Protecting Your Information

TRUSTED CYBER SERVICES AND SOLUTIONS
ADVANCED MALWARE THREAT DETECTION AND DEFENSE

Your networks contain critical information that your organization uses to sustain a competitive advantage across your industry, nation, and world. Crime syndicates, state-sponsored actors, and hacktivists want proprietary information for financial, political, and social gain. Their advanced malware infiltrates networks, maneuvers to find and access critical systems, sends information to their malware masters, while remaining present and undetected on your networks for future purposes.

Their capabilities are increasing in sophistication and volume, while the network loses its secure borders due to worker mobility, BYOD, a connected supply chain, social media, and more. The challenge and stakes of protecting the network within this environment have never been higher, and continue to increase dramatically. Where can you turn for help?

Leidos will be your trusted teammate and will defend your network from these constantly evolving threats. Our security engineering and security threat operations subject matter experts will work with you to provide end-to-end solutions and services that safely integrates technologies, institutes best practice processes, and delivers comprehensive solutions to proactively manage the risks posed by advanced threats.

OUR APPROACH

Leidos works with you to protect, detect, respond, and remediate persistent, targeted attacks on your networks by:

- Quickly detecting suspicious and malicious activity either remotely or with our rapid response team onsite
- Diagnosing advanced malware and infiltration methods
- Remediating your systems after a persistent compromise
- Monitoring and defending your network 7x24 to limit the success of advanced threats
- Continually updating you on our progress through your own web-based portal, calls with our analysts, and customized reporting

OUR SOLUTIONS

Threat analysis. To deploy successful solutions that will counter and expose advanced threats, the nature, methodology, and tradecraft of the adversary must be known and tracked. We compile this information through active threat research, analysis and correlation, penetration testing, and monitoring to build a dynamic threat landscape, which can then be incorporated into our detection technology and incident response tools. We can support your situational awareness of global and specific threats to your network.

Security engineering and integration. With a focus on advanced threats, our security engineers will design and implement better defensive architectures, or add capabilities to existing security implementations, to effectively address operational needs, proactively balance risk management, and adhere to compliance. There are so many platforms, appliances, and tools to choose from – we can help you identify the right tools for your needs and integrate them to work seamlessly in your network.
“Live correlation of massive amounts of disparate data in-stream gives organizations their first glimpse of actionable digital intelligence with activity-based, contextual information to drive business decisions.”

— GULU GAMBHIR
SAIC Senior Vice President,
Group Chief Technology Officer

- Advanced malware detection. We help prevent future attacks by building upon previously identified malware and tactics and applying research and analysis results, state-of-the-art malware detections tools, custom behavior-based algorithms, and the honed techniques of our security analysts. Our solution and supporting service identifies malware and anomalous traffic as it enters the network, when resident on endpoints, and when it accesses command and control channels.

- Threat monitoring. Our 7x24x365 detection, alert, and triage managed security service, performed from our redundant secure network operations centers, allows you to leverage our expertise to protect your network through increased situational awareness. We deploy a solution to enable log collection, correlation, and analysis for effective advanced malware monitoring by our threat analysts. We keep you informed through a custom portal and real-time alerts.

- Threat Validation and Incident Response. After a suspected compromise, we can perform diagnostics and validation of compromises caused by advanced malware and offer mitigation advice and services to protect the network, hosts, and users from further attacks. We give you the information you need in time to make critical decisions about your network and its defenses. We can help you deploy the mitigation strategies to protect your network, hosts, and users.

- Forensic Analysis. Our team of digital forensic analysts will discover and assess compromised systems for unauthorized access, suspicious behavior, or command and control channels to identify attack vectors, malware, and persistent activity. We use rigorous processes and state of the art tools to provide thorough, accurate, and timely analysis.

ALMOST 3/4 OF AMERICANS HAVE FALLEN VICTIM TO CYBER CRIME

73%
Why Leidos?

We bring extensive experience in advanced security services and solutions:

- As a member of the Defense Industrial Base, Leidos is a prime target for advanced malware from modern threat actors, giving us daily experience in detecting and remediating advanced malware intrusions. The same team that defends Leidos’s networks defends our customers’ networks.

- Over the past 10 years, our monitoring services have successfully defended our clients’ networks by identifying advanced malware through hallmarks of its behavior and compromises.

- Our forensic and incident response teams deploy within a day’s notice to diagnose and mitigate incidents on the largest military network, as well as for our commercial clients.

Our own network environment is a tremendous test-bed for our solutions and services, as it is distributed globally, includes diverse operating environments in multiple zones of security, and services 40,000 users with over 100,000 devices. We prove our solutions and services within Leidos’s networks before offering them to our clients.