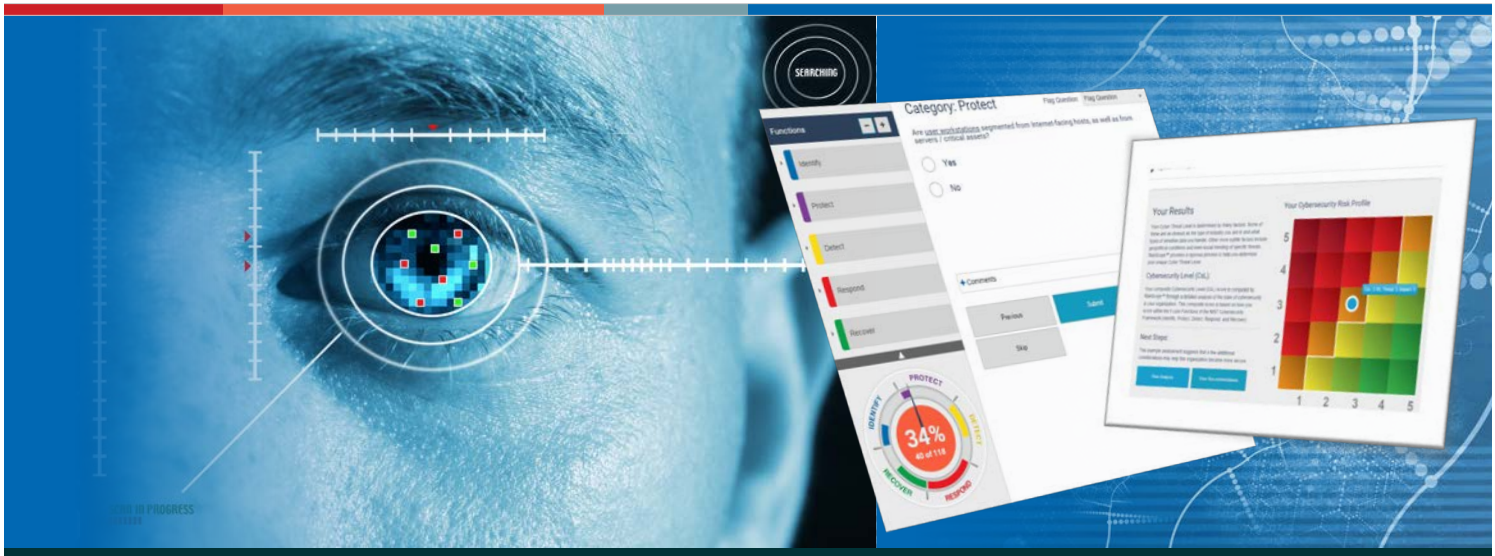
SelfAssure



Affordable Cyber Risk Management

Dynetics recognizes that many organizations struggle to allocate the resources necessary to assess and mitigate cyber risks. Therefore, our Cyber RiskScope® methodology, which we use for onsite, independently validated, cyber risk assessments, has been tailored and automated as **SelfAssure** so that clients have access to an affordable, cloud-based cyber risk management tool.

The Cyber RiskScope® Methodology

To create the necessary insight, Cyber RiskScope measures three Key Risk Indicators of cyber risk (Business Impact Value (BIV), Cyber Threat Level (CTL), and Cybersecurity Level (CsL)) and brings them together as a Cyber Risk Profile that visually conveys cyber risk. This simple approach helps bridge the communication gap between cybersecurity professionals and business leaders and is effective for small and large businesses alike. To remain affordable, SelfAssure focuses on your CsL and uses an industry characterization of CTL. Business Impact Values are not calculated within SelfAssure.

The Dynetics Difference

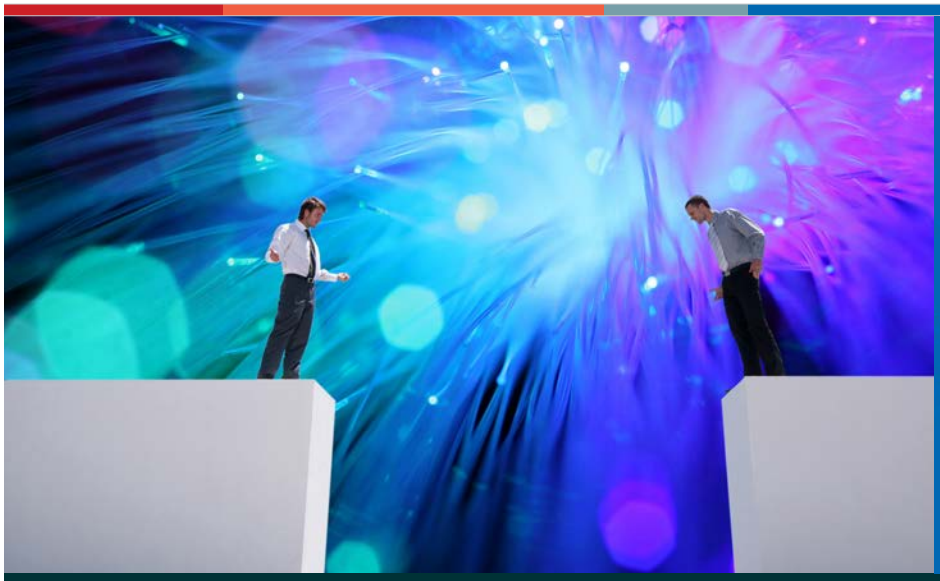
Dynetics has over 40 years' experience ensuring the success of high value, high risk, national security missions for agencies such as NASA, U.S. Army and Defense Intelligence Agency. Our experience includes over 16 years of information systems security assessment, mitigation and operations and literally over 1,000 cyber risk assessments for large and small, public and private entities using a variety of governance standards. However, our experience conducting advanced penetration tests really sets us apart and provides unique insights into cyber risks.

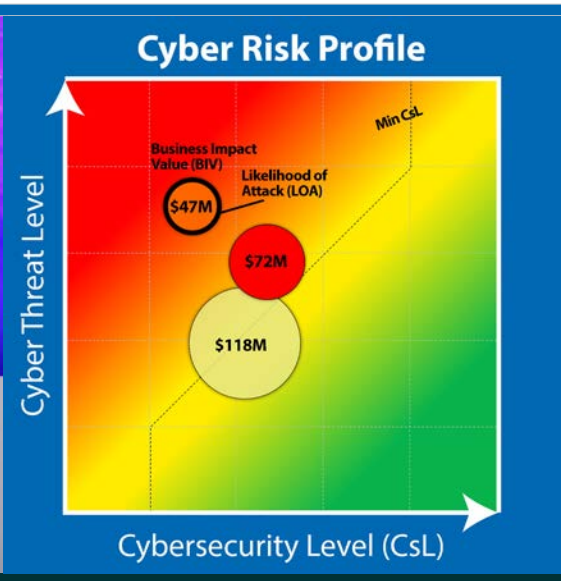
Dynetics supports one of only six Red Teams approved by National Security Agency to tests Department of Defense weapon systems. Therefore, our cyber risk analysts understand how sophisticated cyber criminals attack and avoid cybersecurity controls. This unique experience led to the development of a holistic set of cybersecurity objectives that are used to calculate a client's CsL, which is a measure of the efficacy of implemented cybersecurity controls. When compared to the strength of a client's anticipated cyber threat, or CTL, the ratio of CsL to CTL indicates the likelihood of a successful cyber attack. A ratio of 1.0 is considered the minimum acceptable level of risk.

To view introductory videos on SelfAssure and for more information on the complete portfolio of Cyber RiskScope solutions, visit www.CyberRiskScope.com.

SelfAssure's key features and benefits are described on the reverse of this page.

SelfAssure





Key Features and Benefits

Usability

- Internet-based "Software-as-a-Service" for easy, universal access
- Multi-user to allow the various organizations (even external contractors) that contribute to cybersecurity to participate in the self-assessment
- Question flagging to allow one user to assign a question to another user

Assessment Questions

- Based on holistic set of cybersecurity objectives that provide a comprehensive assessment of cyber risk
- Go beyond compliance to measure effectiveness of cybersecurity controls and provide a more accurate assessment of cyber risk

Analysis

- Calculates a customer's Cybersecurity Level (CsL) as a measure of the effectiveness of their cybersecurity
- Identifies a customer's Cyber Threat Level (CTL) by analyzing cybersecurity events and facts associated with the customer's industry
- Compares CsL to CTL to provide an indication of cyber risk
- Maps assessment results to the NIST Cybersecurity Framework so that customers can see specific areas of strength and weakness
  - Mapping to the NIST Cybersecurity Framework also provides customers with documented evidence of use of this important framework that is being viewed by the legal system as a minimum standard of care for cybersecurity.

Results

- Cyber Risk Profile that provides Sr.-level managers an easy-to-understand visualization of cyber risk
- RiskScope charts to show specific areas of strength and weakness
- Recommendations table with list of specific weakness that must be addressed to achieve a minimum level of acceptable risk
- Specific mitigation strategy for each identified weakness
- Decision aids for each identified mitigation strategy so customers can prioritize actions:
  - Impact of weakness of customer's cybersecurity risk
  - Need for hardware to implement mitigation strategy
  - Need for software to implement mitigation strategy
  - Indication of cultural or operation impact resulting from mitigation strategy
  - Relative costs associated with implementing mitigation strategy
- Reports capturing all results

Customer Support

- Service desk to assist clients with administrative issues or accessibility problems
- Service desk to assist clients with understanding questions and choosing appropriate answers

Cyber RiskScope®

www.CyberRiskScope.com

Dynetics

www.dynetics.com

D-16-7601