Best Practices in Cybersecurity for Utilities Vendor Taxonomy (Topics and Companies)

Shining a light on Best Practice Cyber and Physical security for U.S. and Canadian Electric and Natural Gas Utilities – moving to a Culture of Resilience

https://www.protectourpower.com/best-practices/pop-bp-taxonomy.pdf

Purple links are internal to this document; blue links are to external documents or sites.

Introduction:

There are about 1000 companies selling cyber security product to the Utilities in the U.S. and Canada. That is a daunting number to consider on the buying end of the equation, and a highly competitive market on the product and services end. Competition is heightened by high demand and fairly low barriers to entry. The Protect Our Power's Best Practices Project is directed at organizing and analyzing these vendors to make it easier for the Utilities to make good decisions and to pursue Best Practices as defined in the Project.

The Taxonomy included here is an attempt to define meaningful Topics under the broad heading of "Cybersecurity." In general, a Topic relates to a Utility decision area – a Utility would consider addressing the Topic via analyzing the Vendors that can address the Topic/Cybersecurity need. From a Vendor standpoint, Topics are homogeneous within and heterogeneous between (at least that is the intent).

The following is a list of Topics that already have an associated University that is developing the Work Products associated with this Project with links to the Protect Our Power Website for the Educational Institutions:

1. ***George Mason University*** – Remote Access
2. ***Illinois Institute of Technology*** – *Data Protection and Encryption*
3. ***Louisiana Tech University*** – *Social Engineering Protection*
4. ***Michigan Tech*** – *Risk Assessment and Quantification*
5. ***Northeastern University*** – *Identity Access Management*
6. ***Prince Georges Community College*** – *Network Access Control*
7. ***Rutgers University*** – Antivirus

8. ***Sacred Heart University*** (PoP page awaiting Agreement for publication) – DDoS Attack Prevention
9. ***University of Houston*** – Network Segmentation
10. ***University of New Hampshire*** – Threat Intelligence
11. ***University of North Carolina – Charlotte*** – Monitoring of IT/Enterprise Networks in real-time
12. ***Washington State University*** – Monitoring of ICS/OT Networks

We recognize this Taxonomy is incomplete and welcome all suggestions for updating or participation in building a more appropriate Taxonomy. Comments and suggestions can be sent to Paul.Feldman@ProtectOurPower.org

Go to **Topics related to Cybersecurity – showing Vendors addressing each Topic - Table of Contents**

Go to ***Vendor List showing Topics addressed by each Vendor***

Go to ***Vendors offering cybersecurity product(s), but not either focused, available, or interested in the North American Utility Market***

Go to ***Additional Resources***

Go to ***Notes Related to This Taxonomy and Further Development***

Contact

Erick Ford | Project Manager
eford@protectourpower.org

Topics related to Cybersecurity – showing Vendors addressing each Topic
Table of Contents

https://www.protectourpower.org/best-practices/pop-bp-taxonomy.pdf

Links colored purple are internal to this document; links colored blue are to external resources; links colored red are internal to this document, but are Topics where an Educational Institution is developing materials to support moving to Best Practices.

[1] a computer security technology for removing potentially malicious code from files. Unlike malware analysis, CDR technology does not determine or detect malware's functionality but removes all file components that are not approved within the system's definitions and policies.

14. ***Data Protection and Encryption*** – Illinois Institute of Technology has undertaken an analysis of Vendors for this Topic (PoP page coming soon).
15. ***Data Sources*** –
16. ***Data Visualization*** –
17. ***Deception Technology*** –
18. ***DDos Attack Protection*** – Sacred Heart University (PoP page coming soon) has undertaken an analysis of Vendors for this Topic).
19. ***Deep Web, Dark Web*** –

    Defense in Depth – See various other elements of the Taxonomy

    DevOps Best Practices – see "Software Development / Inspection / Management"

20. ***Digital Certificates*** –
21. ***Digital Risk Protection*** -

    Distributed Energy – Solar Farms – See "Generation Solar"

    Distributed Energy – Wind Farms – See "Generation Wind"

ToC

22. ***Drone Attack Defense*** –
23. ***Education for Employees*** -

    Email Focused Security – see Phishing -

    Employee Education – see "Education for Employees"

24. ***EMS Protection (In a Balancing Authority)*** –
25. ***Endpoint Detection & Response*** [2]-

    Endpoint Encryption – see "Encryption"

26. ***Endpoint Protection Platforms (EPPs)*** [3]-
27. ***File Integrity*** –

    Firewalls – see "Network Segmentation"

    Firmware – see "Patching"

28. ***Frameworks and Controls*** –
29. ***Generation – Central Station*** –
30. ***Generation – Solar*** –
31. ***Generation – Wind*** -
32. ***Governance, Risk Management and Compliance (GRC) Platforms*** –

    Host-Based Intrusion Detection Systems (HIDS) [4]– see Antivirus

    Host-Based Intrusion Detection Systems (HIDS) – see Monitoring Devices and Hosts

    Host-Based Intrusion Detection Systems (HIDS) – see Monitoring Electric and Analog Signals

[2] a cyber-security solution that differs from other endpoint protection platform (EPP) for instance antivirus and anti-malware, where the major focus isn't to automatically stop threats in pre-execution phase on an endpoint. EDR is more focused on providing overall endpoint visibility with the right insights, which help security analysts to investigate and respond to a very advanced threat. This category deals with Enterprise IT endpoints, not ICS/OT endpoints.

[3] An Endpoint Protection Platform (EPP) is an integrated security solution designed to detect and block threats at device level. Typically, this includes antivirus, anti-malware, data encryption, personal firewalls, intrusion prevention (IPS) and data loss prevention (DLP). Traditional EPP is inherently preventative, and most of its approaches are signature-based – identifying threats based on known file signatures for newly discovered threats. The latest EPP solutions have however evolved to utilize a broader range of detection techniques.

[4] Wikipedia – Host-Based Intrusion Detection Systems - https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

33. ***Identity Access Management and Governance*** – Northeastern University has undertaken an analysis of Vendors for this Topic.
34. ***Incident Response*** –
35. ***Information Sharing*** –
36. ***Insider Threats*** -
37. ***Internet of Things (IoT)*** -

Intrusion Detection Systems [5]– see Monitoring Electric and Analog Signals
Intrusion Detection Systems – see Monitoring Enterprise/IT Networks
Intrusion Detection Systems – see Monitoring OT/ICS Networks
IT/Enterprise Real-Time Network Monitoring – see "Monitoring IT/Enterprise Networks in real-time"
Level 0 Devices within the Purdue Reference Architecture – see "Monitoring Electric and Analog Signals in real-time"

38. ***Log Management*** –
39. ***Managed Services (MSSPs)*** –

ToC

40. ***Monitoring Devices and Hosts*** -
41. ***Monitoring Electric and Analog Signals*** - the real-time capability to monitor operations (pumps, boilers, etc.) at Purdue level 0

Monitoring – Enterprise IT Networks and Endpoints – see Endpoint Detection & Response

42. ***Monitoring ICS/OT Networks in real-time*** - the real-time capability to monitor ICS networks and underlying assets in passive and active modes. Washington State University has undertaken an analysis of Vendors for this Topic.
43. ***Monitoring IT/Enterprise Networks in real-time*** - the real-time capability to monitor IT/Enterprise Networks and underlying devices. The University of North Carolina Charlotte has undertaken an analysis of Vendors for this Topic.
44. ***Network Access Control (NAC)*** – Network Access Control (NAC) is an approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement. Prince Georges Community College has undertaken an analysis of Vendors for this Topic.

Network Intrusion Detection Systems (NIDS) – see Monitoring Enterprise/IT Networks
Network Intrusion Detection Systems (NIDS) – see Monitoring OT/ICS Networks

45. ***Network Segmentation*** – The University of Houston has undertaken an analysis of Vendors for this Topic.
46. ***Organizational Best Practices*** – addressing culture, organizational structure, positions, reporting relationships, etc.
47. ***Patch and Firmware Management*** –
48. ***Penetration Testing*** –

Phishing – see "Social Engineering"

49. ***Portable Media*** –

Privileged Remote Access – see "Remote Access"

50. ***Remote Access*** – George Mason University has undertaken an analysis of Vendors for this Topic.

Removable Media – see Portable Media above

51. ***Risk Assessment and Quantification, and Management*** – Michigan Technical Institute has undertaken an analysis of Vendors for this Topic.
52. ***Sandboxing*** -

ToC

[5] Wikipedia – Intrusion Detection Systems - https://en.wikipedia.org/wiki/Intrusion_detection_system

53. ***SCADA Protection*** –
    Secure Remote Access - see Privileged Remote Access Solutions
54. ***Security Analytics Platforms*** -
    Security Awareness in the Workforce – see Training Security Awareness
55. ***Security Information and Event Managers (SIEMs)*** –
56. ***Security Investment Prudency (at the state level)*** – at the state level, what are the Best Practices states are following to approve/deny/evaluate security investments
57. ***Security Operations Centers (SOCs)*** -
58. ***Security orchestration automation and response (SOAR)*** -
59. ***Situational Awareness*** –
    SMShing – see "Social Engineering"
60. ***Social Engineering*** - Louisiana Tech University has undertaken an analysis of Vendors for this Topic (PoP page coming soon).
61. ***Software Development / Inspection / Management*** –
    Segmentation – see "Network Segmentation"
    Spear-Phishing – see "Social Engineering"
62. ***State Cybersecurity Standards and Best Practices*** –
63. ***Substations, Distribution*** –
64. ***Substations, Transmission*** -
65. ***Supply Chain*** –
66. ***Tabletop Exercises / Wargaming*** – ToC
67. ***Threat Intelligence*** – The University of New Hampshire has taken this Topic.
    Threat Intelligence Platforms – see "Threat Intelligence" above
    Threat Vulnerability Assessment – see "Risk Assessment and Quantification, and Management"
68. ***Training – Security-Awareness in the workforce*** –
69. ***Training – Cyber Workforce Development*** -
70. ***Transient Cyber Assets*** –
    USB Devices – see Portable Media above
71. ***Virtualization*** –
    Vishing – see "Social Engineering"
72. ***VPN Security*** –
    Vulnerability Assessment – see "Risk Assessment and Quantification, and Management"
73. ***WAN Edge Infrastructure*** -
74. ***Web Application Firewalls (WAF)*** -
75. ***Whitelisting*** –
    Wireless – see "Communications Systems – Wireless" above
76. ***Zero Trust*** -

Access Management – see Identity Access Management and Analysis below

1. ***Advanced Persistent Threat (APT) Protection*** [6] – ToC
   - **1.1.** ***Barracuda*** - https://www.barracuda.com/solutions - Targeted industries do not include Utilities/Energy.
   - **1.2.** ***Cisco Systems*** – https://www.cisco.com -
   - **1.3.** ***FireEye*** - https://www2.fireeye.com/stop-advanced-persistent-threats-today.html
   - **1.4.** ***Forcepoint*** - https://www.forcepoint.com/product/cloud-security/forcepoint-advanced-malware-detection
   - **1.5.** ***Fortinet*** - https://www.fortinet.com/solutions/enterprise-midsize-business/advanced-threat-protection.html
   - **1.6.** ***Kaspersky Lab*** - https://usa.kaspersky.com/enterprise-security/apt-intelligence-reporting
   - **1.7.** ***McAfee*** - https://www.mcafee.com/enterprise/en-us/products/advanced-threat-defense.html
   - **1.8.** ***Microsoft*** - https://www. microsoft.com/en-us/windowsforbusiness/windows-atp
   - **1.9.** ***Owl*** - http://library.owlcyberdefense.com/opds-100/page/1
   - **1.10.** ***Palo Alto Networks*** - https://www.paloaltonetworks.com/
   - **1.11.** ***Symantec*** - https://www.symantec.com/products/advanced-threat-protection
   - **1.12.** ***Webroot*** - https://www.webroot.com/us/en/business/smb/endpoint-protection

   Analog Signal Monitoring – see "Monitoring Electric and Analog Signals"
2. ***Antivirus*** [7] [8] – Ruggers University has taken this Topic (POP page coming soon). **1/5** partial list ToC
   - **2.1.** ***Carbon Black*** -
   - **2.2.** ***Cylance*** - https://www.cylance.com -
   - **2.3.** ***McAfee*** – https://www.mcafee.com -
   - **2.4.** ***Symantec*** – https://www.symantec.com –
   - **2.5.** ***Verve*** -

   Application Whitelisting – see Whitelisting below
3. ***Application Control*** [9] [10]– ToC
   - **3.1.** ***Carbon Black*** -
4. ***Attacker Capability*** -

   Authentication – see Identity Access Management and Analysis below
5. ***Building Automation Systems*** –
   - **5.1.** ***FoxGuard Solutions*** **-** *https://foxguardsolutions.com/bas/* **-**
6. ***Change Management and Ticketing***
   - **6.1.** ***ServiceNow*** – https://www.servicenow.com -
   - **6.2.** ***bmcRemedy*** – http://www.bmc.com -

[6] Radicati Market Quadrant - https://www.EnergyCollection.us/Companies/Radicati/MQ-APT-2018.pdf

[7] Recommended Practice: Updating Antivirus in an Industrial Control Systems (from DHS NCCIC) - https://tinyurl.com/ybdcuywo

[8] Comparison of Antivirus Software - https://en.wikipedia.org/wiki/Comparison_of_antivirus_software

[9] What is Application Control? Definition, Best Practices & More - https://digitalguardian.com/blog/what-application-control

[10] Application Control vs. Application Whitelisting - https://www.airlockdigital.com/application-control-vs-application-whitelisting/

7. Cloud Security and Services [11] [12] [13]

7.1. **Alert Logic** – https://www.alertlogic.com –
7.2. **Bitglass** - https://www.bitglass.com/
7.3. **Blue Coat** – Now Symantec - https://www.symantec.com/ https://en.wikipedia.org/wiki/Blue_Coat_Systems
7.4. **CensorNet** - https://www.censornet.com/products/cloud-application-security/ -
7.5. **Cisco** - https://www.cisco.com/c/en/us/products/security/cloud-security/index.html -
7.6. **CypherCloud** - https://www.ciphercloud.com/ -
7.7. **Elastic** - https://www.elastic.co/
7.8. **FireLayers** – acquired by Proofpoint - https://en.wikipedia.org/wiki/Proofpoint,_Inc. https://tinyurl.com/hbtebzn
7.9. **Forcepoint** - https://www.forcepoint.com/ -
7.10. **Lastline** - https://www.lastline.com/use-cases/
7.11. **Leidos** – https://cyber.leidos.com/services/cloud-deployed-devices -
7.12. **McAfee** – https://www.mcafee.com/enterprise/en-us/solutions/fearless-innovation.html -
7.13. **Microsoft** - https://www.microsoft.com/en-us/cybersecurity/content-hub/cloud-security - ToC
7.14. **Netscope** - https://www.netskope.com/
7.15. **OpenDNS** – https://www.opendns.com
PerspecSys – Acquired by Blue Coat - https://tinyurl.com/yc66qs67 https://en.wikipedia.org/wiki/Perspecsys
7.16. **Outpost24** - https://outpost24.com/
7.17. **Oracle** – https://www.oracle.com/security/ -
7.18. **Palo Alto Networks** - https://www.paloaltonetworks.com/cyberpedia/cloud-security
7.19. **Proofpoint** - https://www.proofpoint.com/us
7.20. **Qualys** - https://www.qualys.com/cloud-platform/
7.21. **Saviynt** - https://saviynt.com/ -
7.22. **StackRox** - https://www.stackrox.com/
7.23. **Symantec** - https://www.symantec.com/ -
7.24. **Trend Micro** – https://www.trendmicro.com/en_us/business.html -
7.25. **Unity Technology** -
7.26. **Zscaler** - https://www.zscaler.com

8. Compliance [14] – ToC

8.1. **AlienVault** -
8.2. **Archer Energy Solutions** - http://www.archersecuritygroup.com/
8.3. **AssurX** - https://www.assurx.com/energy-utilities/
8.4. **Axway** – https://www.axway.com/en#
8.5. **BlackStratus** – https://www.blackstratus.com -
8.6. **Check Point** - https://www.checkpoint.com/products/security-compliance/

[11] Gartner MQ for Cloud Access Security Brokers - https://www.EnergyCollection.us/Companies/Gartner/MQ-CASB-2018.pdf https://www.EnergyCollection.us/Companies/Gartner/MQ-CASB-2019.pdf

[12] Forrester Wave: Cloud-Security-Gateways-2019 - https://www.EnergyCollection.us/Companies/Forrester/Wave-Cloud-Security-2019.pdf

[13] Critical Capabilities for Cloud Access Security Brokers – a 2019 Gartner publication - https://www.EnergyCollection.us/Companies/Gartner/Critical-Capabilities-Cloud.pdf

[14] Assured Compliance Assessment Solution - https://www.disa.mil/cybersecurity/network-defense/acas

8.7. ***D3 Security*** - https://d3security.com/industries/energy-utilities/

8.8. ***EnergySec*** – https://www.energysec.org/

8.9. ***Intellibind*** – http://www.intellibind.com/

netForensics – now BlackStratus – https://tinyurl.com/yaulcmj9

8.10. ***Network Perception*** - https://www.network-perception.com/

8.11. ***Network & Security Technology*** – http://www.netsectech.com

8.12. ***Qualys*** – https://www.qualys.com

8.13. ***Quanexus*** – https://quanexus.com –

8.14. ***Proven Compliance Solutions*** - http://provencompliance.com/web/

8.15. ***RedSeal*** - https://www.redseal.net/industries/utilities/

8.16. ***SailPoint*** - https://www.sailpoint.com/blog/auditable-compliance-nerc/

SecureState – acquired by RSM - https://tinyurl.com/yd3hm23v

8.17. ***SUBNET*** – http://www.subnet.com/news-events/white-papers/unified-ied-management-solution-whitepaper.aspx

8.18. ***Tenable (Nessus)*** - https://tinyurl.com/y9j2um9x

8.19. ***Tripwire*** - https://www.tripwire.com

9. ***Communications Systems*** –

ToC

9.1. ***Broadcom*** - https://www.broadcom.com/applications/industrial-automotive/solar-power

9.2. ***iS5 Communications*** - https://is5com.com/about/

9.3. ***Pwnie Express*** - https://www.pwnieexpress.com/pulse

9.4. ***RAD*** - https://www.rad.com/solutions/critical-infrastructure-communications

10. ***Communications Systems – Wireless*** -

10.1. ***Perspecta Labs*** - https://www.perspectalabs.com/securesmart-cmaas

11. ***Consultants*** –

11.1. ***Accenture*** – https://www.accenture.com/us-en/security-index -

Accuvant (now Optiv) -

11.2. ***Anfield Group*** – https://theanfieldgroup.com/cyber-physical-security-2 -

11.3. ***ARC Advisory Group*** – https://www.arcweb.com/blog/cybersecurity-viewpoints -

11.4. ***Archer Energy Solutions*** – http://www.archersecuritygroup.com -

11.5. ***Atos*** – https://atos.net/en/solutions/cyber-security -

11.6. ***AT&T*** – https://www.business.att.com/categories/cybersecurity-consulting-services.html -

11.7. ***Booz Allen Hamilton*** – https://www.boozallen.com/expertise/cybersecurity.html -

11.8. ***BT*** – https://www.globalservices.bt.com/en -

11.9. ***Corporate Risk*** – https://www.rcpholdings.com/cyber-technology-eo-risk -

11.10. ***Dell*** – https://www.dellemc.com/en-us/solutions/data-protection/isolated-recovery-solution.htm -

11.11. ***Deloitte*** – https://www2.deloitte.com/cy/en/pages/risk/solutions/cyber-security-services.html -

11.12. ***EmeSec*** – https://www.emesec.net -

Encari (acquired by PowerSecure) –

11.13. ***EnergySec*** – https://www.energysec.org -

11.14. ***EY*** – https://www.ey.com/gl/en/services/advisory/ey-cybersecurity -

Fishnet Security (now part of Optiv) –

11.15. ***FoundStone*** – https://en.wikipedia.org/wiki/Foundstone -

11.16. ***Gartner Group*** – https://www.gartner.com/en/information-technology/insights/cybersecurity -

ToC

11.17. ***GeNUA*** – https://www.genua.de/en.html

11.18. ***Grimm*** - https://www.grimm-co.com/

11.19.IBM – https://www.ibm.com/security/services/cyber-security-consulting-for-active-threats -

11.20.ICF International – https://www.ibm.com/security/services/cyber-security-consulting-for-active-threats -

11.21.Insight Cyber – https://www.insightcybergroup.com -

11.22.IPsecure - http://www.ipsecureinc.com -

11.23.Hewlett Packard – https://www.hpe.com/us/en/services/consulting/security.html -

11.24.KPMG – https://home.kpmg.com/xx/en/home/services/advisory/risk-consulting/cyber-security-services/cyber-defense.html -

11.25.Kratos - http://www.kratossecureinfo.com -

11.26.NCI Security – https://www.ncisecurity.com -

11.27.NEC – https://www.nec.com/en/global/solutions/cybersecurity/index.html -

11.28.Optiv Security – Accuvant and Fishnet Security Are Now Optiv - https://www.optiv.com -

11.29.Ponemon – https://www.ponemon.org -

11.30.PowerSecure - https://powersecure.com -

Premier Alliance (now part of Route9B) –

11.31.Protiviti – https://www.protiviti.com/US-en/technology-consulting/cybersecurity -

11.32.PwC – https://www.pwc.com/gx/en/services/advisory/forensics/cyber-security.html -

Rkneal Engineering (now Verve Industrial Protection) –

11.33.Route9B – https://www.root9b.com -

11.34.Saint Corporation - http://www.saintcorporation.com -

11.35.SCADAhacker – https://www.scadahacker.com -

Scitor (now part of SAIC) – http://www.saic.com/what-we-do/information-technology/cyber -

11.36.Securicon - https://www.securicon.com/

11.37.Sisco – http://www.siscocorp.com –

11.38.ThreatGEN – https://threatgen.com -

11.39.UtiliSec – acquired by InGuardians

11.40.Verve - http://verveindustrial.com/ot-cyber -

11.41.VioPoint – http://www.viopoint.com -

12.Content Disarm & Reconstruction (CDR) [15]-

ToC

12.1. Check Point –

12.2. Deep Secure –

12.3. Fortinet –

12.4. Glasswall Solutions –

12.5. Jiransecurity –

12.6. Net at Work –

12.7. Peraton (Purifile) –

12.8. ReSec –

12.9. ODI-X –

12.10.OPSWAT –

12.11.Resec –

12.12.SASA Software (Gate Scanner CDR) –

12.13.Softcamp –

12.14.Votiro (Disarmer) –

[15] Wikipedia article with vendor listing - https://en.wikipedia.org/wiki/Content_Disarm_%26_Reconstruction

12.15. YazamTech -

Dark Web & Deep Web Monitoring – see "Deep Web…" below

13. Dashboards and Analysis – ToC

BrightPoint Security – acquired by ServiceNow - https://tinyurl.com/ya75tpey

13.1. Cytegic – http://www.cytegic.com

13.2. Digital Shadows – https://www.digitalshadows.com/

13.3. Palo Alto Networks – https://www.paloaltonetworks.com/

13.4. ServiceNow - https://www.servicenow.com

13.5. Skybox Security – https://www.skyboxsecurity.com/

13.6. Swimlane – https://swimlane.com/

14. Data Protection and Encryption [16] [17] [18] - Illinois Institute of Technology has undertaken an analysis of Vendors for this Topic (PoP page coming soon). **01/38** ToC

14.1. ABB - https://new.abb.com/safety

14.2. Aclara - https://www.aclara.com/products-and-services/communications-networks/twacs-plc/

14.3. Amazon Web Services - https://aws.amazon.com

14.4. BEA Systems - https://www.baesystems.com/en-us/product/cyber-r-d

14.5. Black & Veatch - https://www.bv.com/

14.6. DellEMC - www.dellemc.com

14.7. Digital Guardian - https://digitalguardian.com

14.8. Fortress - https://www.fortressinfosec.com/a2v/

14.9. GE - https://www.ge.com/security

14.10. Google Cloud - https://cloud.google.com

14.11. IBM - https://www.ibm.com/expressadvantage/br/downloads/The_IBM_Solution_Architecture_for_Energy_and_Utilities_Framework.pdf

14.12. IOActive - https://ioactive.com/service/security-team-development/

14.13. Itron - https://www.itron.com/na/solutions/what-we-enable/meter-data-management

14.14. Mcafee - www.mcafee.com

14.15. Microfocus - https://www.microfocus.com/en-us/solutions/data-security-encryption

14.16. Microsoft Azure Information Protection - https://azure.microsoft.com/en-us/services/information-protection

14.17. Opower (Oracle Corporation) - https://www.oracle.com/corporate/acquisitions/opower/

Oracle – see "Opower (Oracle Corporation)' above

14.18. Protegrity - https://www.protegrity.com

14.19. Qubitekk – http://qubitekk.com

14.20. Schneider Electric - https://www.se.com/us/en/work/solutions/for-business/data-centers-and-networks/

14.21. Siemens - https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/grid-applications/energyip.html

14.22. Stealthbits - https://www.stealthbits.com

14.23. Spirion - https://www.spirion.com

[16] Topic Description and Discussion – https://cultureofresilience/pop-bp-t-data-protection.pdf

[17] Top Endpoint Encryption Technology Vendors - https://www.EnergyCollection.us/Energy-Security/Top-Endpoint-Encryption-Technology-Vendors.pdf

[18] See also "Digital Certificates"

- ***14.24.Symantec*** – https://www.symantec.com/products/encryption / https://www.broadcom.com/solutions/data-center/data-center-solutions
- ***14.25.Tenable*** - https://www.tenable.com/solutions/energy
- ***14.26.Thales eSecurity*** - https://www.thalesesecurity.com
- ***14.27.TrendMicro*** –
- ***14.28.Varonis*** - https://www.varonis.com

15.Data Sources –

ToC

- ***15.1. Blue Heron*** –
- ***15.2. DomainTools*** –
- ***15.3. Farsight Security*** –
- ***15.4. Financial Services Affiliate*** –
- ***15.5. iSIGHT Partners*** –
- ***15.6. Malcovery*** –
- ***15.7. National Cyber Watch*** –
- ***15.8. OpenDNS*** –
- ***15.9. Wapack Labs*** –

16.Data Visualization

- ***16.1. Malformity Labs*** –

17.Deception Technology

- ***17.1. AttivonNetworks*** - https://attivonetworks.com
- ***17.2. TrapX*** - http://prnewswire.sys-con.com/node/4356829 / https://trapx.com/industries/manufacturing-scada/

18.DDoS Attack Protection – Sacred Heart University (POP page coming soon) is doing an analysis of Vendors for this Topic. **00/13** partial list

ToC

- ***18.1. Akamai*** - https://www.akamai.com/us/en/resources/ddos-protection.jsp
- ***18.2. AppTrana*** - https://apptrana.indusface.com/managed-ddos-protection-mitigation/
- ***18.3. AWS Shield*** - https://aws.amazon.com/shield/
- ***18.4. Cloud Armor*** - https://cloud.google.com/armor/
- ***18.5. Cloudflare*** - https://www.cloudflare.com/ddos/
- ***18.6. Imperva*** - https://www.imperva.com/learn/application-security/ddos-attacks/
- ***18.7. Incapsula*** - https://www.incapsula.com/ddos-protection-services.html
- ***18.8. Link11*** - https://www.link11.com/en/
- ***18.9. Netscout*** - https://www.netscout.com/arbor-ddos
- ***18.10.Perspecta Labs*** - https://www.perspectalabs.com/cybersecurity-research
- ***18.11.SiteLock*** - https://sitelock.p5ld.net/bB52M
- ***18.12.StackPath*** - https://tracking.stackpath.com/OWZzK
- ***18.13.Sucuri*** - https://sucuri.net/ddos-protection/

19.Deep Web, Dark Web [19] –

ToC

- ***19.1. Cyber Edge*** –
- ***19.2. Flashpoint*** –
- ***19.3. Hold Security*** - https://holdsecurity.com/services/deep-web-monitoring
- ***19.4. Intsights*** - https://www.intsights.com/solutions-use-case-dark-web-monitoring
- ***19.5. Ipswitch*** - https://blog.ipswitch.com/deep-web-monitoring-future-data-breach-detection
- ***19.6. KELA*** –
- ***19.7. Massive*** - https://www.massivealliance.com
- ***19.8. SpyCloud*** - https://spycloud.com/do-dark-web-monitoring-tools-work

[19] Scan the dark web for threat intelligence - https://www.csoonline.com/article/3245587/scan-the-dark-web-for-threat-intelligence.html

20.Digital Certificate Management – ToC

20.1. Digicert –

20.2. Venafi –

21.Digital Risk Protection [20] – ToC

21.1. Axur -

21.2. Blueliv -

21.3. CTM360 -

21.4. CyberInt -

21.5. Cyxtera -

21.6. Digital Shadows – https://www.digitalshadows.com/

21.7. IntSights - https://www.intsights.com/tailored-intelligence

21.8. LookingGlass Cyber Solutions -

21.9. Proofpoint -

21.10.Recorded Future -

21.11.RiskIQ -

21.12.Social SafeGuard -

21.13.Sweepatic -

21.14.ZeroFOX -

Distributed Energy – Solar Farms – See "Generation Solar"

Distributed Energy – Wind Farms – See "Generation Wind"

22.Drone Attack Defense - ToC

22.1.

23.Education for Employees -

23.1. Anomali - https://www.anomali.com

Email Focus – see Phishing -

24.EMS Protection (in a Balancing Authority) -

[20] Forrester New Wave™: Digital Risk Protection, Q3 2018 - https://www.EnergyCollection.us/Energy-Security/Digital-Risk-Protection-01.pdf

25.Endpoint Detection & Response (EDR) [21] [22] [23] [24] [25] [26] [27] [28] [29]- ToC

25.1. Appthority – https://www.appthority.com
25.2. AT&T -
25.3. Axonius -
25.4. Bit9 – now Carbon Black - https://tinyurl.com/ya2mauhw
25.5. Bromium –
25.6. Carbon Black – https://www.carbonblack.com – MITRE attack analysis - https://attackevals.mitre.org/evaluations/carbonblack.1.apt3.1.html
25.7. Check Point - https://www.checkpoint.com/products/endpoint-policy-management/
25.8. Cisco Systems (Cisco ICE) – https://www.cisco.com -
25.9. Claroty -
25.10.CounterTack – https://www.countertack.com/ / MITRE attack analysis - https://attackevals.mitre.org/evaluations/carbonblack.1.apt3.1.html
25.11.CrowdStrike – https://www.crowdstrike.com / https://tinyurl.com/yckl2hn2 / MITRE Attack analysis - https://attackevals.mitre.org/evaluations/crowdstrike.1.apt3.1.html
25.12.Cyber Edge - c-Assur –
25.13.Cybereason – https://www.cybereason.com/ / MITRE Attack Analysis - https://attackevals.mitre.org/evaluations.html
25.14.CyberX -
25.15.Cylance - https://www.cylance.com -
25.16.Dell [30]-

[21] Endpoint Detection and Response (EDR) platforms are security systems that combine elements of next-gen antivirus with additional tools to provide real-time anomaly detection and alerting, forensic analysis and endpoint remediation capabilities. By recording every file execution and modification, registry change, network connection and binary execution across an organization's endpoints, EDR enhances threat visibility beyond the scope of EPPs.

[22] Wikipedia on Endpoint Security - https://en.wikipedia.org/wiki/Endpoint_security

[23] IDC MarketScape - https://www.EnergyCollection.us/Companies/IDC/MarketScape-Endpoint-Protection-2018.pdf

[24] Forrester Endpoint Detection and Response 2018 - https://www.EnergyCollection.us/Companies/Forrester/Wave-Endpoint-Detection-2018.pdf ToC

[25] SANS Survey, Endpoint Protection and Response - https://www.EnergyCollection.us/Companies/SANS/Endpoint_Detection_Response.pdf

[26] Top Endpoint Encryption Technology Vendors - https://www.EnergyCollection.us/Energy-Security/Top-Endpoint-Encryption-Technology-Vendors.pdf

[27] Forrester Endpoint Security Suites 2018 - https://www.EnergyCollection.us/Companies/Forrester/Wave-Endpoint-Security-2018.pdf

[28] Network Access Control - Wikipedia - https://en.wikipedia.org/wiki/Network_Access_Control - Network Access Control (NAC) is an approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.

[29] NSS Labs re Advanced Endpoint Protection - https://www.nsslabs.com/aep-test-overview

[30] Dell unveils endpoint security portfolio with CrownStrike, Secureworks - http://www.energycollection.us/Best-Practices/Endpoint-Detection-And-Response/Dell-Unveils-Endpoint.pdf

25.17.Endgame – MITRE Attack Analysis - https://attackevals.mitre.org/evaluations/crowdstrike.1.apt3.1.html

25.18.ESET - https://www.eset.com/us/ -

25.19.Fidelis Security - https://www.fidelissecurity.com/products/network

25.20.FireEye - https://www.fireeye.com/ / MITRE Attack Analysis - https://attackevals.mitre.org/evaluations.html

25.21.FireLayers –

ToC

25.22.ForeScout –

25.23.Gravwell – http://www.gravwell.com - https://www.gravwell.io/technology

25.24.Hexis –

25.25.IronNet -

25.26.Ivanti - https://www.ivanti.com/ -

25.27.Juniper Networks – https://www.juniper.net/us/en/products-services/security/advanced-threat-prevention-appliance/

25.28.Kaspersky Labs - https://usa.kaspersky.com/ -

25.29.Leidos -

25.30.Lumension –

25.31.Lumenta - http://www.lumeta.com/products/spectre

25.32.Malwarebytes - https://www.malwarebytes.com/ -

25.33.McAfee - https://www.mcafee.com -

25.34.Microsoft – https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-protection - / MITRE Attack Analysis - https://attackevals.mitre.org/evaluations/microsoft.1.apt3.1.html

25.35.Mobile System 7 –

25.36.Morphisec PAS –

25.37.Open Text Corporation – https://www.opentext.com/

25.38.Palo Alto Networks - https://www.paloaltonetworks.com/

25.39.ProofPoint -

25.40.RSA Security – https://www.rsa.com/en-us/index / MITRE Attack Analysis - https://attackevals.mitre.org/evaluations/rsa.1.apt3.1.html

25.41.Secureworks -

25.42.SentinelOne – MITRE Attack Analysis - https://attackevals.mitre.org/evaluations/sentinelone.1.apt3.1.html

33.1. ***Skybox Security*** -

33.2. ***Sophos*** - https://secure2.sophos.com/en-us/lp/edr-check.aspx?

33.3. ***SSH*** - https://www.ssh.com/ -

ToC

25.43.Symantec – https://www.symantec.com/

25.44.Tanium – https://www.tanium.com/

25.45.Tenable -

25.46.Trend Micro - https://www.trendmicro.com/en_us/business.html

25.47.Tripwire - https://www.tripwire.com/

25.48.Zimperium –

26.Endpoint Protection Platforms [31] -

ToC

26.1. ***Bitdefender*** - https://www.bitdefender.com/

26.2. ***BlackBerry Cylance*** - https://www.cylance.com/en-us/index.html

26.3. ***Carbon Black*** – https://www.carbonblack.com –

26.4. ***Check Point*** - https://www.checkpoint.com/products/endpoint-policy-management

26.5. ***Cisco Systems*** (Cisco ICE) – https://www.cisco.com -

[31] Gartner MQ on Endpoint Protection Platforms - https://energycollection.com/Companies/Gartner/MQ-Endpoint-Protection-Platforms.pdf

26.6. ***CrowdStrike*** – https://www.crowdstrike.com / https://tinyurl.com/yckl2hn2 -
26.7. ***ESET*** - https://www.eset.com/us -
26.8. ***F-Secure*** - https://www.f-secure.com/en_US/welcome
26.9. ***FireEye*** - https://www.fireeye.com -
26.10. ***Fortinet*** - https://www.fortinet.com/solutions/enterprise-midsize-business/endpoint-and-device-protection.html
26.11. ***Kaspersky Labs*** - https://usa.kaspersky.com -
26.12. ***Malwarebytes*** - https://www.malwarebytes.com -
26.13. ***McAfee*** - https://www.mcafee.com -
26.14. ***Microsoft*** – https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-protection - /
26.15. ***Mocana*** - https://www.mocana.com/solutions/electricity
26.16. ***Panda Security*** - https://www.pandasecurity.com/usa -
26.17. ***Palo Alto Networks*** - https://www.paloaltonetworks.com -
26.18. ***SentinelOne*** – https://www.sentinelone.com - MITRE Attack Analysis - https://attackevals.mitre.org/evaluations/sentinelone.1.apt3.1.html -
26.19. ***Sophos*** - https://secure2.sophos.com/en-us/lp/edr-check.aspx? -
26.20. ***Symantec*** – https://www.symantec.com -
26.21. ***Trend Micro*** - https://www.trendmicro.com/en_us/business.html

27. File Integrity - ToC

27.1. ***Tripwire*** - https://www.tripwire.com/products/tripwire-file-integrity-manager/

28. Frameworks and Controls[32] – Private Notes -

28.1. ***AlienVault*** - https://www.alienvault.com/products/usm-anywhere (supports CSF)
28.2. ***BSIMM*** - https://www.bsimm.com/about.html
28.3. ***CIS Controls*** - https://www.cisecurity.org/controls/
28.4. ***NIST CSF (Cyber Security Framework)*** - https://www.nist.gov/cyberframework
28.5. ***ES-C2M2*** – https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-1
28.6. ***ISO IES 2700 Family*** - https://www.iso.org/isoiec-27001-information-security.html
28.7. ***MITRE*** - https://www.tripwire.com/state-of-security/mitre-framework/mitre-attack-framework-what-know/
28.8. ***PCI DSS*** - https://www.itgovernanceusa.com/shop/product/pci-dss-documentation-toolkit
28.9. ***PCI Security Standards Council*** - Software Security Framework - https://www.pcisecuritystandards.org/documents/FAQs-for-PCI-Software-Security-Framework-v1_0.pdf?agreement=true&time=1554722214000

Firewalls – see "Network Segmentation"

29. Generation – Central Station – ToC

29.1.

Generation – Solar – see "Distributed Energy – Solar" above
Generation – Wind – see "Distributed Energy – Wind" above

30. Generation – Solar –

31. Generation – Wind –

32. Governance, Risk, And Compliance (GRC) Platforms – ToC

32.1. ***BWise (acquired by SAI Global)*** -
32.2. ***EMC RSA*** – https://www.rsa.com/en-us/index

[32] Topic initially presented at the POP BP Conference 2019-02-04 by *Steven Parker, President, EnergySec* -

32.3. *Enablon* – https://enablon.com
32.4. *Fortress Information Security* – https://fortressinfosec.com/about/
32.5. *GuidePoint Security* - https://www.guidepointsecurity.com
32.6. *IBM* – https://www.ibm.com/analytics/hk/en/business/governance-risk-compliance/
32.7. *LogicManager* – https://www.logicmanager.com/
32.8. *MetricStream* – https://www.metricstream.com
32.9. *Nasdaq BWise* – https://www.bwise.com/
32.10. *NAVEX Global* – https://www.navexglobal.com/en-us
32.11. *Protiviti* – https://www.protiviti.com
32.12. *Resolver* – https://www.resolver.com/
32.13. *Rsam* – https://www.rsam.com/
32.14. *SAI Global* – https://www.saiglobal.com
32.15. *SAP* – https://www.sap.com/products/technology-platforms/grc.html
32.16. *Thomas Reuters* – https://www.thomsonreuters.com/en/products-services/risk-management.html
32.17. *Trusted Integration* – http://www.trustedintegration.com/
32.18. *Wolters Kluwer Financial Services* - https://wolterskluwer.com/products-services/our-portfolio/governance-risk-compliance.html

33. Identity Access Management and Governance [33] [34] [35] [36] [37] [38] [39] [40] – Northeastern University has undertaken an analysis of Vendors for this Topic. **5/40** ToC

33.1. *AlertEnterprise* – http://www.alertenterprise.com/ - in NE Study
33.2. *Altos (Evidian)* - https://www.evidian.com/ - in NE Study
33.3. *Auth0* - https://auth0.com/ - in NE Study
33.4. *BeyondTrust (PAM)* - https://www.beyondtrust.com/ - in NE Study
33.5. *BioCatch* – https://www.biocatch.com – in NE Study
33.6. *BlackRidge Technology* - https://www.blackridge.us/solutions/iiot-and-utilities - In NE Study
Broadcom – see "CA Technologies" below
33.7. *CA Technologies (Broadcom)* - https://www.broadcom.com/products/software/cybersecurity/identity-and-access-management - in NE Study

[33] Northeastern University has undertaken an analysis of Vendors for this Topic.

[34] Forrester - The Future Of Identity And Access Management - https://www.EnergyCollection.us/Best-Practices/Identity-Management-and-Governance/Forrester-Future.pdf

[35] Forrester Wave: Identity-As-A-Service (IDaaD) for Enterprise, Q2 2019 - https://www.okta.com/resources/analyst-research-forrester-wave-leader-identity-as-a-service/

[36] SailPoint - the 2018 Identity Report - https://www.EnergyCollection.us/Best-Practices/Identity-Management-and-Governance/SailPoint-Identity-Report-2018.pdf

[37] NCCoE on Identity Access Management - https://www.nccoe.nist.gov/projects/use-cases/idam

[38] Forrester Wave - https://www.EnergyCollection.us/Best-Practices/Identity-Management-and-Governance/Forrester-2018.pdf

[39] Gartner – Magic Quadrant for Identity Governance and Administration - https://www.EnergyCollection.us/Companies/Gartner/MQ-Identity-Access.pdf

[40] Gartner – Critical Capabilities for Access Management - https://www.EnergyCollection.us\Companies\Gartner\Critical-Capabilities-Access-Management.pdf

33.8. ***Centrify (PAM)*** – https://www.centrify.com/privileged-access-management/privileged-access-service/ – in NE Study
33.9. ***Cisco*** - https://www.cisco.com/ - in NE Study
33.10. ***Core Security*** - https://www.coresecurity.com/ - in NE Study
33.11. ***CyberArk (PAM)*** – https://www.cyberark.com – in NE Study
33.12. ***Dell Technologies (RSA)*** - https://www.delltechnologies.com/en-us/index.htm - in NE Study
Fortscale – acquired by RSA - https://www.rsa.com/en-us/blog/2018-04/rsa-acquires-fortscale
Evidan – see "Atos (Evidan)" above
33.13. ***ForgeRock*** - https://www.forgerock.com/ - in NE Study
33.14. ***GlobalSign*** - https://www.globalsign.com/en/ - in NE Study
33.15. ***HID Industries*** - https://www.hidglobal.com/oil-gas
33.16. ***Hypr*** – https://www.hypr.com
33.17. ***IBM*** – https://www.ibm.com/security/identity-access-management - in NE study
33.18. ***Idaptive*** - https://www.idaptive.com/ - in NE Study
33.19. ***IDM365*** - https://idm365.com/ - in NE Study
33.20. ***Micro Focus (NetIQ)*** – https://www.microfocus.com/en-us/home - in NE Study
33.21. ***Microsoft*** - https://www.microsoft.com/en-us/security/technology/identity-access-management - in NE Study
NetIQ – see "Micro Focus (NetIQ) above
33.22. ***Nok Nok Labs*** – https://www.noknok.com – in NE Study
33.23. ***Okta*** - https://www.okta.com/iam-identity-and-access-management/ – in NE Study
33.24. ***Omanda*** - https://omadatechnologies.com/ - in NE Study
33.25. ***One Identity*** - https://www.oneidentity.com/ - in NE Study
33.26. ***OneLogin*** - https://www.onelogin.com/ - in NE Study
33.27. **Oracle** - https://www.oracle.com/index.html - in NE Study
PAM – see "BeyondTrust (PAM)" above
PAM – see "Centrify (PAM)" above
PAM – see "CyberArc (PAM)" above
PAM – see (Thycotic (PAM)" below
33.28. ***PAS*** – https://www.pas.com – in NE Study
33.29. ***Ping Identity*** - https://www.pingidentity.com/en.html - in NE Study
Quantum Secure – See "HID Industries" above
33.30. ***Radiflow*** - https://radiflow.com/ - in NE Study
RSA Security – see "Dell (RSA) above
33.31. ***SailPoint*** – https://www.sailpoint.com – in NE Study
33.32. ***SAP NS2*** - https://sapns2.com/ - in NE Study
33.33. ***Saviynt*** – https://saviynt.com/ - in NE Study
33.34. ***SecureAuth*** - https://www.secureauth.com/ - in NE Study
33.35. ***SSH*** - https://www.ssh.com/ - in NE Study
Stormpath – bought by Okta - https://stormpath.com -
33.36. ***Thales*** - https://www.thalesgroup.com/en/markets/digital-identity-and-security/enterprise-cybersecurity - in NE Study
33.37. ***ThreatMetrix*** – https://www.threatmetrix.com / https://risk.lexisnexis.com/products/threatmetrix/ - in NE Study
33.38. ***Thycotic (PAM)*** - https://thycotic.com/ - in NE Study
33.39. ***Ubisecure (CIAM)*** - https://www.ubisecure.com/ - in NE Study
33.40. ***XTech*** - http://www.xtec.com/solutions/critical-infrastructure.html

34.Incident Response [41] – ToC

- 34.1. ***AlienVault USM*** -
- 34.2. ***D3 Security*** - https://d3security.com/platform/automated-incident-response/
- 34.3. ***Dragos*** -
- 34.4. ***Resilient Systems*** –

35.Information Sharing -

- 35.1. ***CRISP*** -
- 35.2. ***E-ISAC*** –
- 35.3. ***Energy Analytic Security Exchange (EASE)*** - https://www.isao.org/information-sharing-group/sector/energy-analytic-security-exchange-ease/
- 35.4. ***IronNet*** -

36.Insider Threats [42] –

- 36.1. ***Claroty*** –
- 36.2. ***Dtex*** - https://www.dtexsystems.com/about/
- 36.3. ***ForeScout*** -
  - ***Fortscale*** – acquired by RSA - https://www.rsa.com/en-us/blog/2018-04/rsa-acquires-fortscale
- 36.4. ***RedOwl Analytics*** –
- 36.5. ***PAS*** – https://www.pas.com -
- 36.6. ***PhishMe*** –
- 36.7. ***Veriato*** - https://www.veriato.com/

37.Internet of Things (IoT) [43] - ToC

- 37.1. ***Affinity Security*** - https://affinity-it-security.com
- 37.2. ***Cisco*** –
- 37.3. ***Claroty*** - https://finance.yahoo.com/news/claroty-extends-visibility-market-leading-120000484.html

IT Monitoring - see Enterprise IT Network Monitoring and Threat Detection above

Level 0 Devices within the Purdue Architecture [44] – see "Monitoring Electric and Analog Signals in real-time"

38.Log Management – ToC

- 38.1. ***BlackStratus*** – https://www.blackstratus.com -
- 38.2. ***Cyber Edge*** –
- 38.3. ***Tripwire*** - https://www.tripwire.com/products/tripwire-log-center/

39.Managed Services (MSSPs) [45] [46] –

- 39.1. ***Alert Logic*** –
- 39.2. ***AT&T*** –
- 39.3. ***Atos*** -

[41] ICS Cyber Incident Response Plan RP - https://ics-cert.us-cert.gov/Abstract-ICS-Cyber-Incident-Response-Plan-RP

[42] Note: Vendors that have the capability to actively monitor IT Networks, or ICS networks are potentially able to identify a given device is a rogue that is spoofing an IP Address for a valid device

[43] The Industrial Internet of Things - What's the Difference Between IoT and IIoT? https://www.leverege.com/blogpost/difference-between-iot-and-iiot

[44] A Grim Gap: Cybersecurity of Level 1 Field Devices - https://www.powermag.com/a-grim-gap-cybersecurity-of-level-1-field-devices/

[45] Forrester Wave 2018 - https://www.EnergyCollection.us/Companies/Forrester/Wave-MSSPs-2018.pdf

[46] Gartner MQ on Managed Security Service Providers – 2019 - https://www.EnergyCollection.us/Companies/Gartner/MQ-MSSP-2019.pdf

39.4. *BAE Systems* -

39.5. *BT* –

39.6. *Capgemini* -

39.7. *CenturyLink* –

39.8. *CSC* –

39.9. *Datto* – www.Datto.com

39.10. *Dell Networks* –

39.11. *Fujitsu* -

39.12. *GridSME* - https://www.gridsme.com/gridsec.html

39.13. *HP* –

39.14. *IBM* –

39.15. *NTT* –

39.16. *Orange Business Services* –

39.17. *Outpost24* - https://outpost24.com/

39.18. *Secureworks* -

39.19. *SolarWinds* - https://www.solarwindsmsp.com/

39.20. *Solutionary* –

39.21. *Symantec* –

39.22. *Tripwire* -

39.23. *Trustwave* – https://www.trustwave.com/en-us/ - not targeting Utilities on industry focus page.

39.24. *Unity Technology* -

39.25. *Verizon* –

39.26. *Wipro* -

Network Access Control (NAC) - see Enterprise IT Network Monitoring and Threat Detection above

40. Monitoring Devices and Hosts [47] [48]- ToC

41. Monitoring Electric and Analog Signals in real-time -

41.1. *Exacter* -

41.2. *Mission Secure* - https://www.missionsecure.com/solutions/products/

41.3. *North Carolina State University* - https://www.helpnetsecurity.com/2019/04/29/identify-malware-in-embedded-systems/

41.4. *Siga* - https://sigasec.com/how-it-works/

[47] Host-Based Intrusion Detection System Comparison - https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system_comparison

[48] Mobile Device Security: Cloud and Hybrid Builds - https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid

42.*Monitoring – Real-Time Operational Technology Network Analysis and Security*

[49] [50] [51] [52] [53] [54] – Washington State University has undertaken an analysis of Vendors for this Topic. **24/49** ToC

42.1. ***802 Secure*** -

42.2. ***AICS*** - https://inl.gov/article/federal-laboratory-consortium-awards/

42.3. ***Ampex*** - https://www.ampex.com/ceadil/

42.4. ***Aperio*** - https://www.aperio-systems.com/

42.5. ***Armis*** – https://armis.com/product/

42.6. ***Bayshore Networks*** -

42.7. ***BlackStratus*** - https://www.blackstratus.com/industries/energy-utility-sectors/

Centri - https://www.centritechnology.com/ - not relevant in this space

42.8. ***Centripetal Networks*** – https://www.centripetalnetworks.com/

42.9. ***Check Point*** - https://www.checkpoint.com/solutions/critical-infrastructure/

Cisco Systems – see Sentryo below / also see Snort below

42.10. ***Claroty*** – https://www.claroty.com/continuous-threat-detection

ControlWatch – see "Fortiphy" below

42.11. ***Cyberbit*** – https://www.cyberbit.com/solutions/ics-scada-security-continuity/

42.12. ***CyberProof*** – https://www.cyberproof.com/

CyberLens - https://cyberlens.io/ - now part of Dragos

42.13. ***CyberX*** – https://cyberx-labs.com / http://www.EnergyCollection.us/Companies/NIST/NISTIR-8219.pdf

42.14. ***Cyglass*** - https://www.cyglass.com/

42.15. ***D&G - Darktrace*** – https://www.darktrace.com/en/industries/#utilities

42.16. ***DarkTrace*** -

42.17. ***Dragos*** – https://dragos.com/

42.18. ***Fidelis Security*** - https://www.fidelissecurity.com/products/network -

42.19. ***FireMon (Lumeta)*** - https://www.firemon.com/products/lumeta/ -

FlowTraq – https://www.flowtraq.com/industries/ - Utilities not a target market

42.20. ***Forcepoint*** - https://www.forcepoint.com/solutions/industry/critical-infrastructure-cybersecurity - ToC

42.21. ***ForeScout*** – SecurityMatters (acquired by ForeScout) – https://www.forescout.com/platform/operational-technology/

42.22. ***Fortiphy (ControlWatch)*** - https://www.fortiphyd.com/products/

42.23. ***FoxGuard Solutions*** - https://foxguardsolutions.com/sentrigard/

42.24. ***GAI Technologies*** -

42.25. ***GE Digital (Wurldtech acquisition)*** – https://www.ge.com/digital/applications/cyber-security

[49] Topic initially presented at the POP BP Conference 2019-02-04 by *Dale Peterson, Creator and Program Chair of S4 Events; Leader in ICS Security Research; Industry Evangelist* -

[50] Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection - https://www.EnergyCollection.us/Companies/NIST/NISTIR-8219.pdf

[51] NCCOE on Asset Management - https://www.nccoe.nist.gov/projects/use-cases/energy-sector/asset-management

[52] NIST Cybersecurity Practice Guide, Special Publication 1800-7: "Situational Awareness for Electric Utilities" - https://www.nccoe.nist.gov/projects/use-cases/situational-awareness

[53] See NISTR 8219 – Securing Manufacturing Industrial Control Systems: Behavioral-Anomaly Detection - https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf

[54] See list of vendors at https://en.wikipedia.org/wiki/Network_behavior_anomaly_detection#Commercial_products

42.26.*GrayMatter* - https://graymattersystems.com/cyber-security-for-operational-technology/

Great Bay Software - https://www.greatbaysoftware.com – only targeting Healthcare and Financial Services Industries

42.27.*Indegy* – https://www.indegy.com/

IronNet (via Claroty partnership) – https://www.claroty.com/continuous-threat-detection

42.28.*Kaspersky Lab* - https://usa.kaspersky.com/enterprise-security/industrial-solution -

ToC

42.29.*Leidos* - https://www.leidos.com/markets/energy/utilities/utility-security

Lumeta – see FireMon above

42.30.*Mission Secure* – https://www.missionsecure.com/solutions/products/

42.31.*mPrest* - https://www.mprest.com/industries/security-cip

42.32.*Network Perception* - https://www.network-perception.com/np-live/

NexDefense – Acquired by Dragos

42.33.*Nextnine* – https://nextnine.com/ics_cybersecurity/

42.34.*Nozomi Networks* – https://www.nozominetworks.com/solutions/electric-utilities/

Omnivise – Siemens product name – see Siemens below

42.35.*PAS* – https://www.pas.com -

42.36.*Positive Technologies* - https://www.ptsecurity.com/ww-en/solutions/utilities/

42.37.*ProtectWise* – https://www.protectwise.com/converged-it-ot/

42.38.*RAD* – https://www.rad.com/hot-trends/Cyber-Security-1

42.39.*Radiflow* - https://radiflow.com/products/isid-industrial-threat-detection/

SCADAfence - https://www.scadafence.com/platform/ - no apparent U.S. operations

42.40.*Secure-NOC* - https://www.securenok.com/our-products/#ids / http://www.EnergyCollection.us/Companies/NIST/NISTIR-8219.pdf

SecurityMatters (SilentDefense) – see ForeScout above

42.41.*Sentryo* – https://www.sentryo.net/product-ics-cybervision/

42.42.*Siemens / Chronicle Partnership* - https://press.siemens.com/global/en/pressrelease/siemens-and-chronicle-join-forces-provide-industrial-monitoring-and-detection-energy?content[]=GP

SilentDefense – product name – see SecurityMatters

42.43.*Snort* - https://www.snort.org/ - https://en.wikipedia.org/wiki/Snort_(software) mainly maintained by Cisco

Sophia – now part of Dragos community tools - https://dragos.com/community-tools/

42.44.*Tenable* – https://www.tenable.com/solutions/energy

42.45. Tripwire (Private labels Claroty) – https://www.claroty.com/continuous-threat-detection

42.46.*Utilidata* - https://utilidata.com/solutions/#top -

ToC

42.47.*Verve* – http://verveindustrial.com/ot-cyber/ /// Verve Commended by Frost & Sullivan for Developing a Growth Strategy Based on Its Ability to Innovate Industrial Cybersecurity Services - https://tinyurl.com/y9kjzwhe (Frost & Sullivan Best Practices Award 2018)

42.48.*Waterfall* - https://waterfall-security.com/pr-waterfall-for-intrusion-detection-systems

42.49.*Xage Security* - https://xage.com/industries/#utilities

43. Monitoring IT/Enterprise Networks in real-time [55] [56] [57] - The University of North Carolina Charlotte has undertaken an analysis of Vendors for this Topic. **02/7** partial list ToC

43.1. *IronNet* –

43.2. *Ixia* – https://www.ixia.com

43.3. *Network Perception* - https://www.network-perception.com/np-live/

43.4. *Outpost24* - https://outpost24.com/

43.5. *Paessler* - https://www.paessler.com/prtg

43.6. *RiskIQ* - https://www.riskiq.com/products/passivetotal/

43.7. *SolarWinds* - https://www.solarwinds.com/network-performance-monitor

44. Network Access Control (NAC) [58] [59] [60] [61] – Prince Georges Community College has undertaken an analysis of Vendors for this Topic. **01/22** ToC

44.1. *Aerohive* – (cloud solution)

44.2. *Auconet* -

44.3. *CheckPoint* -

44.4. *Cisco* -

44.5. *Cyxtera AppGate*

44.6. *Easy NAC* - https://easynac.com/use-cases

44.7. *Extreme Networks* -

44.8. *ForeScout* –

44.9. *Fortinet* -

44.10. *HPE (Aruba)* –

44.11. *Impulse Point* -

44.12. *InfoExpress* -

44.13. *McAfee* -

44.14. *Palo Alto* -

44.15. *Portnox* -

44.16. *Pulse Secure* –

44.17. *Siemens* -

44.18. *SnoopWall* –

44.19. *Symantec* –

44.20. *Tempered Networks* -

44.21. *Trend Micro* –

44.22. *Verizon SDP (formerly Vidder)* -

[55] The University of North Carolina Charlotte has undertaken an analysis of Vendors for this Topic.

[56] See list of vendors at https://en.wikipedia.org/wiki/Network_behavior_anomaly_detection#Commercial_products

[57] Gartner Magic Quadrant for Network Performance Monitoring and Diagnostics - https://www.gartner.com/doc/reprints?id=1-6876F3Z&ct=190214&st=sb

[58] Frost & Sullivan - Network Access Control (NAC) Market, Global, Forecast to 2022 - https://www.EnergyCollection.us/Energy-Information-Technology/NAC-Market-2022.pdf

[59] Network Access Control Tutorial - https://www.networkcomputing.com/careers/tutorial-network-access-control-nac/880346581/page/0/8

[60] Wikipedia - https://en.wikipedia.org/wiki/Network_Access_Control

[61] Gartner PeerInsights - https://www.gartner.com/reviews/market/network-access-control/vendors

45.*Network Segmentation* [62] [63] - The University of Houston has undertaken an analysis of Vendors for this Topic. **08/20** ToC

45.1. ***Advenica*** - https://www.advenica.com/

45.2. ***BAE Systems*** - https://www.baesystems.com/en/home -

45.3. ***Blue ridge Networks*** - https://www.blueridgenetworks.com/linkguard/

45.4. ***Check Point*** - https://www.checkpoint.com/solutions/critical-infrastructure/

45.5. ***Claroty*** - http://blog.claroty.com/virtual_segmentation

45.6. ***Deep Secure*** – https://www.deep-secure.com/

45.7. ***Fibersystem*** - https://www.fibersystem.com/

45.8. ***Forcepoint*** - https://www.forcepoint.com/solutions/industry/critical-infrastructure-cybersecurity

45.9. ***Fortinet*** - https://www.fortinet.com/

45.10. ***Fox-IT*** – https://www.fox-it.com/en -

45.11. ***Genua*** – https://www.genua.de/en/products/data-diode-for-industrial-applications.html -

45.12. ***Mission Secure*** - https://www.missionsecure.com/solutions/products/

45.13. ***Nexor*** – https://www.nexor.com -

45.14. ***Owl Computing*** – http://library.owlcyberdefense.com/opds-100/page/1

45.15. ***Palo Alto Networks*** - https://www.paloaltonetworks.com/

45.16. ***Seclab*** – https://www.seclab-security.com/vs-diode-3 -

45.17. ***Siemens*** - https://new.siemens.com/global/en/company/stories/mobility/new-siemens-data-diode-now-available-secure-monitoring-of-your-networks.html

45.18. ***VADO One Way*** – https://www.vadosecurity.com -

45.19. ***Verve Industrial Protection*** - https://verveindustrial.com/network-design/

45.20. ***Waterfall Security*** – https://www.helpnetsecurity.com/2018/12/03/sec-ot/

46.*Organizational Best Practices* – addressing culture, organizational structure, positions, reporting relationships, etc. ToC

47.*Patch and Firmware Management* [64] [65] –

47.1. ***Adolus*** - https://www.adolus.com/

47.2. ***Finite State*** - https://finitestate.io/

47.3. ***GFI LanGuard*** - https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard (no utilities listed as customers)

47.4. ***ForeScout*** - https://www.forescout.com/solutions/network-segmentation/

47.5. ***FoxGuard Solutions*** - https://foxguardsolutions.com

HEAT PatchLink – see "Ivanti" below (HEAT is now part of Ivanti)

47.6. ***ICS-CERT*** - https://ics-cert.us-cert.gov/Abstract-Patch-Management-ICS-RP

47.7. ***Ivanti*** - https://www.ivanti.com/solutions/needs/manage-my-os-and-third-party-application-patches / https://www.ivanti.com/blog/patch-management-best-practices (Utilities not listed as a target market)

47.8. ***Kaseya VSA Patch Management*** - https://www.kaseya.com/products/vsa/

[62] Topic initially presented at the POP BP Conference 2019-02-04 by *Art Conklin, Director, Center for Information Security Research and Education, University of Houston* -

[63] Firewall Deployment on ICS Networks RP - https://ics-cert.us-cert.gov/Abstract-Firewall-Deployment-ICS-Networks-RP

[64] Topic initially presented at the POP BP Conference 2019-02-04 by *Monta Elkins – SANS Instructor, ICS Researcher, author of "Defense against the Dark Arts"* - Video/Audio - https://vimeo.com/329632669/c25a1d9a61 Presentation - https://protectourpower.org/best-practices/monta-elkins-presentation.pdf

[65] Patching Like a Boss (from ReliabilityFirst) - https://www.EnergyCollection.us/Companies/Reliability-First/Newsletter-2018-11-01.pdf

47.9. ***ManageEngine Patch Manager Plus*** - https://www.manageengine.com/patch-management/ Utilities listed as customers - https://www.manageengine.com/customers.html
47.10. ***Microsoft SCCM Patch Management*** - https://docs.microsoft.com/en-us/sccm/
47.11. ***Owl*** - http://library.owlcyberdefense.com/ssus/page/1
47.12. ***Quest KACE Patch Management*** - https://www.quest.com/products/kace-systems-management-appliance/patch-management-security.aspx
47.13. ***Symantec Patch Management Solution*** -
https://www.symantec.com/products/patch-management-solution
https://support.symantec.com/en_US/article.HOWTO3124.html
47.14. ***SolarWinds*** - https://www.solarwindsmsp.com –
47.15. ***TDI Technologies*** – ConsoleWorks - https://www.tditechnologies.com/
47.16. ***Verve*** -

48. ***Penetration Testing (including Vulnerability Assessments and Risk Assessments)*** – ToC
48.1. ***Affinity Security*** https://affinity-it-security.com
48.2. ***AT&T / AlienVault -*** https://learn.alienvault.com/c/attcyber-penetration-testing
48.3. ***Black Hills*** -
48.4. ***Cyber Edge*** - v-Motiv –
48.5. ***Lockheed*** –
48.6. ***OPAL-RT –*** https://www.opal-rt.com/cybersecurity-overview
48.7. ***Outpost24*** - https://outpost24.com/
48.8. ***Quanexus*** –
48.9. ***Red Team Project*** - https://redteamproject.org/
48.10. ***RTDS Technologies*** – https://www.rtds.com/applications/cybersecurity
48.11. ***Saint*** -
48.12. ***Scythe*** - https://www.scythe.io/platform
48.13. ***Secure Info*** –
48.14. ***Siemens*** –

Phishing – See "Social Engineering"

49. ***Portable Media*** – ToC
49.1. ***Symantec*** - https://tinyurl.com/yc7ewvrw / https://im-mining.com/2018/12/10/symantecs-icsp-neural-protect-operational-technology-cyber-attacks/

50. ***Remote Access Solutions (including secure remote access)*** [66] [67] [68] [69] – George Mason University has undertaken an analysis of Vendors for this Topic. **10/38** ToC
50.1. ***ABB*** - https://new.abb.com/uk/about/our-businesses/power-grids
50.2. ***ARCON*** -
50.3. ***Attila Cybertech*** - https://www.attilatech.com/aboutus
50.4. ***Bayshore Networks*** – https://www.bayshorenetworks.com/beacon
50.5. ***BeyondTrust*** - https://www.beyondtrust.com/solutions/energy/

[66] Topic presented at the POP BP Conference 2019-02-04 by *Dave Weinstein, Policy Fellow at New America, Previous U.S. Cyber Command, and New Jersey CIO* - https://protectourpower.org/best-practices/dave-weinstein/ Video/Audio - https://vimeo.com/329626259/98ecafa34f Presentation - https://protectourpower.org/best-practices/dave-weinstein-presentation.pdf

[67] Configuring and Managing Remote Access for Industrial Control Systems - https://ics-cert.us-cert.gov/Abstract-Configuring-and-Managing-Remote-Access-Industrial-Control-Systems

[68] The Definitive Guide to Secure Remote Access - https://tinyurl.com/y973ycbg

[69] Wikipedia on Access Control - https://en.wikipedia.org/wiki/Access_control

50.6. ***Blue Ridge Networks*** - https://www.blueridgenetworks.com/linkguard/

Bomgar (part of BeyondTrust now) – https://www.bomgar.com/

50.7. ***Broadcom*** - https://www.broadcom.com/products/software/cybersecurity/privileged-access-management

50.8. ***CA Technologies*** - https://www.ca.com/us.html

50.9. ***Centrify*** - https://www.centrify.com/privileged-access-management/privileged-access-service/secure-remote-access/ -

50.10. ***Claroty*** - https://www.claroty.com/secure-remote-access -

50.11. ***ClickStudios*** - https://www.clickstudios.com.au/about/role-based-access.aspx

Crossbow – see "Siemens Crossbow" below

50.12. ***CyberArk*** - https://www.cyberark.com/resource/cyberark-nerc-secured-remote-access

50.13. ***CyberX*** - https://cyberx-labs.com/secure-remote-access/

50.14. ***Devolutions*** - https://devolutions.net/solutions/privileged-access-management

50.15. ***Dragos*** - https://dragos.com/

50.16. ***EPRI*** - http://eprijournal.com/a-new-tool-to-protect-the-keys-to-the-kingdom/

50.17. ***Forescout*** - https://www.forescout.com/platform/eyecontrol/

50.18. ***Fudo Security*** -

50.19. ***Hitachi ID Systems*** –

50.20. ***Honeywell*** - https://www.honeywell.com/en-us/remote-access

Indegy – now Tenable -

ManageEngine - https://www.manageengine.com – Utilities not included in target markets.

50.21. ***Micro Focus*** - https://www.microfocus.com/en-us/solutions/enterprise-security

50.22. ***Nextnine*** - https://nextnine.com/secure-remote-access/

50.23. ***Nozomi Networks*** - https://www.nozominetworks.com/

50.24. ***One Identity*** - https://www.oneidentity.com/

50.25. ***Owl*** - http://library.owlcyberdefense.com/recon/page/1

50.26. ***Saviynt*** **-** https://devolutions.net/solutions/privileged-access-management

50.27. ***Secomea*** - https://www.secomea.com/remote-access-for-utility-installations/

50.28. ***Securelink*** - https://www.securelink.com/industries/energy/

50.29. ***Senha Segura*** - https://www.senhasegura.com.br/en/

50.30. **Siemens Crossbow** - https://w3.siemens.com/mcms/industrial-communication/en/rugged-communication/ruggedcom-portfolio/software/pages/crossbow.aspx

50.31. ***SSH*** - https://www.ssh.com/

50.32. ***SUBNET*** – http://www.subnet.com/news-events/white-papers/unified-ied-management-solution-whitepaper.aspx

50.33. ***TDI Technologies – ConsoleWorks*** - https://www.tditechnologies.com/

50.34. ***Tenable*** - https://www.tenable.com/solutions/energy

50.35. ***Thycotic*** - https://thycotic.com/ / https://thycotic.com/solutions/energy-utilities-cybersecurity/

50.36. ***Veracity*** - https://veracity.io/product/

50.37. ***WALLIX*** – https://www.wallix.com/en/

50.38. ***Waterfall*** - https://waterfall-security.com/remote-access/remote-screen-view

Remote Access - see Privileged Remote Access Solutions above

51.*Risk Assessment and Quantification, and Management* [70] [71] [72][73] [74] [75] [76] [77] [78] [79] [80]

Michigan Technical Institute has undertaken an analysis of Vendors for this Topic / **1/29**
ToC /

51.1. ***Axio Global*** - https://axio.com
51.2. ***Beyond Trust*** - https://www.beyondtrust.com/solutions/energy/
51.3. ***BitSight*** - https://www.bitsight.com/
51.4. ***CoalFire*** -
51.5. ***CyberGRX*** – https://www.cybergrx.com
51.6. ***FireEye*** - https://www.fireeye.com/services/mandiant-security-program-assessment.html
51.7. ***Guidewire Cyence*** - https://www.guidewire.com/products/cyence
51.8. ***HITRUST*** - https://hitrustalliance.net/performing-risk-assessment-meet-meaningful-use-criteria/
51.9. ***INL*** - Consequence-Driven, Cyber-Informed Engineering (CCE) - https://www.inl.gov/wp-content/uploads/2018/02/18-50019_CCE_R1-1.pdf
51.10.*LookingGlass* - https://www.lookingglasscyber.com/
51.11.*Ncontracts* -
51.12.*NextLabs* – https://www.nextlabs.com/solutions/industry-solutions/energy/
51.13.*NormShield* – https://www.normshield.com
51.14.*OneTrust* -
51.15.*Prevalent* – https://www.prevalent.net/
51.16.*Red Tiger Security* - http://redtigersecurity.com/about-us/
51.17.*RiskLens* - https://www.risklens.com

[70] Topic initially presented at the POP BP Conference 2019-02-04 by *Jason Christopher, SANs Instructor, formerly Senior technical Leader Cyber Security, EPRI; Technical Lead Cyber Security, DOE' Technical Lead, FERC.* -

[71] Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q4 2018 - https://www.EnergyCollection.us/Companies/Forrester/Risk-Rating-Solutions-2018.pdf

[72] Forrester Wave – Vulnerability Risk Assessment Q4 2019 – https://www.EnergyCollection.us/Companies/Forrester/Wave-Vulnerability-Risk-Management-Q4-2019.pdf

[73] Wikipedia - https://en.wikipedia.org/wiki/Cyber_risk_quantification

[74] What Is Cyber Risk Quantification? - https://www.risklens.com/blog/what-is-cyber-risk-quantification

[75] A review of cyber security risk assessment methods for SCADA systems - https://www.sciencedirect.com/science/article/pii/S0167404815001388

[76] *NATF CIP-013-1 Implementation Guidance* - https://www.EnergyCollection.us/Companies/NATF/CIP-13-1-Implementation-Guidance.pdf

[77] Midwest Reliability Organization - MRO - 2018-09-01 Newsletter - The Benefits of Risk-Based Regulation - https://www.EnergyCollection.us/Companies/MRO/Newsletter-2018-09-01.pdf

[78] Forrester Wave - https://www.EnergyCollection.us/Best-Practices/Vulnerability-Risk-Management/Forrester-2018.pdf

[79] Wikipedia – Application Virtualization - https://en.wikipedia.org/wiki/Application_virtualization

[80] Magic Quadrant for IT Vendor Risk Management Tools – June 2017 https://www.energycollection.us/Companies/Gartner/MQ-IT-Vendor-Risk-Management.pdf /// Nov 2019 - https://www.energycollection.us/Companies/Gartner/MQ-IT-Vendor-Risk-Management2.pdf

51.18.*RiskRecon* - https://www.riskrecon.com
51.19.*Scythe* - https://www.scythe.io/platform
51.20.*SecurityScorecard* - https://securityscorecard.com
51.21.*Secuvant* -
51.22.*Skybox Security* - https://www.skyboxsecurity.com/
51.23.*SurfWatch Labs* - https://www.surfwatchlabs.com
51.24.*ThreatConnect* - https://threatconnect.com/company/
51.25.*ThreatQuotient* - https://www.threatq.com/
51.26.*Tripwire* - https://www.tripwire.com/products/tripwire-ip360/
51.27.*UpGuard* - https://www.upguard.com/
51.28.*Venminder* -
51.29.*Verve* -

52.*Sandboxing* - ToC

52.1. *Fortinet* -

53.*SCADA Protection* –

53.1. *DAQ Electronics* – http://www.daq.net
53.2. *Lofty Perch* – https://www.loftyperch.com
53.3. *LogRhythm* – https://logrhythm.com
53.4. *Radiflow* – https://radiflow.com
53.5. *SCADAhacker* – https://www.scadahacker.com/
53.6. *Ultra-Electronics 3eTI* - http://www.ultra-3eti.com
53.7. *Waterfall Security* – https://waterfall-security.com

54.*Security Analytics Platforms* [81] – ToC

54.1. *NetWitness* –
54.2. *Splunk* –

55.*Security Information and Event Management (SIEM)* [82] [83] [84] –

55.1. *AlienVault* – https://www.alienvault.com/
55.2. Alert Logic -
ArcSight – Acquired by Micro Focus - https://en.wikipedia.org/wiki/ArcSight
55.3. *BlackStratus* - https://www.blackstratus.com/
55.4. *Cisco Security Manager* -
55.5. *Dell Secureworks* – https://tinyurl.com/yabkghkt
55.6. *DNIF – NetMonastery* - https://dnif.it/index.html
55.7. *FireEye* – https://www.fireeye.com
55.8. *Fortinet* – https://www.fortinet.com/
55.9. *Graylog* -
55.10.*IBM (QRadar)* – https://www.ibm.com/security/security-intelligence/qradar
55.11.*Logz.io* -
55.12.*LogRhythm* – https://logrhythm.com/
55.13.*Micro Focus NetIQ* - https://www.microfocus.com/
https://en.wikipedia.org/wiki/Micro_Focus
NetIQ – see Micro Focus NetIQ above –
NetMonastery – see DNIF above -
55.14.*Netsurion EventTracker* –

[81] Forrester Wave - https://www.EnergyCollection.us/Best-Practices/Security-Analytics-Platforms/Forrester-2018.pdf

[82] Gartner Magic Quadrant for Security Information and Event Management - https://www.EnergyCollection.us/Energy-Security/MQ-SIEM-2017.pdf // https://www.EnergyCollection.us/Companies/Gartner/MQ-SIEM-2018.pdf

[83] G2 Crowd report for SIEM 2019 - https://twi.li/G2-SIEM-2019

[84] See Grid Report for SEIM Spring 2019 - https://learn.alienvault.com/c/siem-grid-report?

55.15.*OSSIM (Open Source)* -

QRadar – see IBM QRadar above –

55.16.*Rapid7* – https://www.rapid7.com

55.17.*RSA* -

55.18.*SolarWinds Log & Event Manager* – https://www.solarwinds.com

55.19.*Splunk* – https://www.splunk.com

55.20.*Sumo Logic* – https://www.sumologic.com

55.21.*ThreatConnect* –

55.22.*Trustwave* -

56.*Security Investment Prudency (at the state level)* – at the state level, what are the Best Practices states are following to approve/deny/evaluate security investments. ToC

57.*Security Operations Centers (SOCs)* -

57.1. *Leidos* -

58.*Security Orchestration Automation and Response (SOAR)* [85] –

58.1. *Anomali* –

58.2. *Ayehu* –

58.3. *CyberSponse* –

58.4. *Demisto* –

58.5. *DFLabs* –

58.6. *EclecticIQ* –

58.7. *IBM (Resilient Systems)* –

58.8. *Microsoft (Hexadite)* –

58.9. *Phantom* –

58.10.*Resolve Systems* –

58.11.*ServiceNow Security Operations* –

58.12.*Siemplify* - https://www.siemplify.co/

58.13.*Splunk* –

58.14.*Swimlane* - https://swimlane.com/solutions/industries/ - includes Utilities as a target market

58.15.*Syncurity* - https://www.syncurity.net

58.16.*ThreatConnect* –

58.17.*ThreatQuotient* –

UltraSOC - https://www.ultrasoc.com/company/about-us/ (not targeting Utilities)

59.*Situational Awareness* - ToC

60.*Social Engineering Protection* [86] [87] – Louisiana Technical University has taken this Topic (POP page in process). **0/6** partial list

60.1. *Agari* – https://www.agari.com/

60.2. *Cofense* (formerly PhishMe) - https://cofense.com

60.3. *IntSights* - https://www.intsights.com/solutions-use-case-phishing-detection

60.4. *IronScales* - https://ironscales.com/

60.5. *KnowBe4.com* - https://www.knowbe4.com/

60.6. *ProofPoint* - https://www.proofpoint.com/us

[85] Gartner 2017-11-01 - https://www.EnergyCollection.us/Best-Practices/Security-Orchestration-Automation-Response-SOAR/Gartner-Reprint-2017-11-01.pdf

[86] Gartner – Fighting Phishing -

[87] Magic Quadrant for Security Awareness Computer-Based Training - https://www.energycollection.us/Companies/Gartner/MQ-Security-Awareness-2019.pdf

61.Software Development / Inspection / Management [88] [89] –

- **61.1.** ***BSIMM*** - https://www.bsimm.com/about.html
  - ***Codenomicon (bought by Synopsys)*** – http://www.codenomicon.com/index.html - focuses on the software aspect of Supply Chain
- **61.2.** ***Grimm*** - https://www.grimm-co.com/services/application-security
- **61.3.** ***Indium*** - https://www.indiumsoftware.com
- **61.4.** ***National Telecommunications and Information Administration*** - https://www.ntia.doc.gov/SoftwareTransparency
- **61.5.** ***New Context*** - https://www.newcontext.com -
- **61.6.** ***Outpost24*** - https://outpost24.com/
- **61.7.** ***Rapid7*** –
- **61.8.** ***Synopsys*** - https://www.synopsys.com/software-integrity.html
- **61.9.** ***Tripwire*** - https://www.tripwire.com/products/tripwire-for-devops/
- **61.10.** ***Veracode*** -

62.State Cybersecurity Standards and Best Practices – ToC

63.Substations – Distribution –

64.Substations – Transmission -

65.Supply Chain [90] [91] [92] [93] [94] [95] [96]–

- **65.1.** ***Adolus*** - https://www.adolus.com/
- **65.2.** ***BitSight*** - https://www.bitsight.com/
- **65.3.** ***CyberArk*** - https://www.cyberark.com/solutions/security-risk-management/remote-vendor-access-security/
- **65.4.** ***Fortress Information Security*** - https://www.fortressinfosec.com/a2v/
- **65.5.** ***ISASecure*** - https://www.isasecure.org/en-US/About-Us/Mission
- **65.6.** ***Prevalent*** – https://www.prevalent.net/
  - ***ResilInc*** - https://www.resilinc.com/industry - not focused on utilities
- **65.7.** ***RiskRecon*** - https://www.riskrecon.com
- **65.8.** ***SecurityScorecard*** - https://securityscorecard.com/solutions/vendor-risk-management (do not have Utilities as a focus market)
- **65.9.** ***Sonatype*** – https://www.sonatype.com
- Supply Chain - Software Development / Inspection –

66.Tabletop Exercises / Wargaming - ToC

[88] NISTRI 8011 - Volume 3 - Automation Support for Security Control Assessments - https://www.EnergyCollection.us/Companies/NIST/NISTIR-8011-Volume3.pdf

[89] New PCI Software Security Standards - https://blog.pcisecuritystandards.org/just-published-new-pci-software-security-standards

[90] Topic initially presented at the POP BP Conference 2019-02-04 by *Andy Bochman, Senior Cyber & Energy Security Strategist, Idaho National Labs.* -

[91] Managing Cyber Supply Chain Risk-Best Practices for Small Entities - https://tinyurl.com/yb63gjqa

[92] NATF CIP-013-1 Implementation Guidance - https://www.EnergyCollection.us/Companies/NATF/CIP-13-1-Implementation-Guidance.pdf

[93] Supply Chain Risk Management (from ReliabilityFirst) - https://www.EnergyCollection.us/Companies/Reliability-First/Newsletter-2018-11-01.pdf

[94] NEMA Supply Chain Best Practices - https://www.nema.org/Standards/Pages/Supply-Chain-Best-Practices.aspx

[95] Software Supply Chain – see New PCI Software Security Standards - https://blog.pcisecuritystandards.org/just-published-new-pci-software-security-standards

[96] See also - Software Development / Inspection

67.Threat Intelligence - [97] The University of New Hampshire has taken this Topic. **00/28**

67.1. ***AlienVault***– https://www.alienvault.com –

67.2. ***Anomali*** -

BrightPoint Security – acquired by ServiceNow - https://tinyurl.com/ya75tpey

67.3. ***Cyber Edge - r-Motiv*** –

67.4. ***DeepInstinct*** –

67.5. ***Elbit Systems*** –

67.6. ***Energy - Information Sharing and Analysis Center - E-ISAC*** –

67.7. ***FireEye*** - https://www.fireeye.com

67.8. ***IntSights*** - https://www.intsights.com/automated-remediation

67.9. ***Ironer*** -

iSIGHT Partners – bought by FireEye - https://tinyurl.com/y746xp3e

67.10.*KELA* –

67.11.*Lookingglass* –

67.12.*MalCrawler* –

67.13.*OpenDNS* – https://www.opendns.com

67.14.*PinDrop* –

67.15.*Recorded Future* - https://www.recordedfuture.com/solutions/energy/

67.16.*Reversing Labs* –

67.17.*SafeBreach* –

67.18.*Splunk* -

67.19.*SecurityTrains* -

67.20.*ServiceNow* -

67.21.*STIX and TAXII* –

67.22.*Third Party Trust* –

67.23.*ThreatConnect* –

67.24.*ThreatIQ* -

67.25.*TrapWire* –

67.26.*TruSTAR* –

67.27.*VMRay* –

67.28.*ZanttZ* –

Threat Intelligence Platforms – see "Threat Intelligence" above

Threat Vulnerability Assessment – see "Risk Assessment and Quantification, and Management"

68.Training – Security-awareness in the workforce [98] - including computer-based training - ToC

68.1. ***Barracuda*** (PhishLine) -

68.2. ***Cofense*** –

68.3. ***Global Learning Systems*** -

68.4. ***Grimm*** - https://www.grimm-co.com/services/security-training-and-education

68.5. ***InfoSec Institute*** –

68.6. ***Inspired eLearning*** –

68.7. ***Junglemap*** -

68.8. ***KnowBe4*** - https://www.knowbe4.com –

68.9. ***MediaPRO*** -

68.10.*ProofPoint (Wombat Security)* –

[97] Buyer's Guide to TIPs - https://www.EnergyCollection.us/Energy-Security/Buyers_Guide_TIP.pdf

[98] Magic Quadrant for Security Awareness Computer-Based Training - https://www.EnergyCollection.us/Best-Practices/Training-Security-Awareness/Gartner-MQ-2018.pdf

68.11. ***SANS Institute*** –

68.12. ***Security Innovation*** –

68.13. ***Talos (Cisco)*** - https://www.talosintelligence.com/

68.14. ***Terranova*** -

69. Training – Cyber Workforce Development, cybersecurity talent – ToC

69.1. ***Affinity Security*** - https://affinity-it-security.com

69.2. ***Cybrary –*** https://www.cybrary.it

69.3. ***EnergySec*** –

69.4. ***Hack the Box – Penetration Testing*** - https://www.hackthebox.eu

69.5. ***ISC2*** - https://www.isc2.org/about

69.6. ***Metasploit Unleashed*** - https://www.offensive-security.com/metasploit-unleashed

69.7. ***MITRE – Ten Strategies of a World-Class Cybersecurity Operations Center*** - https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

69.8. ***No Starch Press – Hacking & Computer Security*** - https://nostarch.com/catalog/security

69.9. ***OWASP Broken Web Applications Project*** - https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

69.10. ***Pentester Academy*** - https://www.pentesteracademy.com

69.11. ***SANS Cyber Aces*** - https://www.cyberaces.org

69.12. ***Security Mentor*** –

69.13. ***ThreatGen*** - https://threatgen.com -

70. Transient Cyber Assets – ToC

70.1. ***FoxGuard Solutions*** - https://foxguardsolutions.com/tca/

71. Virtualization -

72. VPN Security -

72.1. ***Certes Networks*** –

Vulnerability Assessment – see "Risk Management" above

73. WAN Edge Infrastructure [99] – ToC

73.1. ***Cisco Systems*** – https://www.cisco.com -

73.2. ***Fortinet*** –

73.3. ***Silver Peak*** –

73.4. ***VMware*** -

74. Web Application Firewalls (WAF) [100] –

74.1. ***Fortinet*** -

75. Whitelisting –

75.1. ***Bit9*** –

75.2. ***SecurityMatters*** –

75.3. ***SignaCert*** –

75.4. ***Verve*** –

Wireless - See "Communications Systems – Wireless" above

[99] Gartner Magic Quadrant for WAN Edge Infrastructure - https://www.EnergyCollection.us/Energy-Security/WAN-Edge-Infrastructure.pdf

[100] Wikipedia - Web application firewall - https://en.wikipedia.org/wiki/Web_application_firewall

76.Zero Trust [101] [102] [103] – that nothing in a network environment should be trusted until it is validated against a list of known values. This means users, systems, and processes are all validated prior to any action being authorized, whether that is a login (access), an automated process, or a privileged activity (authorization). ToC

76.1. Akamai Technologies –
76.2. BlackRidge Technology –
76.3. Cato Networks –
76.4. Centrify - https://www.centrify.com –
76.5. Certes Networks –
76.6. Cisco –
76.7. Cloudflare –
76.8. Cyxtera Technologies - https://www.cyxtera.com/blog/three-steps-to-zero-trust?
76.9. Forcepoint –
76.10.Fortinet –
76.11.Google Cloud Platform (GCP) -
76.12.Illumino –
76.13.InstaSafe –
76.14.Meta Networks –
76.15.Microsoft –
76.16.New Edge –
76.17.Okta –
76.18.OPSWAT - https://www.opswat.com https://en.wikipedia.org/wiki/OPSWAT
76.19.Palo Alto Networks –
76.20.Perimeter 81 –
76.21.PulseSecure - https://www.pulsesecure.net/top-reasons/
76.22.Safe-TSAIFE –
76.23.Sophos –
76.24.Symantec –
76.25.Trend Micro –
76.26.Unisys –
76.27.Verizon –
76.28.VMware –
76.29.Waverley Labs –
76.30.Zentera Systems –
76.31.Zscaler -

Top

[101] Forrester Wave – Zero Trust 2018 - https://www.EnergyCollection.us/Companies/Forrester/Wave-Zero-Trust.pdf

[102] Forrester Wave – Zero Trust 2019 - https://www.energycollection.us/Companies/Forrester/Wave-Zero-Trust2.pdf

[103] Gartner – Market Guide – Zero Trust Network Access - https://EnergyCollection.us/Companies/Gartner/MG-Zero-Trust-Network-Access.pdf

Vendor List showing Topics addressed by each Vendor ToC

This list is incomplete and under development

1. ***Alert Logic*** – Topics > Cloud Security and Services /
2. ***AlienVault*** – https://www.alienvault.com - Topics > Compliance / Frameworks and Controls / Incident Response / Security Information and Event Management (SIEM) / Threat Detection / Threat Intelligence via Sharing /
3. ***Archer Energy Solutions*** - Topics > Compliance /
4. ***AssurX*** - Topics > Compliance /
5. ***Axway*** – Topics > Compliance /
6. ***Barracuda*** - https://www.barracuda.com - Targeted industries do not include Utilities/Energy – Topics > Advanced Persistent Threat Protection (APTs) /
7. ***Bitglass*** - Topics > Cloud Security and Services /
8. ***BlackStratus*** – Topics > Compliance /
9. ***Blue Coat*** – Topics > Cloud Security and Services /
10. ***bmcRemedy*** – Topics > Change Management Ticketing /
11. ***Carbon Black*** - Topics > Antivirus / Application Control /
12. ***CensorNet*** - Topics > Cloud Security and Services /
13. ***Check Point*** - Topics > Compliance /
14. ***Cisco Systems*** – https://www.cisco.com - Topics > Advanced Persistent Threat Protection (APTs) / Cloud Security and Services /
15. ***Cylance*** - Topics > Antivirus /
16. ***CypherCloud*** - Topics > Cloud Security and Services /
17. ***D3 Security*** - Topics > Compliance /
18. ***Elastic*** - Topics > Cloud Security and Services /
19. ***EnergySec*** – Topics > Compliance /
20. ***FireEye*** – Topics > Advanced Persistent Threat Protection (APTs) /
21. ***FireLayers*** – Topics > Cloud Security and Services /
22. ***Forcepoint*** - Topics > Advanced Persistent Threat Protection (APTs) / Cloud Security and Services /
23. ***FoxGuard Solutions*** **-** Topics > Building Automation Systems /
24. ***Fortinet*** - Topics > Advanced Persistent Threat Protection (APTs) /
25. ***Intellibind*** – Topics > Compliance /
26. ***Kaspersky Lab*** - Topics > Advanced Persistent Threat Protection (APTs) /
27. ***Lastline*** - Topics > Cloud Security and Services /
28. ***Leidos*** – Topics > Cloud Security and Services /
29. ***McAfee*** - Topics > Advanced Persistent Threat Protection (APTs) / Antivirus / Cloud Security and Services /
30. ***Microsoft*** - Topics > Advanced Persistent Threat Protection (APTs) / Cloud Security and Services /
31. ***Netscope*** - Topics > Cloud Security and Services /
32. ***Network & Security Technology*** – Topics > Compliance /
33. ***OpenDNS*** – Topics > Cloud Security and Services /
34. ***Oracle*** – Topics > Cloud Security and Services /
35. ***Outpost24*** - Topics > Cloud Security and Services /

36. ***Owl*** - Topics > Advanced Persistent Threat Protection (APTs) /
37. ***Palo Alto Networks*** - Topics > Advanced Persistent Threat Protection (APTs) / Cloud Security and Services /
38. ***Proofpoint*** - Topics > Cloud Security and Services /
39. ***Qualys*** - Topics > Cloud Security and Services / Compliance /
40. ***Saviynt*** - Topics > Cloud Security and Services /
41. ***ServiceNow*** – Topics > Change Management Ticketing /
42. ***StackRox*** - Topics > Cloud Security and Services /
43. ***Symantec*** - Topics > Advanced Persistent Threat Protection (APTs) / Antivirus / Cloud Security and Services /
44. ***Trend Micro*** – Topics > Cloud Security and Services /
45. ***Webroot*** - Topics > Advanced Persistent Threat Protection (APTs) /
46. ***Zscaler*** - Topics > Cloud Security and Services /

Top

Vendors offering cybersecurity product(s), but not either focused, available, or interested in the North American Utility Market ToC

This list is incomplete and under development

1. ***Ir.deto*** - https://irdeto.com/video-entertainment/cyber-services/
2. ***KeySight Technologies*** - https://www.keysight.com/us/en/industries.html
3. ***Peregrine -*** http://www.gbpts.com/#about

Additional Resources Related to an ICS/OT Cyber-Taxonomy ToC

Additional References: ToC

1. CISO Platform - https://www.cisoplatform.com
2. Gartner on "OT Security Best Practices" - https://www.gartner.com/doc/reprints?id=1-5ZF6P01&ct=181224&st=sb
3. MITRE ATT&CK Evaluations - https://attackevals.mitre.org/evaluations

Cybersecurity Vendors involved in Critical Infrastructure, but not in the US: ToC

1. ***Applied Risk*** - https://applied-risk.com –
2. ***RedCon*** - http://www.redconsa.sg/homepage/ -
3. ***Secunet*** - https://www.secunet.com/en/ -

Top

Notes Related to This Taxonomy and Further Development

Protect Our Power seeks a credible "Owner" to take ownership of this Taxonomy as co-branded with Protect Our Power as the originator. Criteria for a new owner include commitments to:

1. Continue to develop the Taxonomy with the North American Electric Utilities as the prime focus.
2. Publish as updated and without charge to anyone.
3. Be open to changed submitted by Vendors.
4. Include an Advisory Board that has final say in any disputed updates/changes to the Taxonomy. The Advisory Board will be an even number of individuals with 50% being named by Protect Our Power and 50% by the Taxonomy owner.
5. Continue to develop a Mind Map putting the different Topics in logical order for easier consumption.

Otherwise, the new owner may utilize the Taxonomy for its own purposes including branding, marketing, etc.

Presently the Taxonomy is managed by Protect Our Power using an Advisory Board found at this link: https://protectourpower.org/bestpractices/taxonomy-advisory-board

Top