PACKIT™

Proven, Analytic-Centric Kill Chain Implementation and Transformation

Organizations around the world are facing unprecedented cyber-attacks that are more sophisticated, frequent, and more severe than ever before. Adversaries are well funded, organized, and will stop at nothing to infiltrate targeted networks and exploit sensitive information. Keeping pace with the rapidly growing threat environment takes an approach leveraging intelligence, strategic planning, and teamwork. Security organizations find it difficult to implement a longer-term strategic plan amidst the tactical day-by-day security activities that absorb their security teams' time and focus.

OUR APPROACH

PACKIT™ (Proven, Analytic-Centric Kill Chain Implementation and Transformation) is our threat-based approach to conducting and improving cyber defense. PACKIT leverages people, process and technology to operationalize and implement an analytical framework (such as the Cyber Kill Chain®) to improve an organization's cybersecurity posture.

Best practices in cybersecurity involve a two-fold implementation of a threat-based and intelligence-driven network defense strategy, coupled with a powerful analytic framework. This dual approach ensures tactical daily defensive monitoring and triage is tied to a framework that provides the basis for a customer-focused intelligence repository. The network defense strategy component is derived from Leidos' own comprehensive assessment and concludes with Leidos delivering a detailed, prioritized roadmap that articulates the near- and longer-term initiatives based on the customer's specific goals and available resources.

With PACKIT, we put this methodology into practice, using existing customer teams, technologies, and operations to maximize visibility and return on investment. The analytic framework may be the Lockheed Martin Cyber Kill Chain, the MITRE ATT&CK method, the Intrusion Defense Chain, or a variation of these.

Our Leidos implementation is device- and framework-agnostic, building on the strong foundational commitments and honing the tradecraft of the analysts through strategic initiatives.

Through our decades of experience, we bring the capability to mitigate sustained, persistent attack campaigns; measure our effectiveness against changing adversarial tactics, techniques, and procedures (TTPs); and prioritize cyber mitigation efforts and investment strategies. At Leidos, we have the experience, metrics, cost savings, and lessons learned through true application of the practice. We develop and execute customized plans to improve cybersecurity, preventing adversary activity (both broad-based and nation-state), and conduct cyber operations for a variety of organizations.

PROVEN SUCCESS

Using our cybersecurity maturity model, we have led transformations for three of the four largest federal government SOCs, and more than 20 geographically dispersed Fortune 500 commercial SOCs through our unique PACKIT approach. Our overarching SOC policy and adoption support is unmatched. We achieved superior results by using appropriate personnel and skill sets, applying repeatable PACKIT methods, and optimizing technologies. Results include:

- Discovered four times the number of sophisticated adversaries targeting a large federal agency network. This increased awareness of active cyber-attacks allowed the cyber defenders to improve our defensive TTPs to thwart attacks and mitigate vulnerabilities.
- Identified more than 10 previously unidentified nation-state actor sets.
- Increased the time analysts spend on high-value functions (analysis and knowledge management) by almost 60%.
- Improved sensor tuning, resulting in greater than 50% reduction in false positives reporting.
- Identified 22 duplicative/under performing tools for retirement, which resulted in direct and immediate cost savings to the customer.
- Successfully implemented our advanced cyber measures of effectiveness to quantify and track all advanced persistent threat activity across the customer within 6 months of contract kick-off.

WHY PARTNER WITH LEIDOS?

The PACKIT solution leverages Leidos' own decade-long journey of advanced persistent threat learning and technology deployment and enables us to deploy the same methodology in a fraction of the time. Our breadth of customers from commercial to all areas of government and our extensive experience within SOCs provide a proven partner well-vested in our collective network defense capabilities and experience as a security practitioner.

Leidos' PACKIT solution is flexible to accommodate alternative adversary tracking and security operations models, providing a tailored yet comprehensive security assessment and path forward. By improving our collective network defensive cyber operations (DCO), we are a cyber powerhouse ready to help you build a strong foundation and mature capabilities to meet the challenges of an ever-evolving cyber threat landscape.

NEXT STEP

With our proven solution suite and highly skilled professionals, we can provide comprehensive support no matter where you are on your cybersecurity journey. Contact us today.

FEATURES AND BENEFITS

- Delivers a comprehensive Cyber Defense Maturity Evaluation assessment, a tailored Strategic Cybersecurity Roadmap, and detailed roadmap execution plan
- Leverages technology as a force multiplier for our analysts
- Provides customers access to thought leadership advisors and real-time information flow government and commercial sources
- Operationalizes and implements an analytical framework to improve cybersecurity posture
- Conducts intelligence-based cyber defense and creates an adaptive cybersecurity organization
- Transforms Security Operations Centers (SOCs) to Security Intelligence Centers (SIC)
- Offers operationally-focused cyber training curriculum
- Provides advanced cyber metrics, including:
  - Cyber Threat Heatmap – for threat campaign tracking over time
  - ROI Incident Mitigation Scorecard – for evaluation of investment and ability to detect and block attacks from most prioritized campaign threat actors/groups
- Maximizes ROI of in-house technology investments
- Tracks advanced persistent threat (APT) campaigns
- Increases automation while reducing false positives so analysts can focus on high-value tasks

FOR MORE INFORMATION

leidos.com/competencies/cyber

eTrace Record 20243 | 18-0210 | Leidos Creative