Palo Alto Networks Cybersecurity Academy

Securing the Future Of the Energy Sector

Miguel Ochoa

January 2025

About me:

Name: Miguel Ochoa

College: Florida international University

Hometown: Miami, FL

Fun fact: I like to play pool.

Understanding the Energy Sector

Critical Infrastructure

Powering Homes and Industries

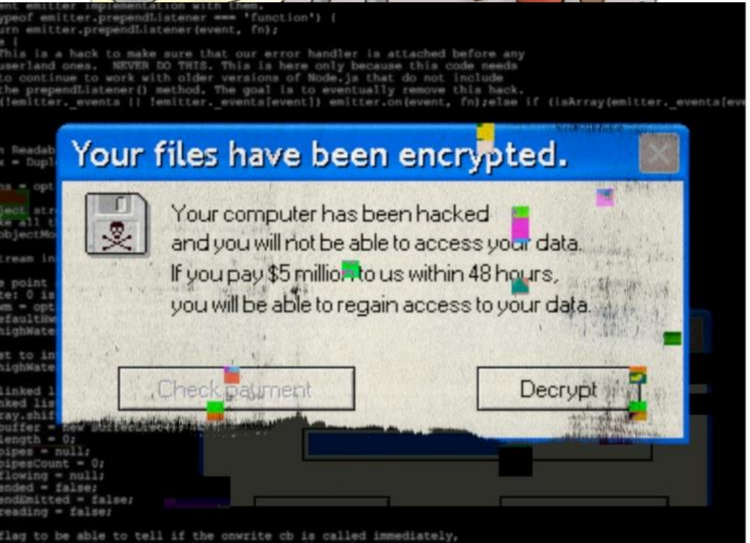
Cyber Threats

Targeting IoT & SCADA Systems

Why it Matters:

Securing National Resilience

*"Strengthening cybersecurity in the energy sector is **not an option—it's a necessity** to ensure resilience and national security."*



```
ent emitter implementation with them.
ypeof emitter.prependListener === 'function') {
urn emitter.prependListener(event, fn);
e {
This is a hack to make sure that our error handler is attached before any
userland ones.  NEVER DO THIS. This is here only because this code needs
to continue to work with older versions of Node.js that do not include
the prependListener() method. The goal is to eventually remove this hack.
(!emitter._events || !emitter._events[event]) emitter.on(event, fn);else if (isArray(emitter._events[eve
```

Your files have been encrypted.

Your computer has been hacked and you will not be able to access your data. If you pay $5 million to us within 48 hours, you will be able to regain access to your data.

```
length = 0;
pipes = null;
pipesCount = 0;
flowing = null;
ended = false;
endEmitted = false;
reading = false;

flag to be able to tell if the onwrite cb is called immediately,
```

Threats to Energy Infrastructure

1 | **Cybersecurity Threats**

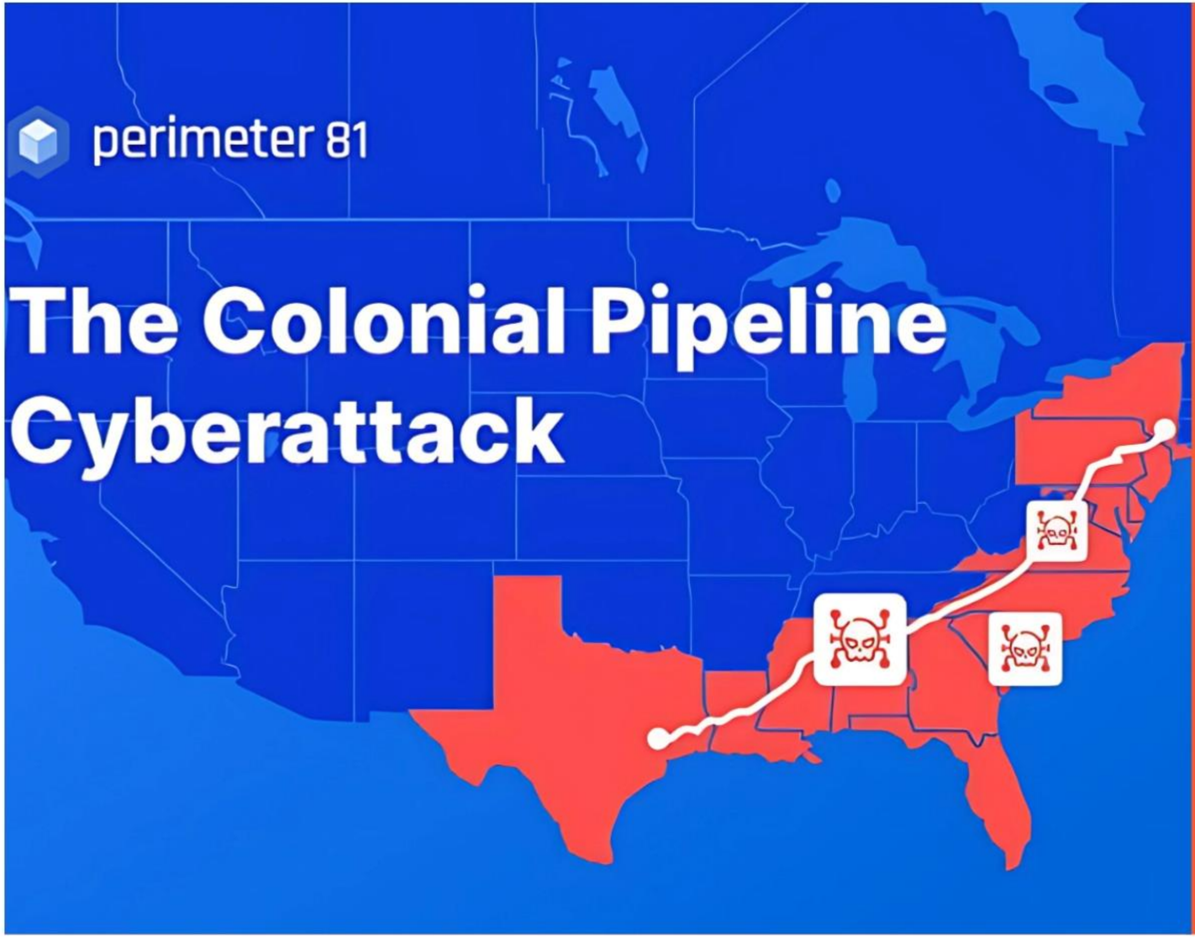
2 | **Advanced Persistent Threats (APTs)**

3 | **Insider Threats**

4 | **Supply Chain Vulnerabilities**

5 | **Outdated Systems**

6 | **Regulatory Compliance Issues**



A Reminder Of The Devastating Impact of unpreparedness.

Preventing Vulnerabilities

Operation

Centralized monitoring to detect abnormal activities

Data

Secure Data using AI Driven tools

Global Compliance

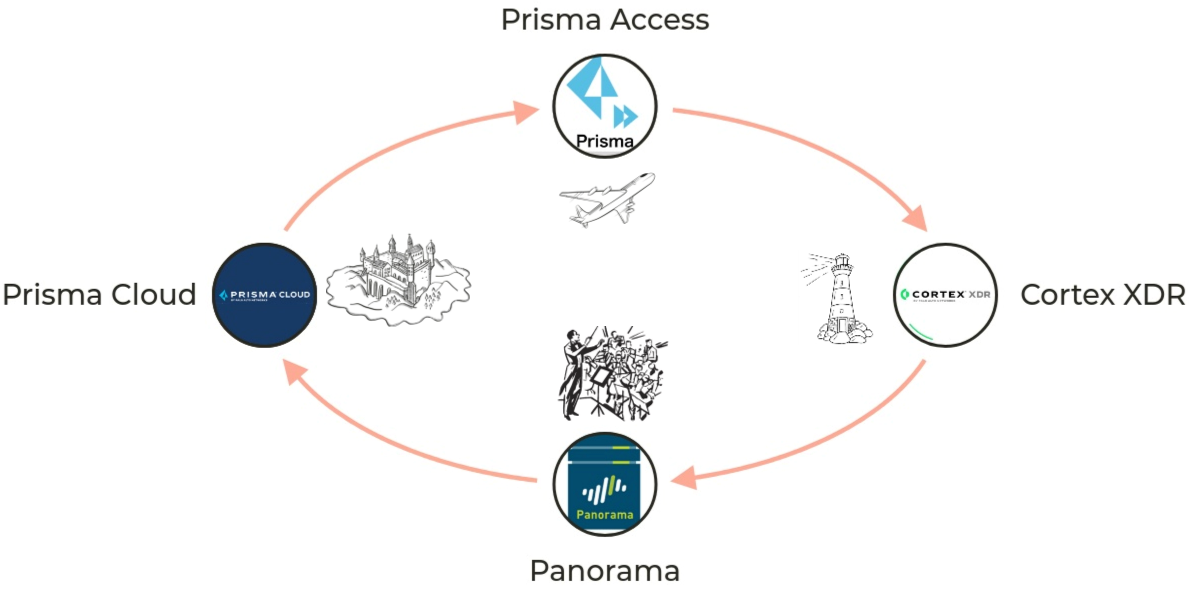
Ensure Adherence to global standards

Frameworks

Integrate Cloud Solutions for Resilience and Recovery

"Addressing these silos strengthens ***resilience*** *against cyber threats"*

Operation Solutions



Prisma Access

Cortex XDR

Panorama

Prisma Cloud

*"In cybersecurity, no single tool provides complete protection—**collaboration** is the cornerstone of **resilience."***

Data Solutions

CORTEX XSOAR
BY PALO ALTO NETWORKS

XSIAM

PRECISION AI

"Empowering data with intelligent solutions ensures ***security, efficiency, and innovation*** *in a connected world****. "***

Global Compliances

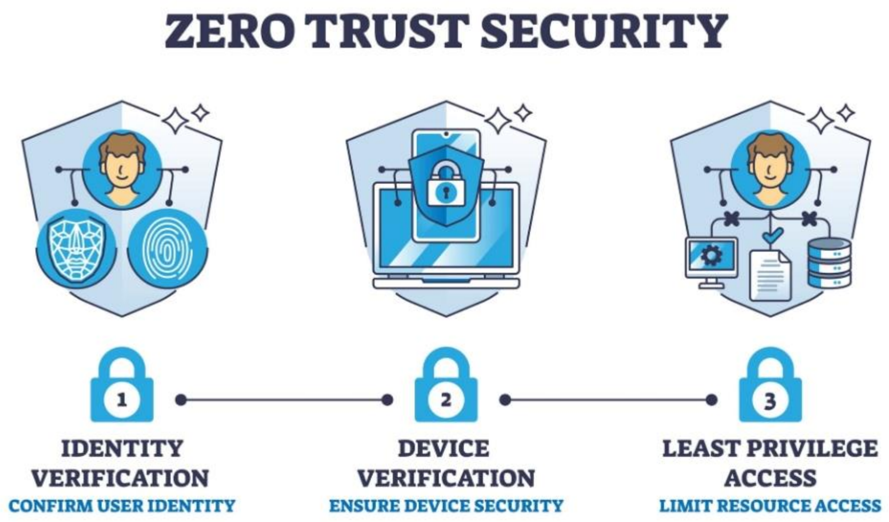
CMMC

ISO

NERC

*"Compliance is not just a checkbox; it is a **cornerstone** for **resilience** in critical sectors like energy"*

Key Frameworks



ZERO TRUST SECURITY

1 IDENTITY VERIFICATION
CONFIRM USER IDENTITY

2 DEVICE VERIFICATION
ENSURE DEVICE SECURITY

3 LEAST PRIVILEGE ACCESS
LIMIT RESOURCE ACCESS

*"Building **resilience** starts with frameworks that enforce **trust and adaptability** across every layer of security"*

Threat Intelligence

"In cybersecurity, intelligence sharing is not just a strategy;
it's a ***shield*** *that strengthens* ***resilience*** *across sectors****."***

Future-Proofing the Energy Sector

Quantum Encryption

Deploy quantum-safe encryption for critical data.

Zero Trust Evolution:

Enhance access control and segmentation across.

AI-Driven Predictive Analytics

Use XSIAM and AI to detect and prevent threats.

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

The Call To Action

1/ Palo Alto Solutions

Leverage XSIAM, XSOAR, and Prisma Access.

2/ Strengthen Collaboration

Partner with JCDC and E-ISAC.

3/ Cyber Development

Train in Zero Trust and SOAR.

4/ Commit to Innovation

Embrace AI, SASE, and quantum encryption

5/ Stay Very Proactive

Audit and segment networks

Collaboration, innovation, and resilience—together, we secure the future!

References

Cybersecurity and Infrastructure Security Agency. “Energy Sector.” U.S. Department of Homeland Security, http://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector.

Perimeter81. "Colonial Pipeline, the Ransomware Task Force, and Your Business." *Perimeter81*, 21 May 2021, www.perimeter81.com/blog/news/colonial-pipeline-the-ransomware-task-force-and-your-business.

National Conference of State Legislatures. "Human-Driven Physical Threats to Energy Infrastructure." *NCSL*, 22 Feb. 2023, www.ncsl.org/energy/human-driven-physical-threats-to-energy-infrastructure.

“Attack on Colonial Pipeline: What We’ve Learned.” U.S. of Homeland Security, 2023, www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

“MITRE ATT&CK.” MITRE, 2023, MITRE ATT&CK®

“Top 10 Security Threats for the Energy Sector.” Kaseware, www.kaseware.com/post/top-10-security-threats-for-the-energy-sector.

“China Hacking Group Volt Typhoon.” Politico, 2024, www.politico.com/news/2024/08/09/china-hacking-group-cybersecurity-0017345

“What Is SASE?” Palo Alto Networks, www.paloaltonetworks.com/cyberpedia/what-is-sase.

“How to Implement Zero Trust.” Fortinet, www.fortinet.com/resources/cyberglossary/how-to-implement-zero-trust.

“Microsegmentation and Zero Trust for Oil, Gas, and Energy Sectors.” Elisity, www.elisity.com/blog/microsegmentation-and-zero-trust-critical-cybersecurity-strategies-for-oil-gas-and-energy-sectors.

Schmid, Frank. "The Future of Cryptography and Quantum Computing." Gen Re, September 2023, www.genre.com/us/knowledge/publications/2023/september/the-future-of-cryptography-and-quantum-computing-en.