

# Incident Response Panel

SANS Forensic Summit 2009

**General Electric**

**GE-CIRT**

**ken.bradley@ge.com**

*IT security pwn@g3*

**IF YOU HAVE A PROBLEM, IF NO  
ONE ELSE CAN HELP, AND IF  
YOU CAN FIND THEM, MAYBE  
YOU CAN HIRE...**

THE

CIRT



**MISSION:**

**LIST THE TRAITS AND  
EQUIPMENT THAT WOULD  
MAKE UP A WORLD CLASS  
INCIDENT RESPONSE TEAM**

**MISSION: H@XOR BM-BF**

# **KEN BRADLEY**

## **INCIDENT HANDLER FOR THE GE-CIRT**

**FORMER AIR FORCE INVESTIGATOR**

**IT SECURITY CONSULTANT**

**INCIDENT RESPONDER FOR THE ENTERPRISE**



# **LEADERSHIP**

**VISIONARY**

**COMMUNICATES WELL WITH CONSTITUENCY**

**RESPECTED BY HANDLERS AND PEERS**



# **BUSINESS RELATIONS**

**THICK SKINNED**

**UNDERSTANDS BUSINESS BEYOND  
TECHNOLOGY REALM**

**STRONG PROJECT  
MANAGEMENT**

**GOOD PEOPLE SKILLS**



# **INTELLIGENCE OPERATIONS**

**JUST A BIT PARANOID**

**STRONG TECHNOLOGIST W/ CHESS PLAYER'S  
MINDSET**

**PASSIONATE PROBLEM  
SOLVER**

**ELEVATED SENSE OF  
OBSERVATION**





**GROUND OPERATIONS**  
***A.K.A HANDLERS***

**MALWARE ASSASSIN**

**STRONG NETWORKING BACKGROUND**

**MULTIPLE OPERATING SYSTEMS POWER USER  
W/ PROGRAMMING OR ADVANCED SCRIPTING  
CAPABILITY**

**SOME INSANITY NECESSARY**





## **TOOLS AND TACTICS**

**WORK FOR YOUR TEAM, NOT FORCE YOUR TEAM TO WORK**

**FACILITATE REMOTE RESPONSE WITH FULL ENTERPRISE REACHABILITY TO PREVENT UNNECESSARY TRAVEL**

**INTEGRATE WITH REPORTING MECHANISMS AND FREE YOUR HANDLERS TO FOCUS ON ANALYSIS**



*ken.bradley@ge.com*

THANK YOU FOR YOUR  
ATTENTION