modiüs

Data Center Infrastructure Management – Threats, Vulnerabilities and Risks

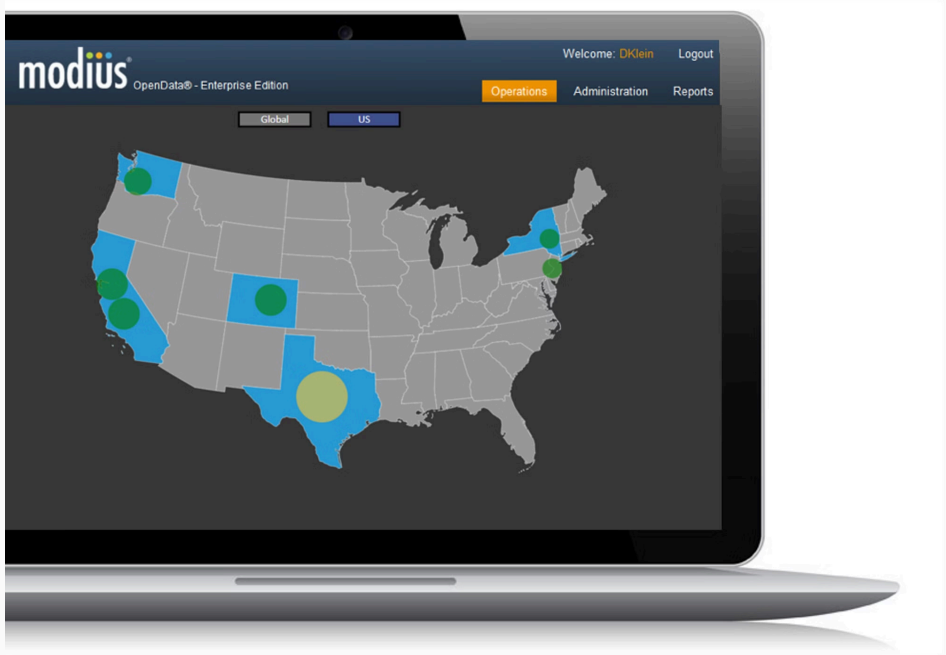
DCD Connect, Virginia, November 6, 2024

Presenters

Craig Compiano, CEO Modius

Tyson Macaulay, CISA, P.Eng

Who is Modius?



Modius provides the solutions for managing the availability, capacity and efficiency of critical facilities

- Based in San Francisco, CA
- Deployed in production environments since 2007
- Veteran Owned Small Business (**VOSB**)
- Product: *OpenData*®

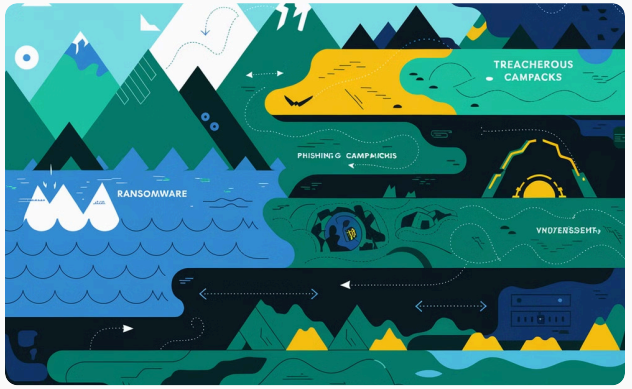
Objectives for the Session

Changing Attack Surface

Understand the ever-evolving threats to data center security.

Data Center Threats

Identify the threats that most affect data centers



Vulnerability Landscape

Analyze the latest vulnerabilities that challenge data center security.

Can DCIM play a role in managing these risks?

Data Center infrastructure is complex

Single and Multi-tenancy

Resources can be shared among tenants, who have limited visibility into hardware and infrastructure.

Mission critical

Data Center systems are designed for large-scale data processing, making them essential commercial and research applications.

High Bandwidth and High Performance

Data Centers use big pipes and provide powerful computing for complex systems for service delivery and research.

IT and OT

DC systems often employ diverse platforms: from commodity IT hardware to specialized OT sensors and actuators for power, cooling, and building management.

The attack surface is changing in DCs

More automation

Necessary to drive efficiency, scalability and savings.

More inter-connection

Brings a mix of legacy systems with new automation and management solutions.

More risk

The criticalities, vulnerabilities and threats facing data centres have never been higher.

Modius is committed to raising awareness and finding solutions.

Data Centers have become designated "Critical Infrastructure"

- U.S. Sectors (16)
  1. Energy
  2. Dams
  3. **Information Technology**
  4. Communications
  5. Finance
  6. Healthcare
  7. Food
  8. Water
  9. Transportation
  10. Safety
  11. **Government** [1]
  12. Chemical
  13. Critical Manufacturing
  14. Defense Industrial Base
  15. Nuclear
  16. Commercial Facilities

- Australian Sectors (11)
  1. Communications
  2. **Data storage or processing**
  3. Defense
  4. Energy
  5. Financial services and markets
  6. Food and grocery
  7. Health care and medical
  8. Space technology
  9. Transport
  10. Water and sewerage
  11. **Education and research** [2]

- UK Sectors (13)
  1. Chemicals
  2. Civil Nuclear
  3. Communications
  4. **Data Centers** (Sept 2024)[3]
  5. Defence
  6. Emergency Services
  7. Energy
  8. Finance
  9. Food
  10. Government
  11. Health
  12. Space
  13. Transport
  14. Water

Threats to Data Center Operations

Denial of Service

CSPs report new level of threat

2024 - Verizon:botnet armies have reached the 1 Billion devices level. [1]

2024 - Microsoft:new focus on application-layer attacks versus network-layer attacks [2]

Ransomware

Extorting cash for (possible) decryption of your data

2021 - University of California, San Francisco paid a $1.14 million ransom. [3]

2024 - Synnovis pathology, hundreds of cancelled surgeries [4]

Crypto-jacking

Stealing resources to mine crypto-currency

2020 - Supercomputing sites in Germany, U.K., and Switzerland report that systems were compromised for cryptojacking purposes. [5]

2023 - Azure acknowledges the prominence of crypto-jacking theft-of-service - and how to detect it. [6]

Storage poisoning

Data sabotage

2024 - 0.01% attacks by Google. Sensitivity of AI datasets . [7]

Cyber-Physical Security

Complex and expensive

2023 - "direct" OT attacks increase through supply-chain and insiders [8]

Compliance

Multi-level / Multi-facet

International / Federal / State

Physical / Logical

Environment

National Security / CIP

Data Center Vulnerabilities

APIs

Exposure to compromised Enterprise systems and tools.

OT Firmware

Power, Cooling, Facilities are "soft" targets.

3rd Party Attack Surface

Vendors and suppliers become attack-pathways

Lagging Indicators

Delays from minutes to days compromise situational awareness.

Corruption of Results

Trust in workloads and results erodes.

Data Leakage and Lateral Movement

Multi-tenant resources can facilitate unintended access

Open Source Software

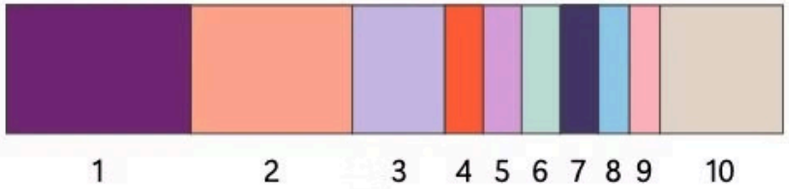
Widely used in both infrastructure management and applications

Sample Data Center Infrastructure Vulnerabilities - late 2024

- NVDIA
  - Sept 2024 - Container toolkit CVE 8.3/10. [1]
  - June 2024 - VGPU driver CVE 7.8/10 [2]
  - Jan 2024 - Bluefield DPU BMC 7.2/10 [3]
  - Jan 2024 - A100 GPU BMC 7.8/10 [4]
- Mellanox (switches)
  - Sept 2024 - Mellanox OS v3.1 - CVE 8.8/10 [5] [6]
  - Infiniband UFM
    - Aug 2024 - cairo [7]
    - Aug 2024 - httpd [8]
- SuperMicro chassis
  - July 2024 - BMC firmware - "under analysis" - [9]
- Juniper switches
  - 2024 Juniper QFX5130 [10]
  - 2023 Juniper SRX 4600 [11]
  - Oct 2024 - Junos [12] [13] [14]
- DCIM
  - Nagios [15]
  - Zabbix [16]
  - OpenBCM [17] [18] [19]
  - ServiceNow DC Now [20]
  - CyberPower PowerPanel [21]
  - Schneider Data Centre Expert [22]
- Operational Technology
  - PDU examples [23] [24]
  - BMS examples [25] [26]
  - HVAC sensors [27]
  - IoT Gateways [28]

Evolving Cyber Threat Landscape

Top 10 targeted sectors worldwide

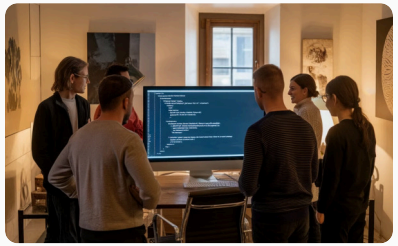


	Sector	Percentage
1	IT	24%
2	Education and Research	21%
3	Government	12%
4	Think tanks and NGOs	5%
5	Transportation	5%
6	Consumer Retail	5%
7	Finance	5%
8	Manufacturing	4%
9	Communications	4%
10	All others	16%

Source: Microsoft Digital Defense Report 2024 [1]

The Modius OpenData Difference

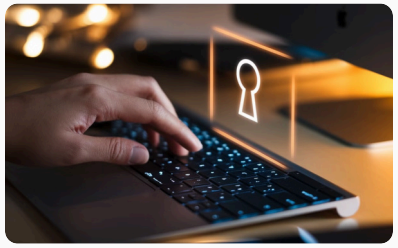
Security hardened and tested



Integrated best-in-class API security

OT device and subnet monitoring

Encrypted communications



Multi-Factor Authentication

Zero-touch firewall provisioning

Forensic logging and analysis

Recap

Data center infrastructure is increasingly complex and distributed.

This makes it challenging to secure.

The attack surface for data centers has expanded significantly.

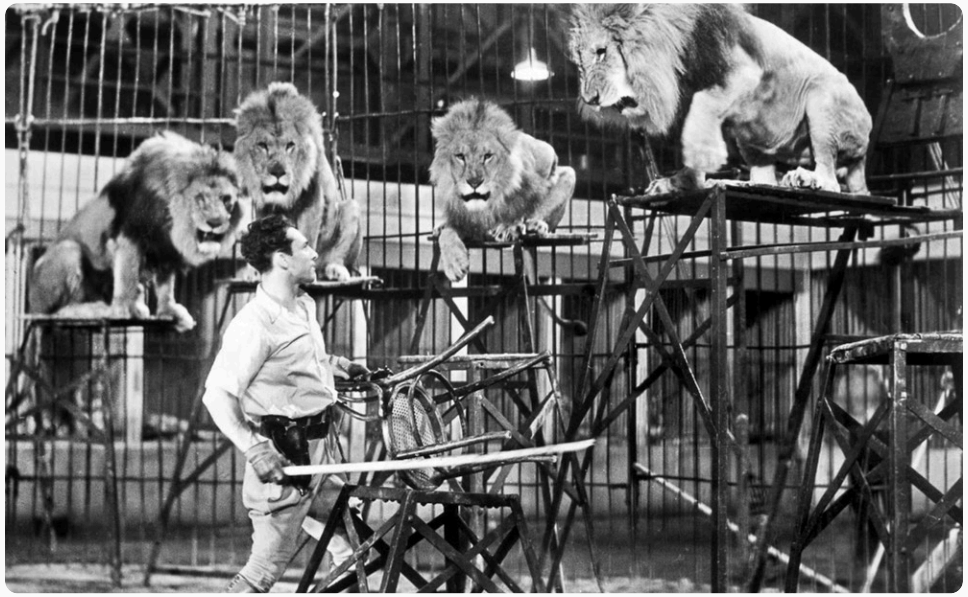
The attack surface is not just the IT infrastructure, but also Operational Technology.

Modern cyberattacks are sophisticated and targeted.

Threat actors are increasingly focused on disruption, data exfiltration, and ransomware.

Make DCIM a trusted part of the cyber security solution for Data Centers.

Call to Action



Review Your Security Assumptions

Are you confident that your data center infrastructure is secure against modern cyber threats? Are you protected against major vulnerabilities like **APIs, third-party suppliers, firmware vulnerabilities and lagging indicators**?

Use DCIM Tools to Close Security Gaps

DCIM platforms like **Modius OpenData** should be trusted systems and inoculate OT against attacks and contribute to creating a more resilient data center.

Questions?

Note: You will receive a copy of this presentation.

Complete the survey and we will send you a copy of **RIoT Control: Risk and the Internet of Things**

Contact data:

info@modius.com

888.323.0066