DoD-DEFENSE INDUSTRIAL BASE COLLABORATIVE INFORMATION SHARING ENVIRONMENT (DCISE)

DOD CYBER CRIME CENTER

DoD-DEFENSE INDUSTRIAL BASE COLLABORATIVE INFORMATION SHARING ENVIRONMENT (DCISE)

DoDD 5505.13e and DODI 5205.13 establish the Department of Defense (DoD) Cyber Crime Center (DC3) as the operational focal point for threat information sharing through the DoD-Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE) to protect unclassified DoD information residing on or transiting DIB unclassified networks.

DCISE and the Defense Industrial Base Network (DIBNet) portal are the entry points for both mandatory (Defense Federal Acquisition Regulations Supplement [DFARS]) and voluntary reporting under the DIB Cybersecurity (CS) Program. DCISE develops and shares actionable threat products, performs cyber analyses, diagnostics, and remediation consults for DIB Partners as directed by DoDI 5205.13. DCISE collaborates with other DC3 directorates to include the Cyber Forensics Laboratory (CFL), Operations Enablement Directorate/Analytic Group (OED/AG), Information Technology (XT), and the Vulnerability Disclosure Program (VDP) to provide strategic, operational, and tactical situational awareness to increase the DIB's ability to safeguard Controlled Unclassified Information (CUI) data on information systems. Through knowledge and situational awareness from DCISE products and services, DIB CS Program Partners benefit from a stronger security posture and are able to better protect their networks and information systems from Advanced Persistent Threats (APTs) and others seeking to steal DoD information and intellectual property.

DoD'S DIB CS PROGRAM

Malicious cyber actors work around the clock to exploit vulnerabilities on your network, compromise and steal data, and exfiltrate your organization's trade secrets and intellectual property. Cyber threats to DIB unclassified information networks represent an unacceptable risk of compromise of DoD information and pose an imminent threat to US national and economic security interests.

DoD's DIB CS Program is a unique public-private cybersecurity partnership and voluntary cyber threat information-sharing program. It was established by the DoD to enhance and supplement Partners' capabilities to safeguard DoD information that resides on or transits DIB unclassified networks or information systems. Through collaborative cyber threat information sharing and Cybersecurity as a Service (CSaaS) capabilities, enrollment in the Program can improve DIB network defenses, reduce damage to critical programs, and increases cyber situational awareness, improving the cybersecurity posture of the DIB to protect the US Government (USG) critical technologies and supply chains.

The DIB CS Program

- Offers actionable Indicators of Compromise (IOCs), mitigation, and remediation strategies.
- Increases USG and industry understanding of cyber threats.
- Enables Partners to better protect Covered Defense Information (CDI).
- Protects confidentiality of Partners and shared information through anonymization.

Value of Participation

- Collaborative partnership between 1,200+ Defense Contractors and USG agencies.
- A 24/7 support hotline that directly connects you with a DCISE analyst, ensuring round-the-clock assistance whenever you need it.
- Access to a no-cost malware analysis portal, allowing Partners the ability to safely and securely submit malware, network traffic, and volatile data to DC3's CFL for examination. Submitters have the option of requesting an examination by CFL's subject matter experts or receiving an Automated Malware Response (AMR) within minutes. Access to IOCs and threat products created from DIB reporting, and multiple USG data streams.
- Engagement opportunities amongst USG and DIB, from the C-suite to analyst level.

Joining the DIB CS Program

To be eligible to participate in the DIB CS Program, DoD contractors must do the following:

- Execute the standardized Framework Agreement with the DoD CIO Program Management Office (PMO).
- Handle DoD CUI in support of a DoD contract.
- Have, or acquire, DoD-approved medium assurance certificates to enable encrypted unclassified information sharing.

Learn more about the DIB CS Program: https://dibnet.dod.mil

Learn more about DFARS 252.204-7012:
https://www.acq.osd.mil/asda/dpc/index.html

Report mandatory cyber incidents to DCISE via the DIBNet portal:
https://dibnet.dod.mil/dibnet/portal/

Learn more about the DoD-Approved Medium Assurance Certificate:
https://public.cyber.mil/eca/

DCISE RECOMMENDED TOP 5 CYBERSECURITY PRACTICES

1-FILTER EMAIL

2-SCAN ATTACHMENTS AND DOWNLOADS

3-PATCH AND UPDATE SOFTWARE

4-USE MULTI-FACTOR AUTHENTICATION

5-RESTRICT ADMINISTRATIVE PRIVILEGES

DC3 DIB COLLABORATION

DFARS Mandatory Reporting

DoD contractors are required to report cyber incidents under DFARS. DFARS clause 252.204-7012, Safeguarding CDI and Cyber Incident Reporting, defines adequate security, controlled technical information, cyber incidents, technical information, and reporting requirements. Any contractor safeguarding DoD unclassified controlled technical information must be familiar with the requirements of DFARS 252.204-7012 and where to access additional information.

Mandatory incident reporting under DFARS 252.204-7012 is required by most DoD contracts and in subcontracts that involve CDI and/or operationally critical support programs involving CDI. Contractors must report the discovery of cyber incidents that affect CDI information systems, or the CDI information residing therein, to https://dibnet.dod.mil within 72 hours. Affected system images, packet capture, and other data relevant to the reported cyber incident must be preserved for 90 days to allow time for DoD to request the data to conduct a damage assessment or decline interest.

DCISE Notification Requirements

DC3 is designated by DFARS 252-204-7012 as the DoD focal point for receiving initial DIB cyber incident reports. Procedures, Guidance, and Information (PGI) 204.73 requires DC3 to provide a copy of the Mandatory Incident Report (MIR) to contracting officer(s) for potentially impacted contracts identified in the report. DC3 is also required to notify various USG stakeholders dependent on circumstances. DCISE provides email notification of mandatory reporting to the DoD Damage Assessment Management Office (DAMO), DIB CS PMO, DC3 Director, and the Joint Acquisition Protection and Exploitation Cell (JAPEC). Copies of MIRs are available within two hours of receipt for USG consumption on DCISE's SIPR Intelshare page at https:// intelshare.intelink.sgov.gov/sites/dodcc/dcise/default.aspx.

Attributional/proprietary information may only be released to entities with missions affected by such information; entities involved in the diagnosis, detection, or mitigation of cyber incidents; USG entities that conduct counterintelligence or law enforcement investigations; and for national security purposes.

What is DCISE's Role in Mandatory Incident Reporting?

DCISE receives and processes MIRs from DIB companies. DCISE analysts routinely perform the following tasks:

- Conduct outreach with submitting companies to obtain relevant information regarding the reported incident.
- Assist the submitting company with any malware submissions.
- Assist in coordinating media submission requirements when DoD elects to conduct a damage assessment.
- Coordinate and deconflict with other DoD and USG entities, such as law enforcement or counterintelligence, that may already be investigating the incident. This helps ensure DIB companies are not burdened by multiple USG entities asking for similar information.

I Submitted a Mandatory Incident Report, What Should I Expect Next?

In most instances, a DCISE analyst will reach out within three business days of submitting the report. The purpose of the contact is to gather incident details, IOCs, malware samples, and to understand the potential impact to DoD data. Depending on the scope and severity of the incident, the DoD DAMO may elect to conduct a damage assessment. If so, the DoD Contracting Officer or Officers responsible for the affected contract will provide an official letter requesting copies of the affected CDI and/or forensic images of media related to the incident reported in the Incident Collection Format (ICF).

What Does DCISE Do With the Information Provided?

The incident details provided to DCISE by a DIB company in the ICF are used to support the cybersecurity posture of the DIB. DCISE does this by generating threat intelligence products that are shared with Partners of the DIB CS Program. The threat intelligence products are non-attributable, which means the identity of the submitting company is never revealed. The threat intelligence products range from incident-level analyses to strategic-level reports on which technologies are being targeted by state-sponsored cyber actors. The information a DIB company provides can also assist in sanctions or arrests of cyber-criminals and adversarial nations. The MIR ICF is also shared with other USG agencies.

Common Misunderstandings About Mandatory Incident Reporting

Media and Malware Submissions

While it is important to work with law enforcement agencies—such as the Federal Bureau of Investigation—on cyber-related crimes, providing forensic images and third-party forensic reports to a Department of Justice entity does not fulfill the DFARS requirement to the DoD.

Ways to Report: The preferred method to report cyber incidents is to acquire a DoD-approved medium assurance certificate, which enables the timely and protected transfer of incident details to DCISE.

Other ways to report cyber incidents include:

- **One-time Token:** Partners must contact the DCISE inbox and our analysts will provide a one-time link from DIBNet so that they may report.
- **DoD SAFE:** Partners will contact DCISE to receive a DoD Safe password that will expire after 72 hours. The Partner will complete the necessary documents, and our analysts will report on the Partner's behalf in DIBNet.

Third-Party Forensic Reports

DCISE will request Partners to submit third-party forensic reports as they become available. In the event of an incident where a DIB company engages a third-party forensic firm for investigation, DCISE will ask for a copy of the report for further analysis and collaboration.

PROGRAM POLICY–RELATED RESOURCES

Please visit dc3.mil for links to the following:

- 32 Code of Federal Regulations Part 236, DoD's DIB Cybersecurity Activities
- DFARS 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting"
- DFARS 252.239-7010 "Cloud Computing Services"
- Federal Acquisition Regulation (FAR) 52.204-23 "Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities"
- FAR 52.204-25 "Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

DCISE'S TOP 5 MITIGATION TIPS BASED ON PERFORMING OUR ADVERSARY EMULATION TESTS (AET)

1. **Patching:** Conduct routine scanning and ensure all software and services are up-to-date.
2. **Insecure Default Configurations:** Ensure that all default configurations are promptly changed and secured.
3. **Spearphishing Weakness:** Deploy email filtering and/or scanning.
4. **Spearphishing Susceptibility:** Conduct user training.
5. **Unnecessary Network Solutions:** Disable any network solution that is not being utilized to make the attack vector smaller.

DCISE THREAT PRODUCTS

DCISE produces products ranging from indicator based to strategic cyber threat analyses.

Voluntary DIB Partner and mandated DFARS reporting are used to create threat products providing situational awareness and context of cyber activity. Products include the following:

- **Threat Activity Reports (TARs)** focus on specific APT sets, campaigns, or malware.
- **Cyber Targeting Analysis Reports (CTARs)** focus on specific technology targeted by APT sets, campaigns, or malware.
- The **Customer Response Form (CRF) Rollup** and **CRF Supplement** enrich DIB mandatory and voluntary reporting to DCISE by providing actionable indicators and relevant context regarding cyber threat actor tactics, techniques, and procedures (TTPs) and targeting.
- **Alerts/Warnings/Advisories** provide the DIB with timely information regarding zero-day and other actively exploited vulnerabilities, critical vulnerabilities, APT activity, and adversarial tactics, techniques, and procedures.
- The **TIPPER** alerts Partners via email about imminent or recent suspicious cyber activities and vulnerabilities specific to the DIB Partner.
- The **Threat Information Product (TIP)** contains CUI or Unclassified indicators from multiple sources.
- The **Weekly Indicator Roundup (WIR)** provides Partners with a regular gathering of indicators, eliminating the need to compile indicators from separate sources. This enables Partners to automatically ingest indicators into their security appliance.

Reports are available to DIB Partners via DIBNet and to USG via NIPR (https://intelshare.intelink.gov/sites/dodcc/dcise/default.aspx) and SIPR Intelshare (https://intelshare.intelink.sgov.gov/sites/dodcc/dcise/default.aspx).

DIBNet PORTAL https://dibnet.dod.mil/

The DIBNet Portal is DoD's gateway for Defense Contractor cyber incident reporting and participation in the DIB CS Program. The splash page and portal serve as the central hub for a variety of DCISE offerings:

- Real-time Alerts & Warning
- Threat Products
- Open-source Articles of Interest for the DIB
- Information on Upcoming Events
- Working Group Meeting Minutes
- The Latest Program Announcements
- Forums on Trending Topics
- DIB-Reported Cyber Threats
- Frequently Asked Questions Related to the DIB CS Program

DCISE EVENTS

- **Partner Familiarization Event (PFE):** Introductory meeting between DCISE and newly onboarded DIB CS Program Partners. Discussions include DCISE and Partner Points of Contact (POCs) as well as a high-level overview of offerings, use of DIBNet, and submission incident reports.

- **Analyst-to-Analyst (A2A) Exchanges:** DIB Partner-driven and may address APT TTPs, technology targeting, and current threat reporting. Opportunity for one-on-one diagnostics and remediation with DCISE analysts.

- **Business-to-Business (B2B) Exchanges:** Introduction to DCISE products and services to DIB POCs and their corporate leadership in addition to highlighting the positive business impact of network security and participation in the DIB CS Program.

- **DC3 Technical Exchange (TechEx):** Bi-annual meetings between DIB Partners and USG stakeholders to share best practices, threat briefs, lessons learned, tools, and other industry insights at classified and unclassified levels.

- **Regional Partner Exchange (RPEX):** Provides an opportunity for local DIB Partners within the same geographic region to have a TechEx experience on a smaller scale. DCISE leadership and analysts provide a tailored threat brief covering the current threat landscape, specific APT trends, and threat actor TTPs. Partners have the opportunity to network, discuss topics of concern, present briefs, chair panels, and collaborate.

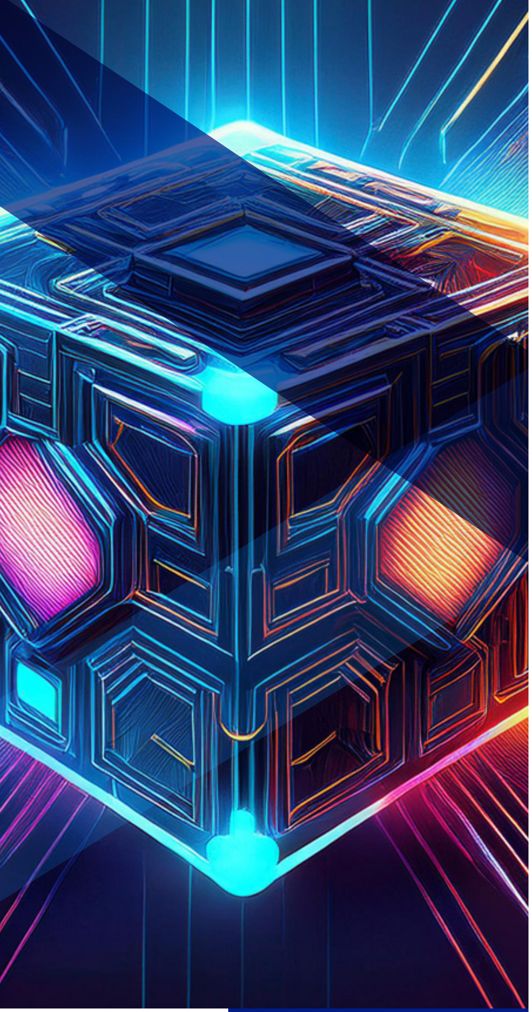
- **DCISE F.I.R.E.:** One-day, technology-supported table top exercise event led by DCISE (in-person or remote) for DIB CS Program participants to test their skills in a variety of topics (e.g., incident response, intrusion detection) while earning Continuing Professional Education credits.

- **DIB Webinar:** DCISE provides a platform for DIB Partners and DCISE analysts to engage in classified, detailed discussions on adversary techniques and trends. These sessions aren't limited to just technical topics; they also cover a broad spectrum of issues relevant to the DIB, led by various experts from DCISE. In addition, DCISE runs a recurring series of introductory web conferences called "Partner Essentials" to help partners stay informed and prepared.

DCISE SERVICE OFFERINGS OVERVIEW

DCISE offers many CSaaS products at no cost to DIB CS Partners:

- **DCISE^3:** automated threat detection, scoring, and blocking solution with integration of DCISE threat intelligence.
- **Cyber Resilience Analysis (CRA):** evaluates processes and practices across 10 security domains and provides insight into an organization's operational resilience and ability to manage cyber risks.
- **Adversary Emulation (AE):** Simulates real-world attacker techniques to assess the resilience of your defenses. This includes network mapping, vulnerability assessments, phishing simulations, and web application testing, providing a focused and actionable roadmap for improving security posture.
- **DIB-Vulnerability Disclosure Program (DIB-VDP):** utilizes independent white hat researchers to help you discover vulnerabilities on your publicly facing infrastructure.



DCISE^3 AT A GLANCE

DCISE recognizes the unique challenges faced by the small and medium businesses within the collective DIB and has partnered with Celerium to provide an automated cyber threat detection, scoring, and blocking solution to our DIB CS Program participants at no cost.

How Does It Work?

DCISE^3 integrates with a company's existing firewall and captures a real-time stream of metadata associated with network traffic that contains the IP address and domains with which communications are occurring.

DCISE^3 automatically aggregates this metadata and provides fully automated risk-scoring capabilities for every network connection without requiring any human interaction. Risk scoring takes into account over 60 sources of threat intelligence (including DCISE indicators), years of historical data, and predictive algorithms to detect and automatically block emerging and pre-existing threats.

This offering has been upgraded to DCISE^3 v2 as of August 2024 and now offers enhanced network reporting, an updated user interface, and expands the network defense orientation of v1 to data breach defense and other additional features. The upgraded solution was tested with DIB CS members that found the new version to be easier to use and provide additional value.

Network Defense Functions

- Port threat activity reports
- Network threat activity reports
- 24-hour network threat reports
- Live network threat data reports
- Optional automated blocking of malicious network traffic
- Re-optimization of network blocklist every 15 minutes per firewall
- Blocking activity–receive notification anytime an IP address is blocked

Data Breach Defense Functions

- Track potential data breach activity
- Enable manual activation of containment via blocking

Malware Defense Functions

- Detect and optionally block selected malware activity (Volt Typhoon, MOVEit, TrueBot, and others)

Implementation

DCISE^{3}v2 is engineered to support companies with overloaded and overwhelmed IT organizations and can be implemented without needing installation of any hardware or software. The implementation is based on configuring public-facing firewalls in 30 minutes or less. The solution is minimally intrusive, meaning it does not access any customer data or packets since it focuses on Layer 3 syslog meta data.

ALL-TIME PROGRAM METRICS

2.92M
Threats Detected

1.23M
Threats Blocked

WE PROVIDE

Federal Compliance

Real-time Visibility

Traffic Analysis

Auto Blocking

WHAT IS A CYBER RESILIENCE ANALYSIS (CRA)?

The CRA is a DC3-facilitated survey that may be conducted during a one-day, in-person session, a two-day virtual session, or it may be downloaded from DIBNet and performed as a self-assessment.

Security domains and organizational practices are mapped to the National Institute of Standards and Technology (NIST) Special Publication 800-171 requirements to protect CUI and the NIST Cybersecurity Framework (CF).

The CRA provides a review of the overall health of an organization's cybersecurity program as it relates to a specific critical service which helps to do the following:

- Develop an understanding of existing process-based cybersecurity capabilities.
- Develop meaningful indicators of operational resilience.
- Improve organizational ability to manage cyber risk to its critical services and related assets.

How Would the CRA Benefit My Organization?

- Provides an understanding of which cybersecurity practices inform specific NIST and CMMC requirements.
- Provides an easy to understand, comprehensive final report indicating the relative maturity of organizational resilience and cybersecurity capabilities that includes the following:
    - A baseline that aids in improvement efforts.
    - Visual scoring depictions for performance across the various security domains.
    - Options for consideration for organizational process improvement.

Cyber Hygiene—A Baseline Set of Practices

The CRA includes cyber hygiene insights that are paramount to organizational success.

These key practices include the following:

- Identify and prioritize key organizational services, products, and their supporting assets.
- Identify, prioritize, and respond to risks to the organization's key services and products.
- Establish an incident response plan.
- Conduct cybersecurity education and awareness activities.
- Establish network security and monitoring.
- Control access based on least privilege and maintain the user access accounts.
- Manage technology changes and use standardized secure configurations.
- Implement controls to protect and recover data.
- Prevent and monitor malware exposures.
- Manage cyber risks associated with suppliers and external dependencies.
- Perform cyber threat and vulnerability monitoring and remediation.

The CRA now includes mappings to the NIST CSF Ransomware Profile. Based on how an organization answers the CRA questions, depictions are created that show how an organization is performing practices that relate to ransomware protections.

Ten Domains of Capability in CRA

AM–Asset Management

CM–Controls Management

CCM–Configuration & Change Management

VM–Vulnerability Management

IM–Incident Management

SCM–Service Continuity Management

RM–Risk Management

EDM–Asset Management

TA–Training & Awareness

SA–Situational Awareness

DISCOVER DCISE ADVERSARY EMULATION (AE) SERVICE

DCISE's AE service offers threat-informed network penetration tests, known as an Adversary Emulation Test (AET), which leverages USG and industry reporting on adversarial TTPs.

An AET provides your organization critical insights into the efficacy of your cyber defenses and technical controls by identifying risks and vulnerabilities outside and inside your network. The AE team utilizes the same tools and methodologies used by today's cyber threat actors to discover these vulnerabilities to enable your organization to better understand and manage the corresponding risks.

How It Works

An AET is a two-week assessment that may include penetration testing, network mapping, vulnerability scanning, phishing assessments, and web application testing. This assessment is preceded by a CRA, if one has not been conducted within the past year, which is an analysis of your organization's processes, documentation, and operational resiliency with regard to sustaining operations and managing cyber risks during times of stress.

The Key Benefits

The AET, coupled with the CRA, will provide your organization with a comprehensive picture of your cyber defense posture. The AE service will provide an in-depth report containing helpful insights and strategies to assist the prioritization of improvement and resourcing efforts as you continue to evolve your defenses.

"The testing allowed cybersecurity and IT personnel to identify anomalous behavior through log/event monitoring and alerts generated by security solutions. Training to detect and identify potential incidents quickly through event correlation as well as automated tools, and confirm a true-positive, is extremely valuable for cyber defense and incident response. These scenarios will be used for tabletop incident response exercises in the near future."

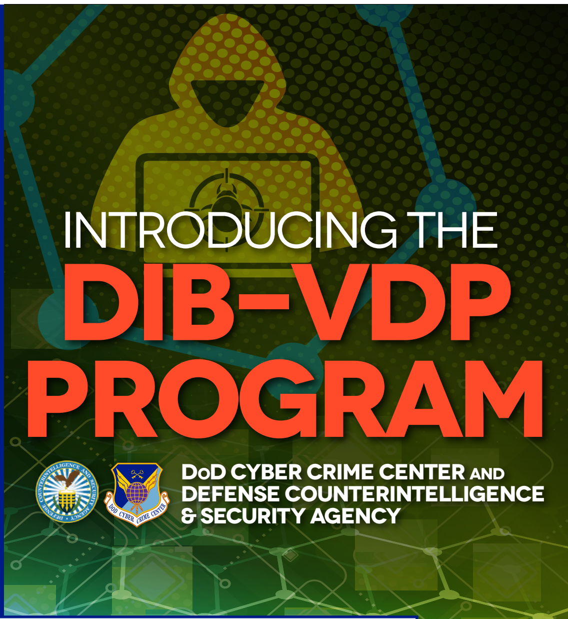
–AET Participant 1

"From an overall perspective, we are pleased that the critical findings are able to be remediated through patch management. There were a few surprises that we would not have known without going through the testing and so we are very thankful to have this information in order to lock those down."

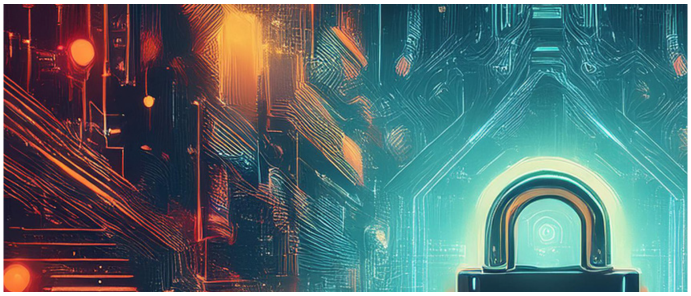
–AET Participant 2

A LOOK INSIDE THE DIB-VDP SERVICE

DC3 and Defense Counterintelligence and Security Agency have established a fully operational vulnerability disclosure program supporting the DIB. DC3's DIB-VDP performs a coordinated vulnerability disclosure process of ingesting information from designated vulnerability researchers. The information is then shared with relevant stakeholders to ensure timely remediation. Once vulnerabilities are validated, DC3 uses non-attributed disclosures to communicate both the vulnerabilities and their mitigations. Leveraging this proven model is the most effective way to encourage vulnerability discovery within DIB companies' publicly accessible information systems.



> *Each mitigated vulnerability saves the affected company an average of $4.3m in response and recovery costs.*
>
> Source: https://www.ibm.com/reports/data-breach

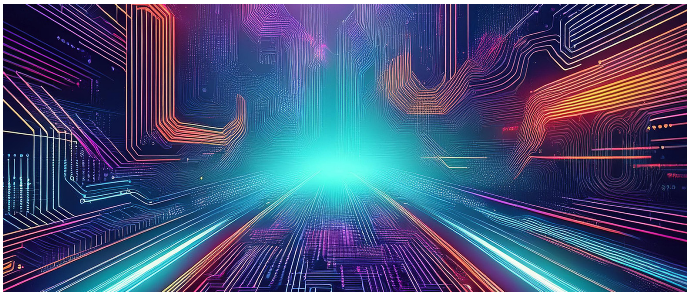


MALWARE AND FORENSIC ANALYSIS

DCISE is your point of contact for submitting malware and/or other relevant files to the DC3 CFL for a quick triage or an in-depth examination, for free, and can be submitted as part of a Voluntary or Mandatory ICF submission.

Ways to Submit Malware to DC3 CFL:

- Traditional mail
- DC3 Electronic Malware Submission (EMS) Portal (https://ems.dc3on.gov/)
  - Can also be accessed directly through DIBNet
  - Application Programming Interface (API) available to upload malware and retrieve analysis results
  - Email service account available for fast upload of suspicious emails
- **DO NOT email malware to anyone at DCISE**



AUTOMATED MALWARE RESPONSE (AMR)

The DC3 EMS portal provides an option for AMR. This capability provides the following:

- A quick, automated analysis of your submitted malware, phishing emails, email attachments, or other suspicious files
- Results ready in less than 15 minutes
- Results that include antivirus engine checks, file attributes, notable strings, YARA signature matches, and more

HOW TO LEARN MORE OR REGISTER FOR THE DIB CS PROGRAM?

The DIB CS program is built upon a strong trusting relationship between DoD and industry Partners. DoD preserves the integrity of the program by protecting sensitive non-public information from unauthorized use and disclosure.

Visit https://dibnet.dod.mil to learn more about or apply to join the DIB CS Program.

"The challenges we face in cyberspace are so complex that no individual or organization has all the answers. Trusted, secure, focused collaboration generates insights which can strengthen the defense of the DoD, our DIB Partners, and the nation."

Mr. Terry Kalka,
DCISE Director

DC3.DCISE@us.af.mil
877.838.2174 | 410.981.0104

DoD CYBER CRIME CENTER
410.981.6610 | www.dc3.mil | DC3.Information@us.af.mil

𝕏 @DC3Forensics • @DC3DCISE
in DC3 Cyber Crime Center