



Idaho National Laboratory (INL) Cybersecurity Support to the Department of Homeland Security (DHS)

April 2022

Changing the World's Energy Future

Timothy R Klett



INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

Idaho National Laboratory (INL) Cybersecurity Support to the Department of Homeland Security (DHS)

Timothy R Klett

April 2022

**Idaho National Laboratory
Idaho Falls, Idaho 83415**

<http://www.inl.gov>

**Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517**



April 2022



Idaho National Laboratory (INL) Cybersecurity Support to the Department of Homeland Security (DHS)

Idaho National Laboratory (INL) Cybersecurity Support to the Department of Homeland Security (DHS)



Controls Environment Laboratory Resource (CELR)



Aviation Cybersecurity Research Test Bed (ACRT)



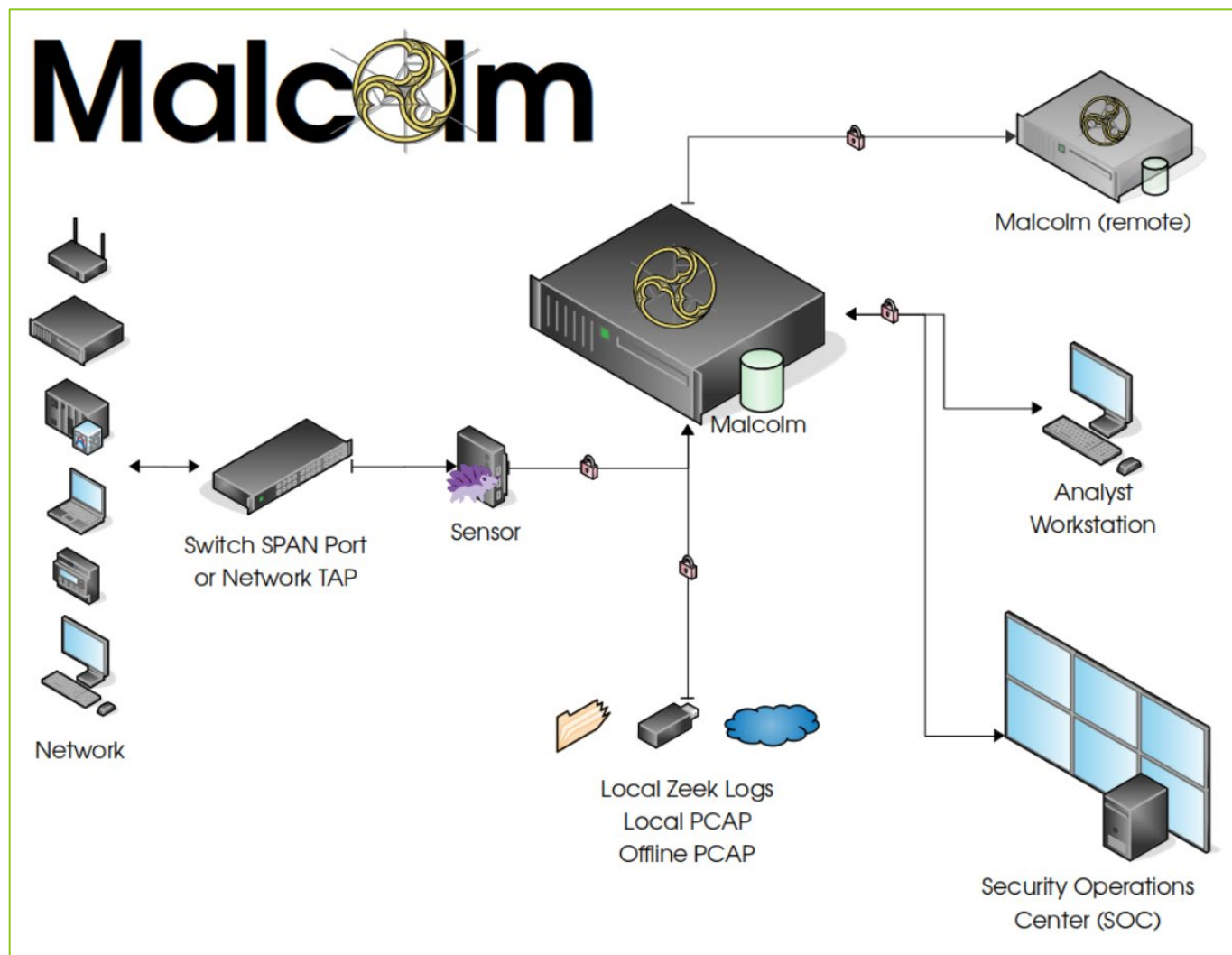
Modular and
Expandable

Generate
Custom Traffic

Real-World
Data Link
Traffic
Repository

Monitoring Taps/
Instrumentation

Malcolm

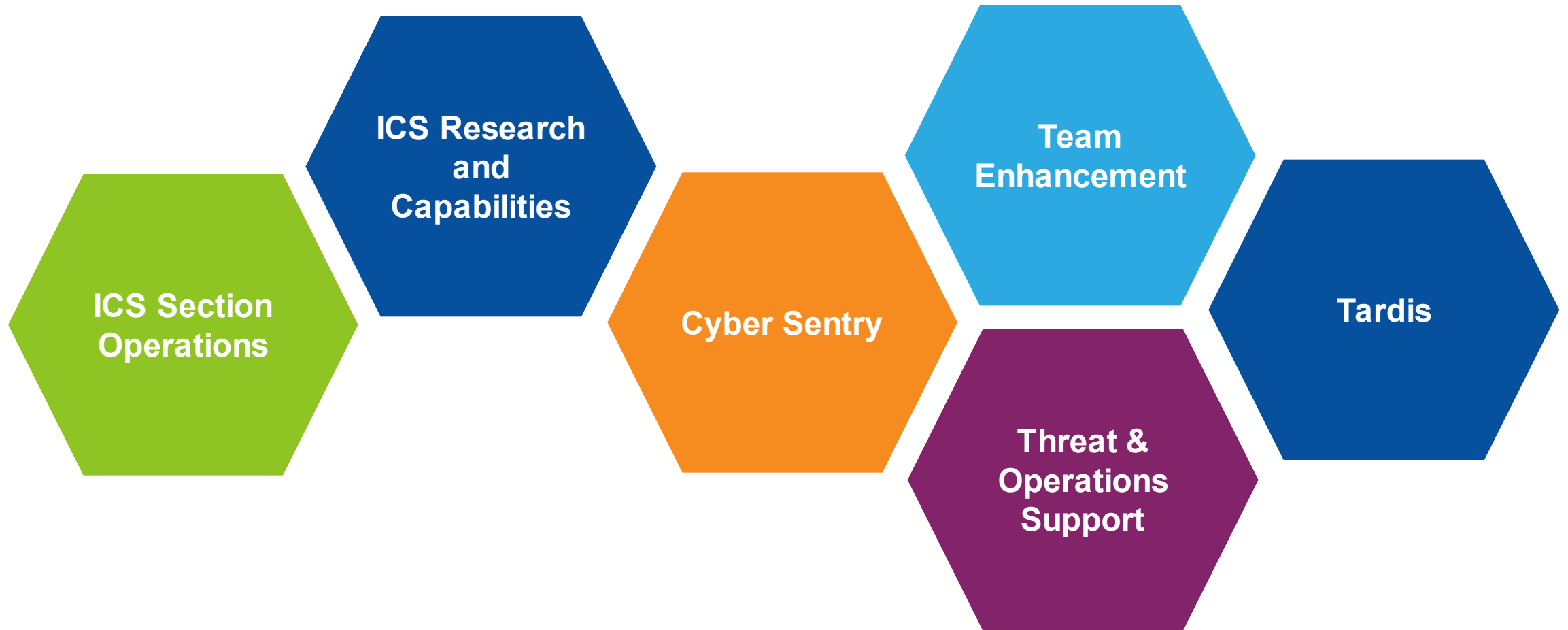


Malcolm

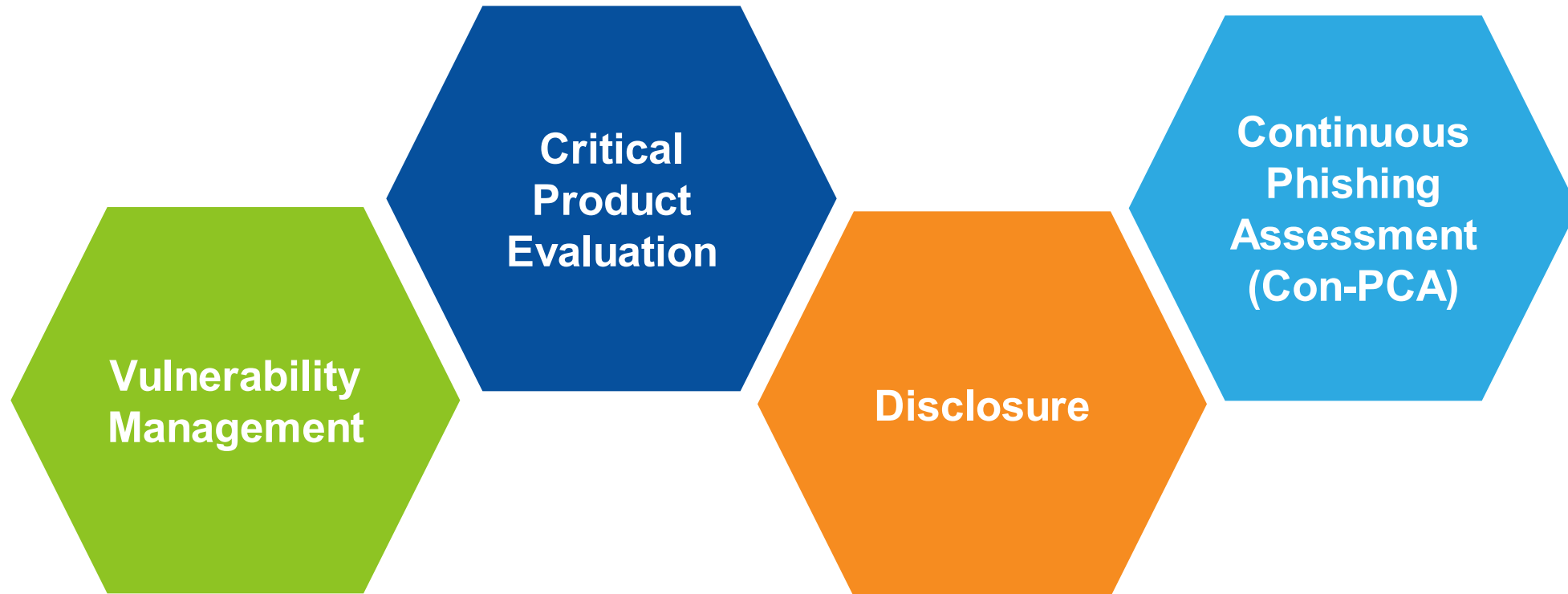
Malcolm is a powerful, easily deployable network traffic analysis tool suite for full packet capture artifacts (PCAP files) and Zeek logs.

- Home
- Getting Started
- Components
- Supported Protocols
- Documentation
- Hedgehog Linux
- Downloads
- Contributions
- ↳ GitHub

Threat Hunting – Industrial Control Systems (ICS) Section Operations



Vulnerability Management



Cyber Security Evaluation Tool

CSET Tools Resource Library Help INEL-NTVHANSBK

Prepare Assessment Results

Assessment

- Practices
- Standard Questions
- Diagram Component Questions

Results

- RRA Results
- Goal Performance
- Assessment Tiers
- Performance Summary

Standards Results

Ranked Categories

Category	Score
System Protection	15
Management Practices	14
Securing the System	13
Risk Management and Assessment	12
Plans	11
Configuration Management	10
Information Protection	9
Account Management	8
Training	7
Remote Access Control	6
Portable/Mobile/Wireless	5
Environmental Security	4
Incident Response	3
System Integrity	2
Procedures	1
Software	1
Respond	1
Information and Document Management	1
Protect	1

Ransomware Readiness Assessment

Robust Data Backup (DB)

Be prepared to recover gracefully from an incident. Employ a backup solution that automatically and continuously backs up your business critical data and system configurations. Ensure the backed-up data is stored securely (encrypted) offsite or in the cloud and allows for at least 30 days of rollback. Periodically test your ability to recover data from backup.

DB-S-Q01: Are important systems and data backed up daily to an offsite location with the ability to restore multiple versions back at least 30 days?

DB-S-Q02: Are data backups tested annually?

Web Browser Management and DNS Filtering (BM)

Approves domains names, and known malicious domains names that will make you vulnerable to malware (such as DNS Blocking or DNS Firewall), with integrated threat intelligence. A number of effective commercial solutions are recommended action.

Conduct ongoing phishing and social engineering campaigns that randomly and periodically send simulated left which will assist in recognizing and reporting phishing attacks. Utilize an SMTP (mail server) proxy that left and content filtering features.

Some scenarios conducted?

EDM ASSESSMENT

The External Dependency Management Assessment

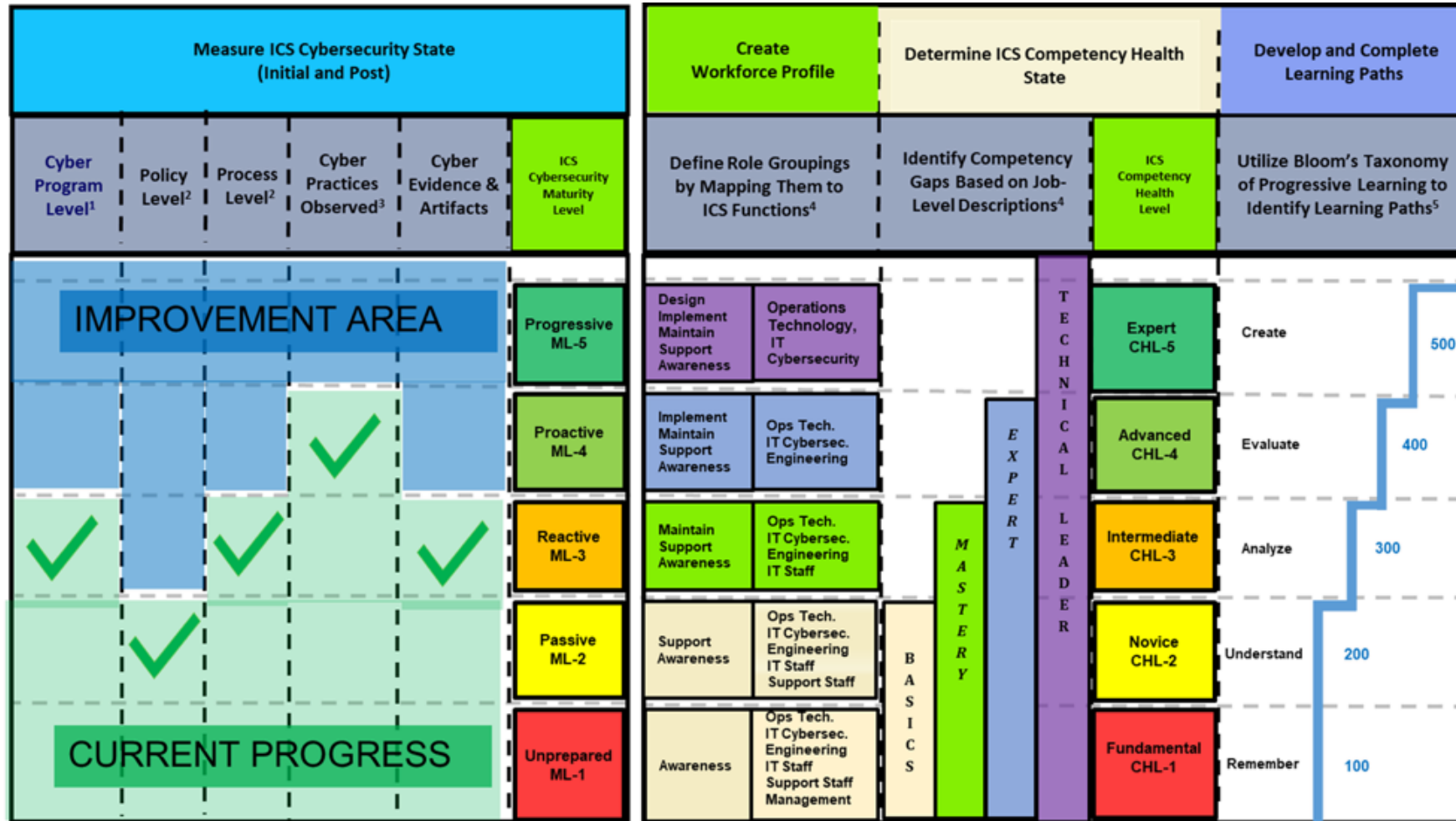
Ransomware Readiness Assessment

Ransomware poses an increasing threat and continues to rise as a top cyber threat impacting both businesses and government agencies. Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. In some instances, attackers may also steal an organization's information and demand an additional payment in return for not disclosing the information to authorities, competitors, or the public. Ransomware disrupts or halts an organization's operations and poses a dilemma for management: pay the ransom and hope that the attackers keep their word about restoring access and not disclosing data, or do not pay the ransom and restore operations themselves. The methods used to gain access to an organization's information and systems are common to cyberattacks more broadly, but they are aimed at forcing a ransom to be paid. Ransomware attacks target the organization's data.

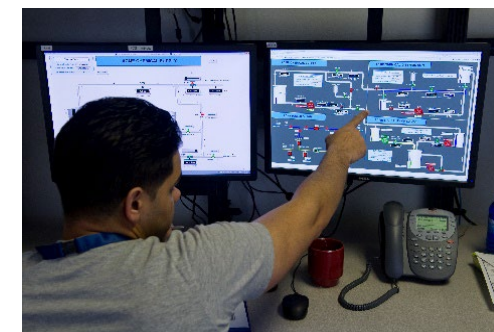
To understand your cybersecurity posture and assess how well your organization is equipped to defend and recover from a ransomware incident, take the Ransomware Readiness Assessment (RSA).

Cyber-CHAMP[®]

The Cybersecurity Competency Health and Maturity Progression Model



Training



INL Resilience Optimization Center (IROC)

A National Center for Advancing Systems Resilience and Risk Management

Tackling infrastructure resilience challenges through applying laboratory-wide capabilities and expertise



INL has the Nation's Premier Critical Infrastructure Environment for DHS, DOE, DoD, and Industry

INSPIRE

Interconnected Systems: Physical-Cyber Infrastructure Research Environment

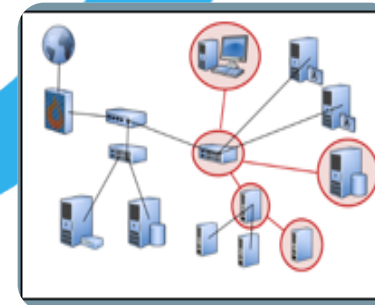
PHYSICAL



Research • Analysis • Testing • Validation



CYBER





Idaho National Laboratory