



Advanced Persistent Threat (APT) Resistance

Are you sure you can trust your network?

"Advanced Persistent Threat" (APT) is the generic term given to the latest wave of cyber criminality. Hackers and organised criminals are using APT's to breach IT defences and steal information. Many of the techniques are not new, or particularly advanced. However, the combination of social engineering and targeted "signature resistant" malware means that organisations should review their existing defences, their risk tolerance and should seriously consider a "what if" scenario. These attacks use 'Spear Phishing' to gain entry into an organisation's network, by carefully constructing a spoofed e-mail which encourages the employee to click on a link to malware or infected website. These are not casual criminal hackers, but professionals aimed at stealing your data and maintaining a presence on your network to gain an economic or intellectual advantage.

"The APT compromises any target it desires. It only needs one vulnerable user!"

To resist these attacks, Enterprises need a Security Partner with a 360° approach. CIPHER'S solution uses a combination of best-of-breed and new technologies, surrounded by an effective security awareness programme and 24x7 Agile Security Information Event Management (SIEM) Service:

"Less than 24% of APT attacks are detected by AV (source: M-Trends report)"

- 1 Digital bodyguard for key executives, making sure that their external profile is protected, as well as their identity.
- 2 Dynamic awareness training, with important information and guidelines for working with safety both at home and in the office.
- 3 Highly efficient content filtering, with links to both internal and external threat monitoring.
- 4 White listing applications / End point virtualisation, enabling kiosk-like locked down security to the desktop.
- 5 Zero-day Malware Protection System (MPS), with sandbox execution of potential malware files and management of port usage.
- 6 Enhanced Privileged User Management, in order to monitor and manage key system administrators.
- 7 State of the Art Endpoint, Network and Database encryption, tied into a single key management system.
- 8 Agile Application-aware Security Information Event Management (SIEM) service, which can give the earliest warning of potential attack.



What next?

CIPHER recommends that an Enterprise needs to understand their current APT exposure through testing and locating active malware and risk assessments. This would be followed by a control improvement initiative, focused on APT resistant technology solutions, combined with awareness campaigns and security process changes. Underpinning the programme is the migration towards a full agile and application aware Security Information and Event Management (SIEM) service.

Gap Analysis	Control Improvement	Agile SIEM service
<ul style="list-style-type: none"> • APT Penetration Testing • APT Locating Active Malware • APT Control Review & Risk Assessment 	<ul style="list-style-type: none"> • Awareness Campaign • Focused Technology Solutions • Security Process Improvement • Architectural Re-engineering 	<ul style="list-style-type: none"> • Design & Implementation <ul style="list-style-type: none"> • Loggers / sensors • Connectors • Correlation engine with CIPHER customised security use cases and rules • Customised Dashboard Views

Key Benefits

- Effective threat detection, response and recovery capabilities
- Defence in depth protection for your critical assets
- Comprehensive visibility of risks, vulnerabilities and threats

“APT Resistant solutions and services will dramatically reduce the likelihood and impact of cyber-attacks”



About CIPHER

CIPHER is a multinational, specialist Information Security and Risk Management company, with over 300 employees. Our services include; Consulting and Auditing (PCI-DSS QSA, ISO 2700x and industry / country regulations), Award winning security system integration and 24x7 SOC/SIEM, with over 300,000 assets under management in 35 countries, correlating 1,000,000 events daily. In addition, we conduct Research & Development through our Intelligence Lab, supporting the CIPHER university and (ISC)² training centres. CIPHER is dedicated to delivering quality, excellence and innovation.