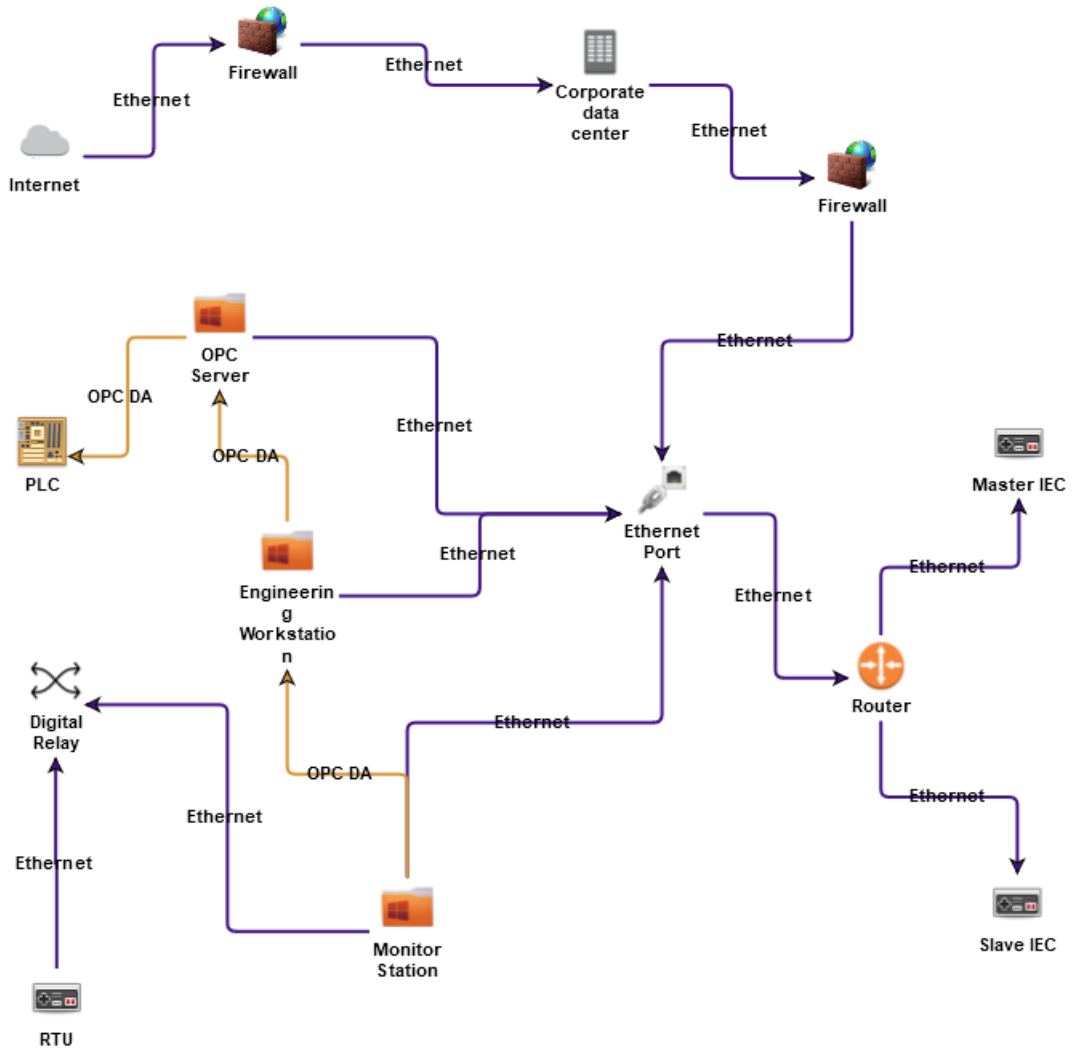
ThreatModeler
Identify • Classify • Prioritize • Mitigate

Electrical Substation ICS - 2

04/11/2018

Threat Model



Description

Threats

Threat	Source	Risk	Status	Date Created
Overflow Buffers	Engineering Workstation	Very High	Open	03/22/2018
Overread Buffers	Engineering Workstation	Very High	Open	03/22/2018
Denial of Service	Engineering Workstation	Very High	Open	03/22/2018
Overflow Buffers	Monitor Station	Very High	Open	03/22/2018
Overread Buffers	Monitor Station	Very High	Open	03/22/2018
Denial of Service	Monitor Station	Very High	Open	03/22/2018
Overflow Buffers	Digital Relay	Very High	Open	03/22/2018
Overread Buffers	Digital Relay	Very High	Open	03/22/2018
Denial of Service	Digital Relay	Very High	Open	03/22/2018
Overflow Buffers	OPC Server	Very High	Open	03/22/2018
Overread Buffers	OPC Server	Very High	Open	03/22/2018
Denial of Service	OPC Server	Very High	Open	03/22/2018
Overflow Buffers	OPC DA	Very High	Open	03/22/2018
Subverting Environment Variable Values	OPC DA	Very High	Open	03/22/2018
Encryption Brute Forcing	OPC DA	Low	Open	03/22/2018
Man in the Middle Attack	OPC DA	Very High	Open	03/22/2018
Weak Identity, Credential and Access Management	OPC DA	Very High	Open	03/22/2018
Identity Spoofing - Impersonation	Internet	Medium	Open	03/22/2018
Man in the Middle Attack	Internet	Very High	Open	03/22/2018
Targeted Malware	Internet	Very High	Open	03/22/2018
Account Footprinting	Internet	Very High	Open	03/22/2018

Create files with the same name as files protected with a higher classification	Internet	Very High	Open	03/22/2018
Exploiting Incorrectly Configured Access Control Security Levels	Internet	Medium	Open	03/22/2018
Exploit Common or default Usernames and Passwords	Internet	High	Open	03/22/2018
User-Controlled Filename	Internet	High	Open	03/22/2018
Manipulating Writeable Configuration Files	Internet	Very High	Open	03/22/2018
Email Injection	Internet	Medium	Open	03/22/2018
DNS Cache Poisoning	Internet	Very High	Open	03/22/2018
Phishing	Internet	Very High	Open	03/22/2018
SPAM	Internet	Medium	Open	03/22/2018
Sensitive Data Exposure	Internet	Very High	Open	03/22/2018
HTTP DoS	Internet	Very High	Open	03/22/2018
Weak Identity, Credential and Access Management	Internet	Very High	Open	03/22/2018
DDOS	Internet	Very High	Open	03/22/2018
Malicious Software Download	OPC Server	Very High	Open	03/22/2018
Verify - Insecure Configuration	OPC Server	Very High	Open	03/22/2018
Malicious Software Download	Digital Relay	Very High	Open	03/22/2018
Malicious Software Download	RTU	Very High	Open	03/22/2018
Malicious Software Download	Master IEC	Very High	Open	03/22/2018
Malicious Software Download	Slave IEC	Very High	Open	03/22/2018
Malicious Software Download	PLC	Very High	Open	03/22/2018
Malicious Software Download	Engineering Workstation	Very High	Open	03/22/2018
Verify - Insecure Configuration	Engineering Workstation	Very High	Open	03/22/2018
CVE-2014-9369	PLC	Very High	Open	03/22/2018

CVE-2000-1227	OPC Server	Very High	Open	03/22/2018
CVE-2001-0341	OPC Server	Very High	Open	03/22/2018
CVE-2001-1452	OPC Server	Very High	Open	03/22/2018
CVE-2002-0366	OPC Server	Very High	Open	03/22/2018
CVE-2002-0693	OPC Server	Very High	Open	03/22/2018
CVE-2002-0694	OPC Server	Very High	Open	03/22/2018
CVE-2002-0724	OPC Server	Very High	Open	03/22/2018
CVE-2002-0862	OPC Server	Very High	Open	03/22/2018
CVE-2002-0863	OPC Server	Very High	Open	03/22/2018
CVE-2002-1257	OPC Server	Very High	Open	03/22/2018
CVE-2002-1258	OPC Server	Very High	Open	03/22/2018
CVE-2002-1260	OPC Server	Very High	Open	03/22/2018
CVE-2002-1325	OPC Server	Very High	Open	03/22/2018
CVE-2002-1561	OPC Server	Very High	Open	03/22/2018
CVE-2003-0003	OPC Server	Very High	Open	03/22/2018
CVE-2003-0010	OPC Server	Very High	Open	03/22/2018
CVE-2003-0112	OPC Server	Very High	Open	03/22/2018
CVE-2003-0345	OPC Server	Very High	Open	03/22/2018
CVE-2003-0352	OPC Server	Very High	Open	03/22/2018
CVE-2003-0525	OPC Server	Very High	Open	03/22/2018
CVE-2003-0528	OPC Server	Very High	Open	03/22/2018
CVE-2003-0659	OPC Server	Very	Open	03/22/2018

		High		
CVE-2003-0660	OPC Server	Very High	Open	03/22/2018
CVE-2003-0661	OPC Server	Very High	Open	03/22/2018
CVE-2003-0711	OPC Server	Very High	Open	03/22/2018
CVE-2003-0715	OPC Server	Very High	Open	03/22/2018
CVE-2003-0717	OPC Server	Very High	Open	03/22/2018
CVE-2003-0813	OPC Server	Very High	Open	03/22/2018
CVE-2003-0818	OPC Server	Very High	Open	03/22/2018
CVE-2003-0825	OPC Server	Very High	Open	03/22/2018
CVE-2004-0201	OPC Server	Very High	Open	03/22/2018
CVE-2004-0210	OPC Server	Very High	Open	03/22/2018
CVE-2004-0567	OPC Server	Very High	Open	03/22/2018
CVE-2004-0568	OPC Server	Very High	Open	03/22/2018
CVE-2004-0571	OPC Server	Very High	Open	03/22/2018
CVE-2004-0893	OPC Server	Very High	Open	03/22/2018
CVE-2004-0899	OPC Server	Very High	Open	03/22/2018
CVE-2004-0900	OPC Server	Very High	Open	03/22/2018
CVE-2004-0901	OPC Server	Very High	Open	03/22/2018
CVE-2004-1080	OPC Server	Very High	Open	03/22/2018
CVE-2004-1305	OPC Server	Very High	Open	03/22/2018
CVE-2004-1306	OPC Server	Very High	Open	03/22/2018
CVE-2004-1361	OPC Server	Very High	Open	03/22/2018

CVE-2005-0050	OPC Server	Very High	Open	03/22/2018
CVE-2005-0416	OPC Server	Very High	Open	03/22/2018
CVE-2005-1184	OPC Server	Very High	Open	03/22/2018
CVE-2005-1935	OPC Server	Very High	Open	03/22/2018
CVE-2006-0010	OPC Server	Very High	Open	03/22/2018
CVE-2006-0034	OPC Server	Very High	Open	03/22/2018
CVE-2006-1184	OPC Server	Very High	Open	03/22/2018
CVE-2006-1591	OPC Server	Very High	Open	03/22/2018
CVE-2006-2379	OPC Server	Very High	Open	03/22/2018
CVE-2008-4609	OPC Server	Very High	Open	03/22/2018