Cyber Security Capability

END TO END CYBER PROTECTION FROM PRODUCER TO CONSUMER
Change how your team handles incidents.
Examine seven ways to apply the Cyber Kill Chain® with a threat intelligence platform.
DOWNLOAD THE WHITEPAPER AT CYBER.LEIDOS.COM/SOLUTIONS/CYBER-KILL-CHAIN

PHASES OF THE INTRUSION KILL CHAIN

- **Reconnaissance**
  Research, identification, and selection of targets

- **Weaponisation**
  Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)

- **Delivery**
  Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)

- **Exploitation**
  Once delivered, the weapon’s code is triggered, exploiting vulnerable applications or systems

- **Installation**
  The weapon installs a backdoor on a target’s system allowing persistent access

- **Command & Control**
  Outside server communications with the weapons providing ‘hands on keyboard access’ inside the target’s network

- **Actions on Objective**
  The attacker works to achieve the objective, which can include exfiltration or destruction of data, intrusion of another target or physical asset, or environmental damage

---

**ENTERPRISE CYBER**

Leidos provides more than just firewalls, intrusion detection systems and encryption to defend against evolving cyber security threats. We understand you need a complete enterprise strategy for maximum protection to defend against evolving threats. Our cyber security experts deliver unmatched expertise in implementing full lifecycle cyber security solutions for the most critical systems through our unique Cyber Kill Chain® and Intelligence-Driven Computer Network Defence methodology.

The threat of not adequately protecting your core business is one of the top 10 risks for most organisations. Leidos can help create a secure and resilient environment through a combination of best practice processes, key technology components and, critically, employee training and awareness.

**FULL SPECTRUM CYBER DEFENCE**

The digital landscape presents a continual challenge to the operators of both Enterprise IT and Critical National Infrastructure. In tandem with the platform, a foundational understanding of how best to protect the network and staying up to date with the latest threat actors is critical.

This knowledge can help build resilience and harden the enterprise by delivering increasing capability and security at a reducing cost. A truly protected organisation requires the appropriate skills and tradecraft as well as the optimal infrastructure and network design.

**PROTECTING CRITICAL NATIONAL INFRASTRUCTURE**

The threat of cyber attack for critical national infrastructure – be it energy networks, transport infrastructure, financial or healthcare systems – is significant. Deviation from normal operations can have a catastrophic effect on the population at large, ranging from the interruption of water supply to large-scale disruption of power generation and availability. At the heart of these complex and key infrastructures lies a network of industrial control systems very different to traditional IT, but just as open to attack.

With our extensive experience of process control system security, in conjunction with traditional IT security for over 200 international customers, Leidos provides in-depth cyber, compliance, asset, policy and change management to ensure our critical national infrastructure remains secure.

**CORPORATE ENABLEMENT**

Cyber threats are human threats – the acts of malicious individuals and organisations. We believe practitioner expertise in cyber tradecraft makes the critical difference in an ever-more dangerous world. Our mission is to up-skill our customers in the tradecraft they need to operate more effectively. As technology continues to level the playing field against governments and corporates, the role of cyber tradecraft and its practitioners becomes increasingly important.

This tradecraft is a vital capability that creates a security advantage and Leidos is committed to helping your key people recognise the risk and identify the actions required to secure your business – from analysts protecting the front line to directors leading the enterprise.

**CYBER KILL CHAIN®**

Leidos’ Computer Incident Response Team has created an Intelligence-Driven Computer Network Defence process, Cyber Kill Chain®, which allows information security professionals to proactively remediate and mitigate advanced threats in the future.

While the challenge of staying ahead of the attacker never ends, at Leidos we’ve developed our cyber tradecraft by systematically protecting both our own, and our customers’, enterprise. Our tradecraft and tools are unmatched, our Cyber Kill Chain® methodology recognised as the leading approach to cyber security and our track record one you can trust to protect your organisation in to the future.
Change how your team handles incidents.
Examine seven ways to apply the Cyber Kill Chain® with a threat intelligence platform.

DOWNLOAD THE WHITEPAPER AT CYBER.LEIDOS.COM/SOLUTIONS/CYBER-KILL-CHAIN

PHASES OF THE INTRUSION KILL CHAIN

- **Reconnaissance**
  Research, identification, and selection of targets

- **Weaponisation**
  Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)

- **Delivery**
  Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)

- **Exploitation**
  Once delivered, the weapon’s code is triggered, exploiting vulnerable applications or systems

- **Installation**
  The weapon installs a backdoor on a target’s system allowing persistent access

- **Command & Control**
  Outside server communications with the weapons providing ‘hands on keyboard access’ inside the target’s network

- **Actions on Objective**
  The attacker works to achieve the objective, which can include exfiltration or destruction of data, intrusion of another target or physical asset, or environmental damage

**ENTERPRISE CYBER**
Leidos provides more than just firewalls, intrusion detection systems and encryption to defend against evolving cyber security threats. We understand you need a complete enterprise strategy for maximum protection to defend against evolving threats. Our cyber security experts deliver unmatched expertise in implementing full lifecycle cyber security solutions for the most critical systems through our unique Cyber Kill Chain® and Intelligence-Driven Computer Network Defence methodology.

The threat of not adequately protecting your core business is one of the top 10 risks for most organisations. Leidos can help create a secure and resilient environment through a combination of best practice processes, key technology components and, critically, employee training and awareness.

**PROTECTING CRITICAL NATIONAL INFRASTRUCTURE**
The threat of cyber attack for critical national infrastructure – be it energy networks, transport infrastructure, financial or healthcare systems – is significant. Deviation from normal operations can have a catastrophic effect on the population at large, ranging from the interruption of water supply to large-scale disruption of power generation and availability. At the heart of these complex and key infrastructures lies a network of industrial control systems very different to traditional IT, but just as open to attack.

With our extensive experience of process control system security, in conjunction with traditional IT security for over 200 international customers, Leidos provides in-depth cyber, compliance, asset, policy and change management to ensure our critical national infrastructure remains secure.

**CORPORATE ENABLEMENT**
Cyber threats are human threats – the acts of malicious individuals and organisations. We believe practitioner expertise in cyber tradecraft makes the critical difference in an ever-more dangerous world. Our mission is to up-skill our customers in the tradecraft they need to operate more effectively. As technology continues to level the playing field against governments and corporates, the role of cyber tradecraft and its practitioners becomes increasingly important.

This tradecraft is a vital capability that creates a security advantage and Leidos is committed to helping your key people recognise the risk and identify the actions required to secure your business – from analysts protecting the front line to directors leading the enterprise.

**CYBER KILL CHAIN®**
Leidos’ Computer Incident Response Team has created an Intelligence-Driven Computer Network Defence process, Cyber Kill Chain®, which allows information security professionals to proactively remediate and mitigate advanced threats in the future.

While the challenge of staying ahead of the attacker never ends, at Leidos we’ve developed our cyber tradecraft by systematically protecting both our own, and our customers’, enterprise. Our tradecraft and tools are unmatched, our Cyber Kill Chain® methodology recognised as the leading approach to cyber security and our track record one you can trust to protect your organisation in to the future.

**FULL SPECTRUM CYBER DEFENCE**
The digital landscape presents a continual challenge to the operators of both Enterprise IT and Critical National Infrastructure. In tandem with the platform, a foundational understanding of how best to protect the network and staying up to date with the latest threat actors is critical.

This knowledge can help build resilience and harden the enterprise by delivering increasing capability and security at a reducing cost. A truly protected organisation requires the appropriate skills and tradecraft as well as the optimal infrastructure and network design.
Regular, accurate and actionable cyber threat intelligence is key to a well-protected infrastructure. Through a combination of our own Security Intelligence Centres, the Cyber Security Alliance and our portfolio of Open Source Intelligence (OSINT) tools, including LM Wisdom™; Leidos ensures predictability on the threat landscape at any given time.

Our specialists combine tradecraft with technical solutions that help to provide integrated and comprehensive intelligence, able to better protect our customers and enable proactive collaboration with the industry at large. We believe cyber security is a team sport and the cyber threat is significantly diminished through consistent and considered intelligence gathering and sharing.

TODAY THERE’S NOTHING MORE VALUABLE THAN INFORMATION. AND THE ABILITY TO SECURE IT.

Leidos is a global science and technology solutions leader working to solve the world’s toughest challenges in the defense, intelligence, homeland security, civil, and health markets. The company’s 33,000 employees support vital missions for government and commercial customers.

Headquartered in Reston, Virginia, Leidos reported pro forma annual revenues of approximately $10 billion for the fiscal year ended January 1, 2016 after giving effect to the recently completed combination of Leidos with Leidos’ Information Systems & Global Solutions business (IS&GS).

For more information, visit Leidos.com.

Telephone: +44 (0) 1252 553200 or email: victoria.edwards@leidos.com