COMPENSATING CONTROLS

by James Keeling (Sample)

Chapter 3

Over 10 million different log entries were gathered from Allied Computing that day, from a myriad of different sources; Switches, routers, firewalls, servers, and even desktop PCs forwarded a record of all activity to a centralized logging system totaling 180 GB of data which was then packaged and sent across a Virtual Private Network (VPN) tunnel to SecureMore a Managed Security Services Company providing log review and processing to a number of businesses across the country. This log data is handled by an intelligent sorting system which parses the logs and utilizing state of the art heuristics determines which log entries are of interest and deserve attention. For example, a single logon failure can easily be attributed to a user who is fumbling his coffee while logging in and mistypes his password, whereas groups of two failed logins, repeated consistently 20 minutes apart for 8 hours on the same user account very well might indicate that someone is trying to break into your network. These special cases are flagged and sent for personal review by a fleshy.

* * *

Greg Holland was a fleshy; a bona-fide flesh and blood human. It was his very important task to review these special log entries and determine the appropriate action to take. He could single-handedly save a company, nay - "The World" from ruin by assisting in the capture and prosecution of technologically savvy evil doers. This was Greg Holland's mission. This was his life.

Greg Holland was bored. He was a 3rd year student at a local university and while studying history and library sciences took up most of his time, he still needed a job. SecureMore fit the bill nicely; mindless job, decent pay, and evening hours. Greg's cubicle was set amidst a sea of foam green replicas encompassing the entire third floor of a looming structure in an anonymous office park on the south side of town. Everything about his job was anonymous, from the sparsely furnished cubicles with nothing more to catch the eye than a chair, a phone, and a PC, and a row of binders containing the "General Operating Procedures".

Even the name on the cubicle was anonymous - Technician #32-34.

COMPENSATING CONTROLS

by James Keeling (Sample)

Chapter 3

Over 10 million different log entries were gathered from Allied Computing that day, from a myriad of different sources; Switches, routers, firewalls, servers, and even desktop PCs forwarded a record of all activity to a centralized logging system totaling 180 GB of data which was then packaged and sent across a Virtual Private Network (VPN) tunnel to SecureMore a Managed Security Services Company providing log review and processing to a number of businesses across the country. This log data is handled by an intelligent sorting system which parses the logs and utilizing state of the art heuristics determines which log entries are of interest and deserve attention. For example, a single logon failure can easily be attributed to a user who is fumbling his coffee while logging in and mistypes his password, whereas groups of two failed logins, repeated consistently 20 minutes apart for 8 hours on the same user account very well might indicate that someone is trying to break into your network. These special cases are flagged and sent for personal review by a fleshy.

* * *

Greg Holland was a fleshy; a bona-fide flesh and blood human. It was his very important task to review these special log entries and determine the appropriate action to take. He could single-handedly save a company, nay - "The World" from ruin by assisting in the capture and prosecution of technologically savvy evil doers. This was Greg Holland's mission. This was his life.

Greg Holland was bored. He was a 3rd year student at a local university and while studying history and library sciences took up most of his time, he still needed a job. SecureMore fit the bill nicely; mindless job, decent pay, and evening hours. Greg's cubicle was set amidst a sea of foam green replicas encompassing the entire third floor of a looming structure in an anonymous office park on the south side of town. Everything about his job was anonymous, from the sparsely furnished cubicles with nothing more to catch the eye than a chair, a phone, and a PC, and a row of binders containing the "General Operating Procedures".

Even the name on the cubicle was anonymous - Technician #32-34.

Personal items were strictly prohibited and nobody wanted to cross Mr. Goethe, the shift supervisor. People said he once threw a chair over a cubicle wall and knocked technician #41 out cold. So here Greg sat, night after night, watching as log entries appeared on his screen demanding

attention.

Greg was given two options for each entry that was forwarded to him. There were two buttons on his computer screen so impossibly large that even the legally blind couldn’t miss them. The first one said "Discard" whereas the second said "Escalate". A discard meant simply that. The entry was discarded as a false positive, normal activity which at first seemed suspect, but in reality didn't mean squat. Escalate on the other hand would catapult the entry up with all due speed to the fourth floor where it would be handled by another technician with yet another "Discard/Escalate" choice to make.

Greg knew where he was, he understood the futility of it all. He simply wanted to be a librarian, but this job was notorious for turnover and came open just as he was downsized from a local coffee bar. As network security has become a booming industry of late, the job did indeed pay well.

Greg sighed to himself as the clock on his computer ticked over to 5:30a.m.

See Greg sit.

See Greg click on the buttons.

See Greg die of boredom.

"Discard"

"Discard"

"Discard"

"Discard"

"Escalate"

"Discard"

"Escalate"

"Discard"

"NOTICE: Special Log Entry Occurrence Detected. Call Central Operations at 732-555-7263 immediately! Do nothing else prior to contacting Central Operations. Do NOT contact the client! We repeat, do NOT contact the client"

* * *

Greg stared in disbelief at the screen, not quite sure what to make of what had just happened. Both of the buttons had turned a shade of gray and become inactive. Greg thought about asking one of the other workers as he could hear the monotonous clicking coming from the cubes on either side of him, but he thought better of it. He didn't really know them

and he didn't really want to. He then picked up the phone fully intending to contact Mr. Goethe and inform him of this most unexpected of situations. His fingers hovered over the keypad as he paused to think.

'If I call him before I call this Central Operations, he might yell at me for waiting.'

Greg found himself dialing the number for Central Operations.

"Central Operations, may I help you?" The voice of a calm and self assured woman came across the phone, the sound seeming extremely loud in Greg's ears.

Greg winced inwardly as he realized this was the first real sound he had heard in over five hours.

"Uh, yeah, I work for SecureMore and I just got a message on my screen to call you." Greg's voice sounded idiotic, even to himself.

"Yes, of course, please stay on the line and do not hang up, we will be with you momentarily."

Greg swallowed.

Greg sat.

Greg waited.

Chapter 4

Deputy Director Sands felt the tell tale buzzing on his hip indicating that his presence was requested. A non-descript man of non descript height and wearing a bland suit, Virgil Sands glanced down at his waist to see who had contacted him. Leaving his office through the glass door, Deputy Director Sands stepped out onto the elevated walkway which overlooked the Central Operations floor located five stories below a small business complex in West Falls, Virginia. A quiet hum of activity ran throughout the facility. Soft lights from a vaulted ceiling illuminated the 50 or so employees working diligently at rows of workstations all oriented towards the far wall. Upon this wall were mounted a number of large screen monitors displaying all manner of data to be interpreted, understood, and incorporated into the ethereal world of intelligence. The scene resembled nothing so much as mission control for NASA or the set of the movie War Games. Although conversations were being held everywhere around the room, none of them could be heard. From multiple locations, white noise generators were constantly emitting the signals that would cause a conversation not five feet away to be rendered all but inaudible.

* * *

Sands made his way down the stairs and onto the operations floor where he immediately set out for terminal #28 from which the analyst responsible for his visit had sent the request.

"Analyst, what is it."

Sands very rarely, if ever used names while at work, often preferring to address personnel by job function or title. In his estimation, it provided for a sense of professionalism and reduced the amount of feeling or familiarity that could cause complications in his line of work. The analyst, one Laura Helmford by name and wearing the company issue bland suit addressed her superior with confidence.

"Sir, we just received a hit from SecureMore Consulting. They're a small Managed Security Services company operating in Bloomington, Minnesota. They review logs for a number of companies including some of internal interest."

"Let me see it."

On her screen, Agent Helmsford brought up a record of the log entries that had triggered the alert, along with other information pertaining to the incident.

"Did you want me to bring it up on the big screen?"

"No. Do not. Proceed to Operational Closet #2, code 2451. We'll take care of this there."

* * *

Analyst Helmford immediately blanked and locked her screen, stood up, and strode purposefully off of the operations floor heading for a series of small rooms along the south wall. Grabbing the comset from his hip, Sands paged a technical resource who came running up moments later.

"Get me everything you have on our assets monitored by SecureMore Consulting. I want everything: remote access, control; the works! Bring it to Closet #2 ASAP!"

Sands strode to the south wall and approached a door labeled "Operational Closet #2". He entered the code 2451 into the small keypad located next to door and upon hearing a click, entered the room where Laura was logging into the terminal.

Operational Closet #2 was really no more than that, a closet. There was a small table with four chairs, a single terminal and a lone light bulb flickering above them. Responding to a small tap on the door, Sands glanced at the video screen set into the wall. Seeing the tech he had dispatched, he opened the door, took the proffered folder, wordlessly shutting the door in the poor technician’s face. Laura took the folder from Sands, laid it on the table and flipped it open. Glancing at it occasionally, she began rapidly typing as Sands picked up the phone.

"What's your name son?"

"Greg Holland sir."

"Greg, I need you to listen to me very carefully, you are going to discard this entry and forget that you ever saw it appear on your screen." Sands nodded to Laura who tapped the enter key on her keyboard.

As if by magic the alert message on Greg Holland's screen blinked out of existence and both of the buttons on his display activated again, the grayish hue of suppression being replaced by the vivid blue of normal operations.

"I don't know if I can do that sir."

"Of course you can son. You have to."

"I really should contact my supervisor, maybe you can talk to him and he can help you."

Helmsford hurriedly pointed to a particular piece of information on her screen.

"That won't be necessary Greg, Mr. Goethe will not learn of this and you will be able to go about your business." An emphasis had appeared on the use of the words 'will not' transforming it from a simple statement of fact to a virtual command.

"I'm not sure about this sir"

While this conversation had been going on Analyst Helmsford had brought up a remote Virtual Network Connection or VNC window which linked her computer to the keyboard, video, and mouse of Greg's workstation allowing them to not only see what was happening on his computer, but remotely control it as well.

"Sure you can son." Sands reached down and moved the mouse on Laura's computer causing the cursor on Greg's screen to glide over to the large 'Discard' button. He took his hand off of the mouse, leaving the cursor to hover there expectantly.

There was a sharp intake of breath on the other end of the line as Greg realized his mouse had moved without him touching it. Sands could just picture him glancing nervously over his shoulder to see if anyone was there.

"Sir?"

"I need you to discard this log entry Greg. Discard it and pretend you never saw it in the first place. Do you understand?"

"Yes sir."

Greg clicked on the discard button and the next log entry, a

simple service start message, popped up on his screen.

"Greg?"

"Yes sir?"

"You can hang up the phone now, and remember, we never had this conversation."

"yes sir."

After Deputy Director Sands had hung up the phone, Laura Helmsford turned to her boss, her expression confused.

"Why didn't you just click on the discard button for him sir?"

"Because I needed 'him' to do it analyst, that's why. By actively clicking on the discard button, he has made himself complicit through which we can safely assume he will abide by the secrecy he agreed to. While it is true no one would believe him, this is safer and cleaner. Now show me that log message again."

After reviewing the initial log message as well as a number of other messages Helmsford pulled up for him, Sands took a deep breath. He was visibly struggling to keep the frustration and anger from his voice.

"We need to find out who this Nicholas Edgewood is, but first things first. We have to cut this guy's access to the

system!"