accessing, Modifying or Executing Executable Files	OneDrive	Very High	Mitigated	07/23/2017
Create files with the same name as files protected with a higher classification	OneDrive	Very High	Mitigated	07/23/2017
Manipulating Input to File System Calls	OneDrive	Very High	Mitigated	07/23/2017
Session Hijacking	WiFi	Very High	Open	07/23/2017
Man in the Middle Attack	WiFi	Very High	Mitigated	07/23/2017
WiFi Jamming	WiFi	High	Open	07/23/2017

WiFi MAC Address Tracking	WiFi	Very High	Open	07/23/2017
WiFi SSID Tracking	WiFi	Very High	Open	07/23/2017
Denial of Service	WiFi	Very High	Open	07/23/2017
Eavesdropping	WiFi	Very High	Open	07/23/2017
Insecure WiFi Channel	WiFi	Very High	Open	07/23/2017
Exploiting Incorrectly Configured SSL Security Levels	HTTPS	Low	Open	07/23/2017
IMAP and or SMTP Command Injection	SMTP	Medium	Mitigated	07/23/2017
File Manipulation	Windows 7	Medium	Mitigated	07/23/2017
Windows ::DATA Alternate Data Stream	Windows 7	Medium	Open	07/23/2017
Exploiting Incorrectly Configured Access Control Security Levels	Windows 7	Medium	Open	07/23/2017
Exploiting Incorrectly Configured SSL Security Levels	Windows 7	Low	Open	07/23/2017
TCP Window Scan	Windows 7	Low	Mitigated	07/23/2017
Windows Admin Shares with Stolen Credentials	Windows 7	Very High	Open	07/23/2017
Group Permission Footprinting	Windows 7	Very High	Open	07/23/2017
Sniffing Attacks	TCP	Medium	Mitigated	07/23/2017
TCP SYN Scan	TCP	Low	Mitigated	07/23/2017
TCP Window Scan	TCP	Low	Mitigated	07/23/2017
TCP RPC Scan	TCP	Low	Mitigated	07/23/2017
TCP Sequence Number Probe	TCP	Low	Mitigated	07/23/2017
TCP ISN Greatest Common Divisor Probe	TCP	Low	Mitigated	07/23/2017
TCP ISN Counter Rate Probe	TCP	Low	Mitigated	07/23/2017
TCP ISN Sequence Predictability Probe	TCP	Low	Mitigated	07/23/2017
TCP Congestion Control Flag ECN Probe	TCP	Low	Mitigated	07/23/2017
TCP Initial Window Size Probe	TCP	Low	Mitigated	07/23/2017
CVE-2013-3870	Outlook 2010	Very High	Open	07/23/2017
CVE-2013-3905	Outlook 2010	Very High	Open	07/23/2017
CVE-2016-0008	Windows 7	Very High	Open	07/23/2017
CVE-2016-0016	Windows 7	Very High	Open	07/23/2017
CVE-2016-0020	Windows 7	Very High	Open	07/23/2017
Buffer Overflow	Microsoft SharePoint	Very High	Mitigated	03/29/2017

Explore For Predictable Temporary File Names	Microsoft SharePoint	Medium	Mitigated	03/29/2017
Screen Temporary Files for Sensitive Information	Microsoft SharePoint	Medium	Mitigated	03/29/2017
File Manipulation	Microsoft SharePoint	Medium	Mitigated	03/29/2017
Accessing, Modifying or Executing Executable Files	Microsoft SharePoint	Very High	Mitigated	03/29/2017
Create files with the same name as files protected with a higher classification	Microsoft SharePoint	Very High	Mitigated	03/29/2017
Manipulating Input to File System Calls	Microsoft SharePoint	Very High	Mitigated	03/29/2017
Redirect Access to Libraries	Microsoft SharePoint	Very High	Open	03/29/2017
Configuration or Environment Manipulation	Microsoft SharePoint	Medium	Open	03/29/2017
Exploiting Incorrectly Configured Access Control Security Levels	Microsoft SharePoint	Medium	Open	03/29/2017
Exploit Common and or default Usernames and Passwords	Microsoft SharePoint	High	Mitigated	03/29/2017
User-Controlled Filename	Microsoft SharePoint	High	Mitigated	03/29/2017
Manipulating Writeable Configuration Files	Microsoft SharePoint	Very High	Open	03/29/2017
Exploiting Incorrectly Configured SSL Security Levels	Microsoft SharePoint	Low	Open	03/29/2017
Data Interception Attacks	Microsoft SharePoint	Medium	Open	03/29/2017
Dictionary-based Password Attack	Microsoft SharePoint	High	Mitigated	03/29/2017
Password Brute Forcing	Microsoft SharePoint	High	Mitigated	03/29/2017
Password Recovery Exploitation	Microsoft SharePoint	High	Mitigated	03/29/2017
Exploit Common and or default Usernames and Passwords	Microsoft SharePoint	High	Mitigated	03/29/2017
Obtaining Client Secret	Microsoft SharePoint	High	Open	03/29/2017
Sensitive Data Exposure	Microsoft SharePoint	Very High	Open	03/29/2017
Buffer Overflow	Microsoft SharePoint	Very High	Mitigated	03/29/2017
Explore For Predictable Temporary File Names	Microsoft SharePoint	Medium	Mitigated	03/29/2017
Screen Temporary Files for Sensitive Information	Microsoft SharePoint	Medium	Mitigated	03/29/2017

File Manipulation	Microsoft SharePoint	Medium	Mitigated	03/29/2017
Accessing, Modifying or Executing Executable Files	Microsoft SharePoint	Very High	Mitigated	03/29/2017
Create files with the same name as files protected with a higher classification	Microsoft SharePoint	Very High	Mitigated	03/29/2017
Manipulating Input to File System Calls	Microsoft SharePoint	Very High	Mitigated	03/29/2017
Redirect Access to Libraries	Microsoft SharePoint	Very High	Open	03/29/2017
Configuration or Environment Manipulation	Microsoft SharePoint	Medium	Open	03/29/2017
Exploiting Incorrectly Configured Access Control Security Levels	Microsoft SharePoint	Medium	Open	03/29/2017
Exploit Common and or default Usernames and Passwords	Microsoft SharePoint	High	Mitigated	03/29/2017
User-Controlled Filename	Microsoft SharePoint	High	Mitigated	03/29/2017
Manipulating Writeable Configuration Files	Microsoft SharePoint	Very High	Open	03/29/2017
Obtaining Client Secret	Microsoft SharePoint	High	Open	03/29/2017
Sensitive Data Exposure	Microsoft SharePoint	Very High	Open	03/29/2017
Data Interception Attacks	Microsoft SharePoint	Medium	Open	03/29/2017
Data Interception Attacks	Microsoft SharePoint	Medium	Open	03/29/2017
Input Data Manipulation	Microsoft SharePoint	Medium	Open	03/29/2017
Fake the Source of Data	Microsoft SharePoint	Medium	Open	03/29/2017
TCP SYN Scan	Microsoft SharePoint	Low	Mitigated	03/29/2017
TCP Window Scan	Microsoft SharePoint	Low	Mitigated	03/29/2017
TCP RPC Scan	Microsoft SharePoint	Low	Mitigated	03/29/2017
Session Hijacking	Microsoft SharePoint	Very High	Open	03/29/2017
Man in the Middle Attack	Microsoft SharePoint	Very High	Mitigated	03/29/2017
Dictionary-based Password Attack	Microsoft SharePoint	High	Mitigated	03/29/2017
Password Brute Forcing	Microsoft SharePoint	High	Mitigated	03/29/2017
Password Recovery Exploitation	Microsoft	High	Mitigated	03/29/2017

	SharePoint			
Exploit Common and or default Usernames and Passwords	Microsoft SharePoint	High	Mitigated	03/29/2017
Sensitive Data Exposure	Microsoft SharePoint	Very High	Open	03/29/2017
Inducing Account Lockout	Microsoft SharePoint	Medium	Open	03/29/2017
Inducing Account Lockout	Microsoft SharePoint	Medium	Open	03/29/2017
Inducing Account Lockout	Microsoft SharePoint	Medium	Open	03/29/2017
Targeted Malware	Microsoft SharePoint	Very High	Mitigated	03/29/2017
Account Footprinting	Microsoft SharePoint	Very High	Open	03/29/2017
Sensitive Data Exposure	Microsoft SharePoint	Very High	Open	03/29/2017
Lifting credentials and or key material embedded in client distributions - thick or thin	Microsoft SharePoint	Medium	Open	03/29/2017
Sensitive Data Exposure	Microsoft SharePoint	Very High	Open	03/29/2017
Audit Log Manipulation	Microsoft SharePoint	Medium	Open	03/29/2017
Log Injection-Tampering-Forging	Microsoft SharePoint	High	Open	03/29/2017
Encryption Brute Forcing	Microsoft SharePoint	Low	Open	03/29/2017
Software Integrity Attacks	Microsoft SharePoint	Low	Open	03/29/2017
Man in the browser	Microsoft SharePoint	Very High	Mitigated	03/30/2017
Automation Attack	Microsoft SharePoint	Very High	Mitigated	03/30/2017
Identity Spoofing - Impersonation	Microsoft SharePoint	Medium	Mitigated	04/23/2017
Open Redirectors on Client	Microsoft SharePoint	Medium	Open	04/23/2017
Privilege Abuse	Microsoft SharePoint	Very High	Mitigated	04/27/2017
Privilege Escalation	Microsoft SharePoint	Very High	Mitigated	04/27/2017
TCP Sequence Number Probe	Microsoft SharePoint	Low	Mitigated	04/27/2017
TCP ISN Greatest Common Divisor Probe	Microsoft SharePoint	Low	Mitigated	04/27/2017
TCP ISN Counter Rate Probe	Microsoft	Low	Mitigated	04/27/2017

	SharePoint			
TCP ISN Sequence Predictability Probe	Microsoft SharePoint	Low	Mitigated	04/27/2017
TCP Congestion Control Flag ECN Probe	Microsoft SharePoint	Low	Mitigated	04/27/2017
TCP Initial Window Size Probe	Microsoft SharePoint	Low	Mitigated	04/27/2017
Sniffing Attacks	Microsoft SharePoint	Medium	Mitigated	04/27/2017
WiFi Jamming	Microsoft SharePoint	High	Open	05/19/2017
WiFi MAC Address Tracking	Microsoft SharePoint	Very High	Open	05/19/2017
WiFi SSID Tracking	Microsoft SharePoint	Very High	Open	05/19/2017
Insecure WiFi Channel	Microsoft SharePoint	Very High	Open	05/19/2017
Eavesdropping	Microsoft SharePoint	Very High	Open	05/25/2017
Denial of Service	Microsoft SharePoint	Very High	Open	05/25/2017
Privilege Escalation	Microsoft SharePoint	Very High	Mitigated	06/08/2017
Privilege Escalation	Microsoft SharePoint	Very High	Mitigated	06/08/2017
DNS Cache Poisoning	Microsoft SharePoint	Very High	Mitigated	06/12/2017
Denial of Service	Microsoft SharePoint	Very High	Open	06/12/2017
Identity Spoofing - Impersonation	Microsoft SharePoint	Medium	Mitigated	06/12/2017
HTTP Parameter Pollution	Microsoft SharePoint	Very High	Open	06/12/2017
Character Injection	Microsoft SharePoint	Medium	Open	06/12/2017
Using UTF-8 Encoding to Bypass Validation Logic	Microsoft SharePoint	High	Open	06/12/2017
TCP Flood	Microsoft SharePoint	Very High	Mitigated	06/16/2017
TCP SYN Scan	Microsoft SharePoint	Low	Mitigated	06/16/2017
TCP ACK Ping	Microsoft SharePoint	Low	Mitigated	06/16/2017
TCP FIN scan	Microsoft SharePoint	Low	Mitigated	06/16/2017
TCP Null Scan	Microsoft SharePoint	Low	Mitigated	06/16/2017

TCP Window Scan	Microsoft SharePoint	Low	Mitigated	06/16/2017
TCP RPC Scan	Microsoft SharePoint	Low	Mitigated	06/16/2017
TCP Sequence Number Probe	Microsoft SharePoint	Low	Mitigated	06/16/2017
TCP ISN Greatest Common Divisor Probe	Microsoft SharePoint	Low	Mitigated	06/16/2017
TCP ISN Counter Rate Probe	Microsoft SharePoint	Low	Mitigated	06/16/2017
TCP ISN Sequence Predictability Probe	Microsoft SharePoint	Low	Mitigated	06/16/2017
TCP Congestion Control Flag ECN Probe	Microsoft SharePoint	Low	Mitigated	06/16/2017
TCP Initial Window Size Probe	Microsoft SharePoint	Low	Mitigated	06/16/2017
Sniffing Attacks	Microsoft SharePoint	Medium	Mitigated	06/16/2017
Targeted Malware	Microsoft SharePoint	Very High	Mitigated	06/16/2017
Manipulate Data Structures	Microsoft SharePoint	Very High	Open	07/07/2017
Manipulate Data Structures	Microsoft SharePoint	Very High	Open	07/07/2017