For the last several decades, cybersecurity implementation has been driven by compliance standards. But the nature of cyber threats has changed dramatically and compliance with traditional cybersecurity controls is no longer sufficient to ensure a resilient enterprise.

So when “compliance” is not the goal, how much cybersecurity is enough? **The answer demands a risk management approach.**
Dynetics has a comprehensive portfolio of solutions enabling **risk-based decisions** by providing critical insights into **costly and potentially catastrophic** cyber risks.

We support all phases of cyber risk management including **strategic planning**, **assessment**, **implementation**, **monitoring**, and **test**.

**01. Strategize** to prioritize risks and maximize your ROI.
**02. Assess** to enhance your approach.
**03. Implement** tailored solutions to meet your needs.
**04. Monitor** to detect and respond to malicious activity.
**05. Test** to ensure resilience.

We offer these Cyber Risk Management Solutions:

**Cooperative Assessments**.................6
- Business Impact Assessment (BIA)
- Controls Self-Assessment (SelfAssure)
- Controls Assessment
- Credentialed Vulnerability Assessment
- Architecture Assessment
- Compliance Assessment
- Source Code Assessment
- Wireless Network Assessment
- Web Application Assessments

**Adversarial Assessments**...............10
- Phishing Assessment
- Uncredentialed Vulnerability Assessment
- Social Engineering Test
- Penetration Test
- Physical Information Security Test
- Adversarial Simulation
- Internal Adversarial Simulation

**Operational Solutions**...............14
- Real-time Threat Monitoring (NetAlert)
- Cyber Incident Response
- Cyber Risk Awareness Training
- Controls Implementation
Over 40 years of responsive, cost-effective solutions

Dynetics was founded in 1974 in Huntsville, Alabama to provide engineering expertise to national security missions. For over 40 years, Dynetics has supported high-value, high-risk programs within the Department of Defense and NASA while also providing similar expertise to large commercial businesses such as Ford and Chrysler.

Since 2000, Dynetics has provided expertise in information security for commercial and government clients ranging in size from small local businesses with a handful of employees to large agencies and multi-national corporations with thousands of employees.

Dynetics has the experience to help you understand cyber risks, optimize current investments, and plan future investments.

Let us help you protect what matters.
Dynetics has conducted over 1,000 cybersecurity assessments using numerous compliance standards for public and private organizations.

We have supported one of only 6 “Red Teams” approved by the NSA to conduct Adversarial Simulations against DoD weapon systems.

We have years of experience conducting “threat-faithful,” simulated cyber attacks (Adversarial Simulations), providing us with unique insight into cybercriminals’ motivations, tactics and techniques, and ability to avoid traditional controls.

Tailorable to meet your priorities—and fit your budget

When it comes to cyber risk priorities and budgets, every company is unique. Therefore, to ensure we address your needs and maximize your return on investment, Dynetics solicits your inputs and tailors our recommendations when presenting options.

For more information on tailoring solutions and pricing, contact Dynetics at

800-922-9261 ext. 5020
Know your risk to build a resilient enterprise

Controls Self-Assessment (SelfAssure)

Deliverable(s): 1-year license to the SelfAssure cloud-based portal.

While a comprehensive Controls Assessment (page 7) is essential to assuring an effective cyber risk management program, Dynetics recognizes that, for some clients, the associated costs can be beyond current budgets. Therefore, Dynetics developed SelfAssure to fit smaller budgets while still providing the foundation for increasing assurance levels over time. SelfAssure is a low-cost, online, cyber risk management tool that assesses the effectiveness of implemented cybersecurity controls and provides specific recommendations for mitigating identified weaknesses. Each recommendation is accompanied by five decisions aids to help clients build a prioritized action plan. In addition, assessed strengths and weakness are mapped to the NIST Cybersecurity Framework so clients can demonstrate use of this widely accepted framework that has been referenced by regulatory agencies as a “reasonable” approach to managing cyber risk.

SelfAssure is implemented as Software-as-a-Service so clients only need an internet connection to access and use; and, since cyber risk management is generally a shared responsibility, SelfAssure is designed for collaboration among an unlimited number of users, including 3rd-party vendors.

For an additional fee, Dynetics cybersecurity professionals will review SelfAssure results to validate the Cyber Risk Profile and discuss options for next steps.

Assess effectiveness of implemented cybersecurity controls, generate prioritized recommendations to mitigate weaknesses and begin use of the NIST Cybersecurity Framework.
Business Impact Assessment (BIA)

**Deliverable(s):** Report identifying essential functions, related KIAs, associated Business Impact Values, and underlying Digital Profile.

Traditional approaches to cybersecurity focus on perimeter defenses with little regard for the information assets and associated business value being protected. This approach tends to be financially inefficient as KIAs may be under-protected while less important assets are over-protected. A BIA clarifies primary business objectives, identifies essential business functions, and identifies the KIAs that must be protected to sustain business value and ensure resilience. This information is then used to calculate the financial and intangible Business Impact Values (BIVs) that could result from a cybersecurity incident. With the BIA results in hand, clients can prioritize cybersecurity investments to ensure resilience through appropriate protection of KIAs.

In addition to quantifying potential BIVs, a BIA identifies and documents the client’s Digital Profile, which is the data, systems, technologies, web presence, etc. that comprise the KIAs. A client’s Digital Profile provides insights into cyber criminal attack motivations and identifies the attack surfaces that can be exploited during an attack. This insight is necessary to ensure selected cybersecurity controls are sufficient to mitigate anticipated cyber threats.

Quantify the financial impacts that could result from the loss of confidentiality, integrity or availability of Key Information Assets (KIA).

Controls Assessment

**Deliverable(s):** Report with findings and prioritized recommendations. Optional Plan of Action and Milestones (POAM)

Traditional approaches to cybersecurity focus on perimeter defenses such as firewalls, anti-virus and encryption in an effort to prevent cyber criminals from breaching the network and compromising Key Information Assets (KIA). Unfortunately, today’s cyber criminals use social engineering techniques that bypass these traditional defenses leaving KIAs vulnerable to compromise. A comprehensive Controls Assessment based on Dynetics’ proven cybersecurity objectives not compliance, provides assurance that appropriate cybersecurity controls have been implemented to mitigate anticipated threats. At the completion of a Controls Assessment, Dynetics computes a client Cybersecurity Level (CsL) that can be compared to their Cyber Threat Level for a cyber risk determination and then tracked over time to measure progress. Dynetics also provides a validated list of findings with prioritized recommendations that serve as the basis for a Plan of Action and Milestones (POAM). In addition, Dynetics maps assessed strengths and weakness to the NIST Cybersecurity Framework so clients can demonstrate use of this widely accepted framework that has been recognized by regulatory agencies as a “reasonable” approach to managing cyber risk.

A Controls Assessment includes a 1-year “standard” license for SelfAssure (page 6) which is used to collect information on current cybersecurity controls. Clients may upgrade SelfAssure to an “advanced” license which allows unlimited re-assessments during the 1-year license period and tracks progress across multiple assessments. Renewals allows SelfAssure to track progress across multiple years.

Independently assess the effectiveness of implemented cybersecurity controls, generate prioritized recommendations to mitigate weaknesses and begin use of the NIST Cybersecurity Framework.
Cooperative Assessments

**Credentialed Vulnerability Assessment**

**Deliverable(s):** Report identifying vulnerabilities with prioritized recommendations.

New vulnerabilities are discovered and exploited on a daily basis. User error or failure to deploy the latest patches can compromise a previously secure enterprise. To compound the problems, cybercriminals have access to vast amounts of information about today’s technical vulnerabilities, using that information to test the vulnerability of target networks. We proactively identify technical vulnerabilities in your networks and produce a cybercriminal’s view using commercially available tools such as Nessus. Credentialed Vulnerability Assessments should be repeated on a regular basis (quarterly is recommended) to ensure new vulnerabilities are identified and mitigated.

*Note: Credentialed Vulnerability Assessments differ from Un-Credentialed Vulnerability Assessments (page 11) in that scans are not limited to publicly facing systems and findings are more reliable due to the having credentials necessary to access system configuration files.*

**Architecture Assessment**

**Deliverable(s):** Report identifying vulnerabilities with prioritized recommendations.

With an Architecture Assessment, Dynetics’ Elite Ethical Hackers work cooperatively with your network administrators to explore trust relationships within your enterprise and ensure controls are integrated effectively to create the “defense-in-depth” approach necessary to detect today’s cybercriminals. This strategic review allows you to view your IT enterprise and cybersecurity from an “adversarial mentality” and proactively uncover and mitigate weaknesses that may not be discovered during tactical assessments. At the completion of a Architecture Assessment, clients receive a report on identified vulnerabilities with prioritized recommendations for corrective actions.

The “adversarial mentality” during a Architecture Assessment is critical: most IT security professionals are defensive-minded and unfamiliar with the tactics and techniques used by today’s cybercriminals. Our experience in both systems administration and elite ethical hacking provides invaluable insights into vulnerabilities and the controls that make successful cyber attacks less likely. In addition, your network administrators get valuable training and become familiar with cyber attack techniques, enabling them to better protect your enterprise.

*Using an “adversarial mentality,” identify security weaknesses in the design and implementation of enterprise networks and validate effective implementation of cybersecurity controls.*

**Source Code Assessment**

**Deliverable(s):** Report on source code vulnerabilities with prioritized list of corrective actions.

Given the size and complexity of today’s applications, and given the emphasis on developing and delivering capability as soon as possible, source code errors that result in cybersecurity vulnerabilities are commonplace. Therefore, Source Code Assessment by a security professional is essential to identifying security vulnerabilities that are difficult to detect in operational environments.

Moreover, considering that the number of possible coding errors increases exponentially as the lines of code increases, analysts are limited in their ability to find the majority of errors. Consequently, Dynetics uses programming language-specific tools and expert analysis to identify source code errors that create cybersecurity vulnerabilities.

*Identify cybersecurity vulnerabilities in client-developed applications.*
**Compliance Assessment**

**Deliverable(s):** Report on areas of non-compliance with prioritized recommendations for achieving compliance.

For many clients, compliance with a governance standard is a requirement, and Dynetics has over 16 years’ experience with numerous compliance standards to include NIST 800-53, PCI, IRS Pub 1075, GLBA, SOX, HIPAA, DFARS and DIACAP. However, a Dynetics Compliance Assessment goes far beyond “checking the box” for compliance.

After conducting over 1,000 cybersecurity assessments, Dynetics has found that most compliance standards are somewhat ambiguous about “how” to satisfy requirements.

In fact, many “compliant” businesses make the headlines due to the lack of effective cybersecurity controls. This is the main reason for the new DOD Cybersecurity Maturity Model Certification (CMMC). Therefore, in addition to verifying that all requirements have been satisfied, Dynetics assesses the effectiveness of the selected cybersecurity controls, identifies weaknesses that could lead to a breach, and provides prioritized recommendations for ensuring effective security in addition to compliance. At the completion of a Compliance Assessment, Dynetics provides a report that identifies areas of non-compliance, identifies weak cybersecurity controls, and provides prioritized recommendations for addressing both non-compliance and weak cybersecurity.

**Wireless Network Assessment**

**Deliverable(s):** Report identifying vulnerabilities in the design and implementation along with a list of unauthorized devices connected to the wireless network.

Identify vulnerabilities in a wireless network.

Clients implement wireless networks for several reasons to include employee access to work systems, guest access to public internet, and customer/constituent access to services (e.g. student access to school services). Regardless of the requirement, a wireless network provides another entry point into the client’s corporate network, and therefore should be assessed for security. A Wireless Network Assessment determines the effectiveness of wireless security controls, ensures proper segmentation between corporate and non-corporate assets, and identifies unauthorized wireless devices that may have attached to the wireless network.

**Web Application Assessments**

**Deliverable(s):** Report on areas of non-compliance with prioritized recommendations for achieving compliance.

Web applications support the free exchange of information and are a necessary component of e-commerce. Therefore, they must be accessible to everyone, including cyber criminals. For this reason, web applications are consistently one of the most exploited attack surfaces in a client’s IT enterprise. A Web Application Assessment identifies known vulnerabilities and looks for exploitable logic flaws so clients can have confidence their web applications are not creating unnecessary risks for their enterprise.

Identify cybersecurity vulnerabilities in public-facing web applications.
Adversarial Assessments

Assess and validate cyber risk using threat-faithful tactics

Adversarial assessments are intended to assess and validate client cyber risk using “threat faithful” cyber criminal tactics and techniques. That means, for the most part, the client does not provide information or support, and the Adversarial Assessment team is left to discover information using the same resources available to cyber criminals. It also means that user trust will be exploited through deception techniques, just as a cybercriminal will use. This “adversarial mentality” ensures a “threat faithful” assessment that provides the most beneficial insights into how cybercriminals exploit vulnerabilities in client information system.

The adversarial assessments described in this section are divided into three categories:

1) **Assessment.** All data is gathered without breaching the client network.
2) **Test.** Client networks are breached and persistence may be established, but data discovery and removal is not attempted.
3) **Simulation.** Non-destructive, but “threat faithful” simulation of cybercriminal tactics and techniques to include data discovery, exploitation and removal.
Un-Credentialed Vulnerability Assessment

**Deliverable(s):** Report identifying vulnerabilities with prioritized recommendations.

Today’s cyber threat landscape is very dynamic with new vulnerabilities discovered and exploited on a daily basis. User error or failure to deploy the latest patches can compromise a previously secure enterprise. And to compound the problems, cyber criminals have access to vast amounts of information about technical vulnerabilities that can exist in today’s IT systems, and they use that information to test the vulnerability of target networks. To proactively identify technical vulnerabilities in client networks and produce a cyber criminal’s view of those networks, Dynetics conducts Un-Credentialed Vulnerability Assessments using commercially available tools such as Nessus.

*Identify technical vulnerabilities that could be exploited by cybercriminals.*

Un-Credentialed Vulnerability Assessments should be repeated on a regular basis (quarterly is recommended) to ensure new vulnerabilities are identified and mitigated.

**Note:** Un-Credentialed Vulnerability Assessments differ from Credentialed Vulnerability Assessments (see 4.3) in that only publicly facing systems can be scanned and the reliability of findings is lower due to not having authorization to access to system configuration files.

---

Phishing Assessment

**Deliverable(s):** Report describing the phishing email used, the number of employees responding to phishing email, and the extent of cooperation provided by employees.

*Test employee ability to recognize and avoid being victimized by phishing email attacks.*

Over 90% of successful cyber attacks use social engineering techniques to bypass perimeter defenses; and phishing emails are the most common social engineering technique. Therefore, it is imperative that employees be trained to recognize phishing emails and avoid being victimized. With a Phishing Assessment, Dynetics creates phishing emails that are designed to engage employees, exploit their trust and entice them to take actions that will compromise their systems. Since the goal of a Phishing Assessment is training and not network penetration, no malicious actions are taken in response to employee action. However, Dynetics does collect statistics and information on employee responses to provide in a summary report.

**Social Engineering Test**

**Deliverable(s):** Report describing social engineering techniques used, the number of employees compromised, and the extent of cooperation provided by employees.

Over 90% of successful cyber attacks use social engineering techniques to bypass information systems perimeter defenses. Therefore, it is important to educate employees on techniques used by cyber criminals and periodically assess the effectiveness of employee training.

*Determine client’s susceptibility to social engineering attacks including phishing emails, unsecured media and phone calls.*

A Social Engineering Test evaluates employee susceptibility to phishing emails, unsecured media devices (thumb drives, CDs, etc) and phone solicitations, all of which attempt to acquire user credentials or place malware into the client’s network. Clients can then measure the effectiveness of employee cybersecurity awareness training and identify requirements for additional training.
Penetration Test

**Deliverable(s):** Report identifying vulnerabilities with prioritized recommendations

Today’s business models demand internet connectivity for communications, operations and e-commerce using information systems such as web servers, web applications, email systems and wireless networks. Unfortunately, these publicly facing systems also create attack surfaces that can be exploited by cyber criminals. Using cyber criminal techniques, a Penetration Test identifies technology vulnerabilities that can be exploited by cyber criminals and provides recommendations for mitigating those vulnerabilities.

*Identify technical vulnerabilities (no social engineering) that can be exploited to access to client’s network.*

**NOTE:** The term “penetration test” is used frequently in the cybersecurity industry to refer to anything from an automated scan with canned reports to a simulated attack and attempt to remove data. Associated costs vary greatly. Dynetics offers services to address this full spectrum and uses the services catalog to delineate the benefits of each. When comparing costs for competitive service offerings, clients are encouraged to ask for details to ensure pricing is for comparable scope, analysis and expertise.

Physical Information Security Test

**Deliverable(s):** Report describing techniques used to breach physical access controls, facilities/areas compromised, and the extent of cooperation provided by employees.

*Test physical security controls that protect access to information systems.*

The vast majority of cyber attacks are executed remotely. However, highly motivated cyber attacks may include attempts to breach physical security controls in order to access proprietary or sensitive information and are most likely facilitated by an employee. A Physical Information Security Assessment evaluates a client’s ability to control access to facilities, secure areas within a facility, and employee workstations. Physical access controls are tested through direct social engagements such as deceptive justification for needing facility access, following employees into secured areas, or checking for unsecured areas.

Internal Adversarial Simulation

**Deliverable(s):** Report on weaknesses exploited and recommendations for mitigation

An Internal Adversarial Simulation is executed the same as a complete Adversarial Simulation except that the initial breach is “assumed” and the simulation begins after a Dynetics is provided a “normal” user account on a single workstation. By assuming a breach, any cost associated with penetrating the network is avoided. The avoided costs could include open source intelligence gathering, development and execution of a social engineering campaign or exploitation of a known technical vulnerability. An Internal Adversarial Simulation is a cost-effective means to proactively identify cybersecurity weaknesses inside the client network or to periodically re-test the effectiveness of existing cybersecurity controls.

*Use a threat-faithful, simulated cyber attack to test client’s ability to protect network assets, detect intrusions and respond before significant damage occurs.*
Adversarial Simulation

Deliverable(s): Report on weaknesses exploited and recommendations for mitigation

Today’s cyber criminals are resourceful, persistent and patient when motivated to break into a network. In addition, cyber criminal techniques often bypass traditional cybersecurity controls such as firewalls, anti-virus and encryption. Consequently, 100% effective cybersecurity is not achievable and clients must assume that at some point their network perimeter defenses will be breached. To ensure a client’s cybersecurity is preventing as many breaches as possible AND is also detecting inevitable breaches as soon as possible, Dynetics conducts Adversarial Simulations.

An Adversarial Simulation is a “threat faithful” simulated cyber attack that aggressively tests the effectiveness of cybersecurity controls, identifies Key Information Assets that could be compromised in a real cyber-attack, and reveals realistic business impacts that could result from the loss of confidentiality, integrity or availability of those Key Information Assets. Adversarial Simulations allow clients to accurately assess business risks and maximize return on future investments.

To remain “threat faithful,” Dynetics independently collects open-source intelligence on the client’s employees, internet presence and operations (just as a cyber criminal would do) and uses that intelligence to launch a series of technical and/or social engineering cyber attacks. After successfully gaining access to the client’s IT enterprise, Dynetics attempts to traverse the network in order to discover, compromise and remove Key Information Assets as permitted by the pre-negotiated rules of engagement.

Use a threat-faithful, simulated cyber attack to test client’s ability to protect network assets, detect intrusions and respond before significant damage occurs.

Cyber criminals take their time investigating a potential victim, move slowly during an attack to remain undetected and wait patiently for privileged users to return from vacations or to take non-routine actions that disclose important operational procedures or credentials. To be realistic, Dynetics also moves slowly and alternates between periods of activity and inactivity. Therefore, the elapsed time to complete an Adversarial Simulation must be negotiated and depends on the desired level of “threat faithfulness.”
Real-Time Threat Monitoring (NetAlert)

Deliverable(s): Validated alerts with monthly summary reports

The nature of cyber attacks has changed and traditional cybersecurity controls such as firewalls, anti-virus and encryption are no longer sufficient. Well-crafted and targeted social engineering attacks quickly bypass traditional cybersecurity controls and allow cyber criminals to establish a presence inside clients’ networks. Consequently, at some point, all businesses will experience a breach. Unfortunately, most businesses have invested in perimeter defense to the exclusion of host, endpoint and network monitoring necessary to detect and respond to this type of intrusion. Therefore, to help clients detect malicious activity in their networks before significant compromise of Key Information Assets, Dynetics offers NetAlert as a managed cybersecurity monitoring service that includes endpoint detection and response (EDR), full packet capture and analysis, system log analysis and “honeypot” monitoring.

After years of conducting Adversarial Simulations, Dynetics realized that most small to mid-size businesses (SMBs) did not have visibility into their network activity, were unfamiliar with cyber criminal techniques, and were unable to detect intruders (real or simulated). Therefore, NetAlert was designed to offer the benefits of a high-end Security Information & Event Management (SIEM) system, but at a fraction of the cost. And because most SMBs either do not have in-house cyber threat expertise or don’t have enough personnel to effectively monitor for malicious activity, NetAlert is offered as a service that uses Dynetics cyber threat specialists to analyze alerts and notify clients only after an alert has been validated. This approach allows clients to focus on business priorities while accessing Dynetics’ cyber threat specialists at about 25% of the cost of hiring in-house expertise.

Detect malicious activity within a network before significant damage occurs.
Cyber Risk Awareness Training

**Deliverable(s):** 2-Hour, interactive training session

Most users have a limited understanding of the techniques cyber criminals use to gain access to a network. For over 90% of those attacks, the user’s trust is exploited through some type of social engineering attack such as a phishing email, malicious website, or phone call. In other cases, unprotected workstations or passwords may facilitate an attack. To help users recognize cyber attacks and understand how their actions could contribute to an attack, Dynetics offers Cyber Risk Awareness Training led by our Elite Ethical Hackers.

*Train users (employees, customers, community) on the importance of cyber risk management and how to avoid being victimized by cyber criminals.*

Cyber Incident Response

**Deliverable(s):** Incident report

When a cyber incident occurs, quickly and accurately assessing the situation is critical to minimizing financial impacts and returning to normal operations. From a technical perspective, four questions must be answered as soon as possible while maintaining the integrity of potential forensic evidence:

1. Does the intruder still have a presence in our network?
2. How did the intruder get into our network?
3. What information assets were compromised?
4. What actions are required to prevent re-occurrence?

Our forensics examiners have over 20 years’ collective experience examining workstations, servers, portable devices, and networks to obtain forensically sound data that can help with investigations into:

- Cybercrime
- Employee Computer/Network Abuse
- Malicious Insider Activity/ Hacking
- Data Breach and Exfiltration
- Employee Termination for Cause
- Data Recovery

**Collect evidence to support discovery, assessment, remediation and prosecution of a cyber incident.**

**NOTE:** Client should ensure they have a comprehensive cyber incident response plan that encompasses other, non-technical actions not addressed by Dynetics such as individual privacy notifications, legal/regulatory notifications, public relations communications, insurance notifications, etc.

Controls Implementation

**Deliverable(s):** Consulting services

Your IT professionals are busy: ensuring your IT enterprise is operating efficiently, meeting user demands, and staying abreast of the latest cyber threats. Sometimes they need help from outside experts.

Dynetics cybersecurity professionals have hands-on experience implementing cybersecurity controls proven to be effective preventing and detecting cyber intrusions. Many of the necessary controls are available in products you already own or in free, open source tools. We can help your IT staff select, install, and properly configure tools to defend against attacks. Dynetics has standard configuration kits that allow us to complete setup more efficiently while taking into consideration results from your cyber risk assessments.

In addition, we can help you decide how best to manage exceptions that exists in every environment so your business operations remain effective and efficient.

Support for Controls Implementation can be purchased on an “as needed” basis to support your needs and objectives. Dynetics cybersecurity professionals may advise your IT staff, assist with unfamiliar controls, or be tasked to fully implement some or all cybersecurity controls.

*Provide insight, expertise and tools that support the implementation of cyber risk management best practices.*
At Dynetics, a wholly owned subsidiary of Leidos, we help customers accomplish complex, high-value missions. By combining the capabilities of a large business with the responsiveness of a small business, Dynetics put in place extensive R&D capabilities and deep technical expertise in systems engineering, systems analysis, modeling and simulation, cyber, software development, rapid prototyping, test and evaluation, manufacturing, integration, and operations. Using our considerable engineering, scientific, and other technical resources, we help customers identify, analyze, and respond to complex threats to their missions.