CHIEF INFORMATION SECURITY OFFICER (CISO) — IT COMPLIANCE

MERIT 2.0

Cybersecurity can help protect networks and devices from increasingly sophisticated cyber-attacks. The latest attacks use malevolent social engineering and artificial intelligence to try to circumvent traditional security. Business risks will continue to increase as newer generations of smart Internet-enabled devices gain access to your networks via Bluetooth and Wi-Fi.

Cybersecurity can protect personally identifiable information (PII), protected health information (PHI), intellectual property, and business information systems from theft by criminals. MERIT uses the latest tools and an increasing series of Compliance attestations to protect our clients and their data.

A MERIT security governance leader directs the implementation and enforcement of technology and cyber security standards and procedures. By analyzing the needs of departments, lines of business, and future goals, our CISO helps determine ways to meet business objectives by aligning information processing systems following best practices and statutes at the state, national, and international levels.

ISACA – CERTIFIED INFORMATION SECURITY MANAGER (CISM)

ISACA ID: 979363, Member since 5 June 2016

https://www.credly.com/badges/3b542515-a958-4b7f-b608-a3b718a60584

ISACA is a global association which develops industry-leading knowledge and practices for information system experts. The CISM certification acknowledges experienced information security managers, CISOs and CIOs.

A certified CISM must demonstrate a minimum of 5-years of professional information security management within the 10-year period preceding the application date and comply with ongoing training requirements by performing a minimum of twenty (20) CPE annual hours and one hundred and twenty (120) CPE hours over a three-year period. The hours must be appropriate to the CISM's knowledge and ability to perform CISM and CISO related tasks.

CMMC Accreditation Body – Registered Practitioner (RP)

CMMCAB Member #: 8836

https://cmmcab.org/marketplace/gabriel-miller/

The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD A&S) maintains that IT security is paramount to protect American businesses.

The MERIT CISO is a Registered Practitioner (RP) authorized to deliver non-certified advisory service based on the CMMC standard. MERIT will work with a Certified CMMC Professional (CCP) or Certified CMMC Assessor (CCA) to deliver advice based on rigorous training under a CMMC-AB Certified Assessment.

MERIT ESP - Enhanced Security Platform+

IT'S A HEAVY RESPONSIBILITY TO OVERSEE YOUR CYBER SECURITY, SO MERIT HAS ASSEMBLED A TEAM OF EXPERTS AND EQUIPPED THEM WITH THE INDUSTRY'S BEST TOOLS TO ENSURE THE SECURITY OF YOUR DATA. A PLAN THAT WAS "GOOD-ENOUGH" A FEW YEARS AGO IS NO LONGER AN ADEQUATE SOLUTION TO PREVENT BAD ACTORS FROM HOLDING YOUR DATA HOSTAGE. THE MERIT APPROACH ENCOMPASSES MULTIPLE TOUCH POINTS TO STRENGTHEN YOUR DEFENSES ACROSS THE BOARD.

1 TEACH
We educate your coworkers to emphasize their role in keeping your business safe

2 LOCK-UP
Firewalls, anti-malware, and cyber shields help prevent business disruptions by making it hard to break into your business

3 SAFETY NET
Back-up key data to use when emergencies occur combined with email continuity

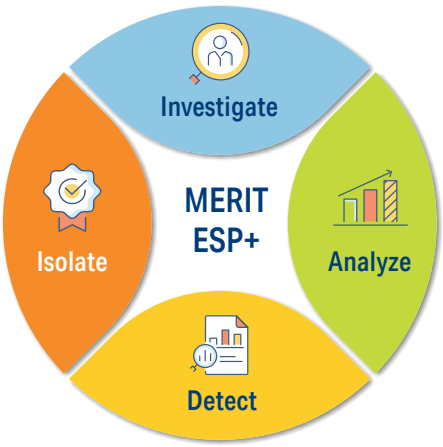
4 SCAN
Constant vigilance of the Dark Web and your Microsoft Cloud for compromises

5 ANALYZE
Artificial Intelligence vector-analysis to determine if worms are lurking inside your systems

6 DETECT
We watch your wireless access points (WAPs) for malicious log-ins and brute-force attacks

7 ISOLATE
Threats and remove them from your network

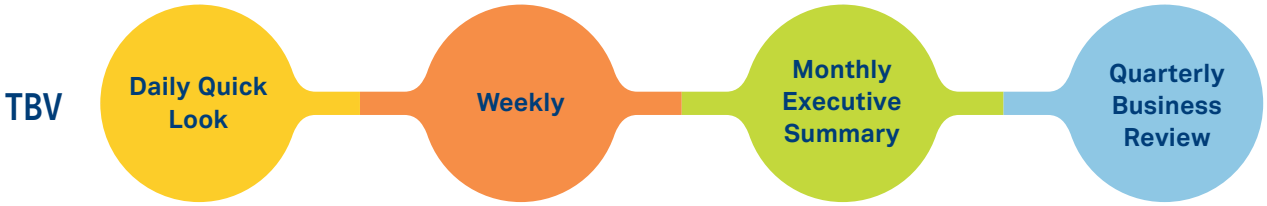
8 REACT & ADJUST
Incident Response, notification, and knowledge base



Ransomware attacks have exploded in recent years, and average ransomware payments now exceed $275,000. To help our clients, MERIT has expanded capabilities to detect and help prevent today's malware, ransomware, phishing, crypto-threats, password crackers and other advanced persistent threats – but we need your help.

We can educate your team and upgrade your cyber defenses today.

We invest time and money to ensure MERIT's cyber tools are upgraded to help keep you safe. And the MERIT Trust But Verify (TBV) reporting illuminates the threats we have overcome and a scorecard of your current defenses.



MERIT 2.0

CONTACT MERIT TODAY TO DISCUSS YOUR SECURITY OPTIONS.

meritsolutions.net | 1407 Stephanie Way, Suite E, Chesapeake, Virginia 23320

Zero-trust incorporated into the MERIT security stack

WHAT THIS MEANS TO YOU:

As part of our evolving capabilities to secure IT systems, we implemented a zero-trust policy to the MERIT security stack. Bad actors and cyber-attacks are more sophisticated, and so is the capability required to thwart software-based threats. As your IT Partner, we understand higher grades of security are fundamental in protecting you from the latest threats and the techniques we implemented were developed for large government organizations, F5000 companies and enterprise organizations.

ZERO-TRUST IS A SECURITY FRAMEWORK THAT STATES:

Organizations should not trust any entity inside or outside of their perimeter at any time.

MERIT provides the IT controls needed to secure, manage, and monitor each device, user, app, and network and our ThreatLocker provides:

- LAYERED SECURITY
- INTERNAL DISPUTES
- RANSOMWARE PREVENTION
- STORAGE CONTROL
- COMPLIANCE
- DATA PRIVACY

About MERIT 2.0

MERIT was founded in 1983 and was re-branded in 2020 as MERIT 2.0. Our Mission Statement is *To educate every worker at every client and provide them the technology to improve.*

How to Contact MERIT 2.0

SERVICE/REPAIRS/HELPDESK:
e: service@meritsolutions.net
p: 757-420-5150
w: www.meritsolutions.net

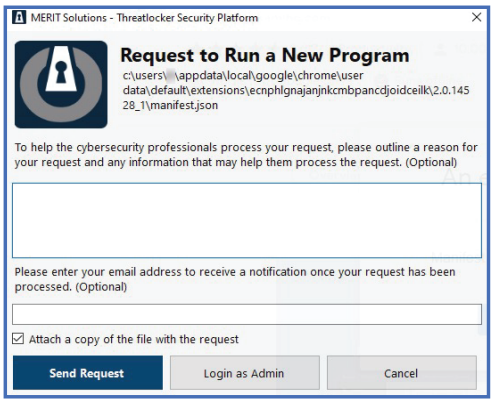
MARKETING:
e: marketing@meritsolutions.net
p: 757-420-5150 x7007

HOW DOES THREATLOCKER WORK:

When you try to install or update a program that is unknown or is not a previously accepted application, you will encounter a popup (see below). This indicates that ThreatLocker has detected an attempt to install software or perform an action that needs to be reviewed by MERIT before allowing you to proceed.

1. Click **Request Access** to submit your application for MERIT review
2. Click **Don't Show Again** to ignore

If you need to use the tool or app which was blocked, click:



1. **Request Access** so MERIT can review your request
2. Enter the required information
3. Press the **Send Request** button to submit

ThreatLocker will block unapproved software, including ransomware, viruses, and other malicious software, from running on your PCs.

Selecting the "Request Access" button and providing the necessary information will notify MERIT support. We will review the request and ensure the application is not malicious in nature and approve it if appropriate.

As such, it is vital to let us know in advance if you need any new software installed by entering a ticket with the service desk.

About MERIT 2.0

MERIT was founded in 1983 and was re-branded in 2020 as MERIT 2.0. Our Mission Statement is *To educate every worker at every client and provide them the technology to improve.*

How to Contact MERIT 2.0

SERVICE/REPAIRS/HELPDESK:
e: service@meritsolutions.net
p: 757-420-5150
w: www.meritsolutions.net

MARKETING:
e: marketing@meritsolutions.net
p: 757-420-5150 x7007