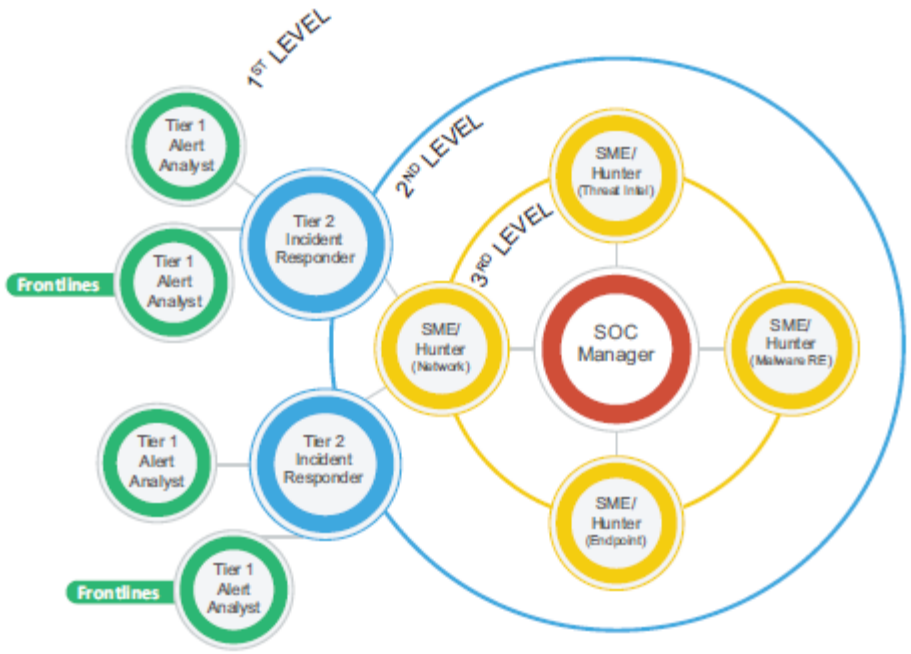
The power to do more

Снижение рисков внутренних угроз ИТ-безопасности

Security Operations Centre (SOC) – **схема процессов**.

Структура SOC.



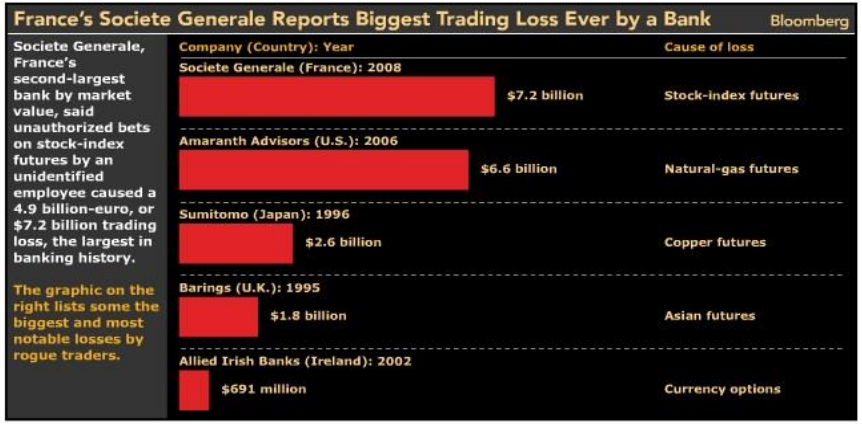
Наиболее опасный
вектор атаки – изнутри.

Хрестоматийный пример.

Bloomberg Our Company | Professional | Anywhere

HOME QUICK NEWS OPINION MARKET DATA PERSONAL FINANCE TECH POLITICS SUSTAINABILI

Societe Generale Reports EU4.9 Billion Trading Loss (Update8)



By Gregory Viscusi and Anne-Sylvaine Chassany - January 24, 2008 15:20 EST

The New York Times

World Business

French Bank Says Rogue Trader Lost $7 Billion

By NICOLA CLARK and DAVID JOLLY
Published: January 25, 2008

Correction Appended

PARIS — A French bank announced Thursday that it had lost $7.2 billion, not because of complex subprime loans, but the old-fashioned way — because a 31-year-old rogue trader made bad bets on stocks and then, in trying to cover up those losses, dug himself deeper into a hole.

TWITTER
LINKEDIN
SIGN IN TO E-MAIL
PRINT
SINGLE PAGE
REPRINTS
SHARE

Jérôme Kerviel, 31, was a low-level bank employee.

Société Générale, one of France's largest and most respected banks, said an unassuming midlevel employee who made about 100,000 euros ($147,000) a year — identified by others as Jérôme Kerviel — managed to evade multiple layers of computer controls and audits for as long as a year, stacking up 4.9 billion euros in losses for the bank.

Unlike many of his high-level trading colleagues, Mr. Kerviel graduated not from one of France's elite

«Пирамида доступа».

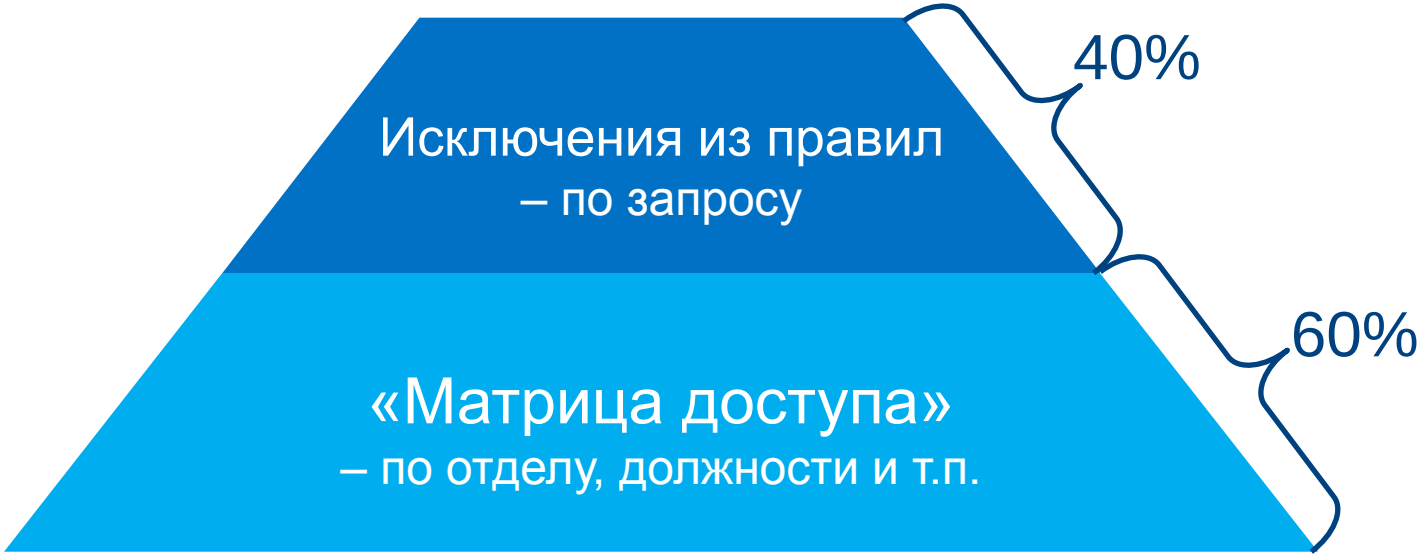
«Пирамида доступа»

«Матрица доступа»
– по отделу, должности и т.п.

Основные рекомендации.

- Ролевая модель.
  - “Role-mining” – понимание существующих ролей в организации.
  - “RBAC” – внедрение «Матрицы доступа».

«Пирамида доступа»



Основные рекомендации.

- Ролевая модель.
- Обработка исключений из ролевой модели.
  - Сохранение разделения полномочий.
  - Вовлечение юридически ответственных лиц.
  - Вовлечение информбезопасности.
- Ре-сертификация доступа.
  - Периодическая проверка доступа юридически ответственными лицами.

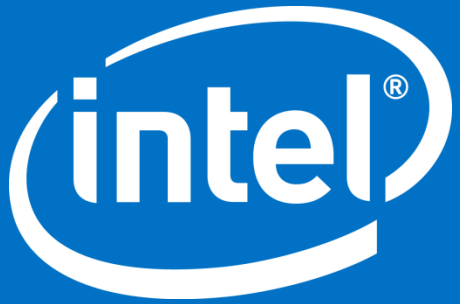
«Пирамида доступа»

Основные рекомендации.

- Ролевая модель.
- Обработка исключений из ролевой модели.
  - Сохранение разделения полномочий.
  - Вовлечение юридически ответственных лиц.
  - Вовлечение информбезопасности.
- Ре-сертификация доступа.
  - Периодическая проверка доступа юридически ответственными лицами.
- а также...

Контроль привилегированного доступа.

- Администраторы ключевых систем.
  - AD.
  - E-mail (Exchange/Notes).
  - SWIFT.
  - …
- Временные администраторы.
  - Консультанты и т.д.
- Прочие учетные записи
  с повышенными привилегиями.


intel®

The power to do more