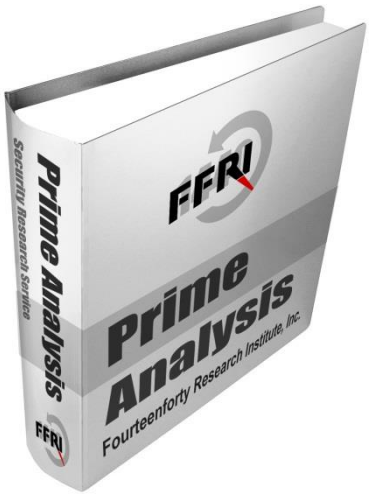

セキュリティコンサルティング、情報提供サービス

Prime Analysis

独自発見脆弱性脅威分析、パッチ解析、マルウェア解析、緊急ブリーフィングなど

世界トップレベルのセキュリティリサーチチームが脅威分析ノウハウを提供

0-day脆弱性の増加、標的型攻撃、見えにくい攻撃、情報のアンダーグラウンド化・・・。 セキュリティを取り巻く脅威はさらに複雑化し、かつ急速に変化しています。的確なリスク管理を実現するためには、日々発生する新たな脅威に対抗するための、迅速かつ正確な情報収集能力、分析能力、問題解決能力が求められます。Prime Analysisは、組織が抱えるこれら課題の解決を強力に支援する包括的リサーチサービスです。

FFRIのセキュリティリサーチチームは、多様化・複雑化するセキュリティ脅威に対抗するための、強力かつ広範な技術力を備えた専門家チームです。ワールドワイドに広がる独自の情報源から日々得られる情報を正確に分析し、迅速かつ的確なソリューションを提供します。

国内最多のクリティカルなソフトウェア&組み込み製品の脆弱性発見の実績

攻撃技術をベースとした技術シーズを対策技術に展開

100を超える日本最多のクリティカルなセキュリティ脆弱性発見の実績
(例) Microsoft Windows (LSASS脆弱性、wkssvc脆弱性、アニメーションカーソル脆弱性、GDI脆弱性、Office製品、Internet Explorer など多数)、 Winny、一太郎、QuickTime、Realplayer、など他多数
(直近例) Microsoft Windows標準搭載のIPv6スタックに脆弱性発見(MS10-058)

Microsoft Windows 7 のセキュリティ機能評価 など、多数のセキュリティ脅威分析の実績
http://www.microsoft.com/japan/business/enterprise/ecc/article/tdm1101_security1-3.mspx

記事、専門雑誌、新聞、NHKニュースなどメディアに多数掲載
- 「標的型攻撃のマルウェアを解析してわかる事実--FFRI 鵜飼裕司氏」 (builder)
  http://builder.japan.zdnet.com/news/story/0,3800079086,20367832,00.htm
- ホワイトハッカー道場「悪魔のツール"ルートキット"最前線」 (日経ITPro)
  http://itpro.nikkeibp.co.jp/article/COLUMN/20070928/283201/
- 「複雑化する標的型攻撃、脅威の解析ツールやエンジニアの育成が課題」 (INTERNET Watch)
  http://internet.watch.impress.co.jp/cda/event/2008/03/25/18937.html

セキュリティ脆弱性対策研究に関する多数の研究発表実績
BlackHat USA/Japan、RSA Conference、CanSecWest、RECONなど多数の国際カンファレンスで脆弱性分析、マルウェア分析に関する研究を発表。
http://www.fourteenforty.jp/research にて、多数の 研究成果を発表。

経済産業省「新世代情報セキュリティ研究開発事業」の研究成果の技術を本サービスに展開
2010年より、情報家電、スマートグリッド、携帯端末など、非PC端末における未知脆弱性の自動検出技術研究を実施
http://www.meti.go.jp/information/data/c101207aj.html

Prime Analysis サービスメニュー

	Lite	Basic	Advanced
■ Weekly Report（1回 / 週） 新たな脆弱性情報やインシデント情報、exploit情報などを収集し、独自の分析を行ったレポートを毎週発行	✓	✓	✓
■ Prime Research（1回以内 / 3ヵ月） ①独自に発見した脆弱性の詳細な脅威分析と対策 ②非公開リサーチプロジェクトへのアクセス	✓	✓	✓
■ Consulting（5時間以内 / 月） 御社組織におけるセキュリティ上の意思決定に関するご相談、各種セキュリティ関連技術に関する質問などをコンサルティング	✓	✓	✓
■ Quarterly Meeting（4回以内 / 年） 御社へ訪問し、Prime Analysisに関するご質問やフリーディスカッション及び弊社内で現在進行中の研究を発表			✓
■ Custom Malware Research（4回以内 / 年） ファイルやペイロードをご提供頂き、exploitやMalwareを解析。また発見された脅威に対抗するため、環境に応じた対策手順をご案内。			✓
■ 0-day Research（不定期・発表あり次第） 公開されたクリティカルな未パッチ脆弱性や検証コードを即座に解析し、情報ソースの信頼性、脆弱性の質、影響範囲、攻撃ベクタ、exploitで利用されているテクニック、exploitingの安定性など、詳細かつ正確な脅威分析をリアルタイムにご提供。		✓	✓
■ Custom 0-day Research（4回以内 / 年） 0-day脆弱性の有無を解析。発見された脅威に対抗するため、環境に応じた対策手順をご案内。設定などで回避できない場合には、パッチ開発など独自の一時回避策に関するリサーチを行い、成果物をご提供。			✓
■ MS-bulletin Research（不定期・発表あり次第） Microsoft Security Bulletinがリリースされると深刻なものから即座に脅威分析を行い、より詳細な情報をご提供。 公開exploitの所在、一次情報源、より詳細な脆弱性の質、攻撃ベクタ、exploit安定性などの分析を行い、また、パッチ差分解析などで得られた有用な情報（脆弱性修正箇所や非公開脆弱性の修正の有無など）があれば詳細な解説をご提供。		✓	✓
■ Rapid Notification（不定期・インシデント発生し次第） 0-day悪用による大きな脅威など緊急対応が必要なインシデントが発生した場合、即座にその脅威を分析し、お客様の緊急連絡先メールアドレスに連絡。発生した脅威に関する詳細かつ正確な情報を速やかにご提供。		✓	✓

製品・サービスについてのお問い合わせは
株式会社ＦＦＲＩ
〒150-0013
東京都渋谷区恵比寿1-18-18　東急不動産恵比寿ビル4階
TEL：03-6277-1811　E-mail：sales@ffri.jp
本製品に関する情報はインターネットでもご覧いただけます。
https://www.ffri.jp/

2014年11月現在
Ver 2.00.05