Is This a Circle?
The Call is Coming from Inside the House
How Do You Run Your SOC When Attackers Are On-Site?

Deviant Ollam
SANS SOC Summit – 2019-06-25
My Team and I Enjoy Our Work
My Team and I Enjoy Our Work
My Team and I Enjoy Our Work
But The Blue Team Doesn’t Always Enjoy Our Work
The Kinds of Threats For Which SOC Teams Plan
LinkedIn

REMINDERS
Invitation reminders:
From (Your employee)

PENDING EVENTS
There are a total of 3 notes awaiting your response. Visit your InBox by clicking here.

Don't wish to obtain email information? Change your auto-informers settings.

LinkedIn respect your privacy. Not once has LinkedIn made your e-mail address acceptable to any third-party LinkedIn member without your allowance. 2013, LinkedIn Corporation.
Data Exfiltration

http://redteamalliance.com
The Kind of Threat that Takes SOC Teams by Surprise
On-Site Entry
On-Site Entry
On-Site Entry
Attacker Preparation
Portable Badge Printer
Who Do You Need to Be?

COMCAST
RAYMOND JONES

ADP
Raymond K. Jones
Field Tech No. 377429

Johnson Controls
Raymond K. Jones
Inspector No. 377429

OTIS

Time Warner Cable
RAYMOND K. JONES

comcast
RAYMOND JONES

Raymond Jones

verizon

Tyco
Raymond Jones

http://redteamalliance.com
Who Do You Need to Be?
Vehicle-Based Surveillance

http://redteamalliance.com
Vehicle-Based Surveillance
Vehicle-Based Surveillance

eBay > Home & Garden > Home Décor > Decals, Stickers & Vinyl Art

Uber Trade Dress, Placard 5.5"x7.5" car display sign

$5.75
+$3.25 Shipping

Get it by Monday, Mar 25 from Gardena, California

- New other (see details) condition
- 30 day returns - Buyer pays return shipping

“A brand-new, unused item (including handmade items)
Uber Trade Dress, Placard. Size: 5.5"x7.5". Suction cup attached on top of the card. Easy to place on and off between
Read full description
See details
Street-Based Surveillance
Street-Based Surveillance
Surveillance at a Greater Distance
Long Range Surveillance Can Be... Costly
Long Range Surveillance Can Be... Amazing
Open Field Surveillance
Open Field Surveillance
Open Field Surveillance
Open Field Surveillance
Spot the Field Operative
Spot the Field Operative
Spot the Field Operative
Spot the Field Operative
Spot the Field Operative

http://redteamalliance.com
Don’t Feel Bad... They Couldn’t See Us, Either
Story Number One: “The Problem Solver”
Outside Consultant
“Well, These Cameras Don’t Work”
“This Lock Fell Apart Last Week”
“This Lock Fell Apart Last Week”
“I’m Pretty Sure That’s Not to Code”
“This Hallway is a Bad Blind Spot”
“Especially with this Rear Entrance”

Enter Code 2182
Push handle down
Then lift handle up to open.
Will be fixed on Monday
“Thank You So Much for Listening and Helping!”
“Wait a Minute ... That Wasn’t the Usual Password Inspector.”
Story Number Two: “Endless Alarms”
Alarmed Server Room Doors
Alarmed Server Room Doors
Alarmed Server Room Doors
Alarmed Server Room Doors

Equipment Issue

Door inoperable

Possible burned up control board

Work Order # 598795
Date 7/9/2017
Employee Facility
Alarmed Server Room Doors
Alarmed Server Room Doors
Alert Chaining at the Perimeter
Story Number Three: “Say Again? Did Not Copy Your Last.”
Inside Their Office
Then, Inside a Security Office
Intel Gathering
Disinformation
Hot Mic / Suppression
Two Stolen Radios Enabled Complete Mayhem
Story Number Four: Keeping Doors in Good Order
Remember Field Surveillance?
Often, Important Facilities Have a Lot of Construction
Often, Important Facilities Have a Lot of Construction
Observation of Vehicle Checkpoint
Vehicle-Based Entry
Time to Service the Doors
Our Point of Contact in the SOC Noticed
“Go Louder” Came the Instruction
“Go Louder” Came the Instruction
“Go Louder” Came the Instruction
That Got Their Attention
What Do You Think The Guards Did?
We Checked In with our Point of Contact

Two guards just confronted us in building 6.

And what happened? Are we terminating the test? Did they stop you?

Not exactly.

Huh?

We told them we were working on the doors. They just left. Any chatter in the SOC?

Standby...

Nope. Proceed.

In fact, go louder.
Then I Took a Golf Cart
Then I Took a Bike
The Guards Clearly Wanted Me to Stop
The Guards Became Very Distracted
To Make the SOC’s Job Easier
1. Cameras
Network Bandwidth
Name Your Cameras Properly

Hello
my name is
Building 4
East Side

Hello
my name is
IDF Closet
5th Floor

Hello
my name is
Vehicle
Checkpoint
Position Your Cameras Properly
Automatic Focus & Tracking, Triggered By Alerts
What’s This?
2. Comms

![Fisher-Price Kid Tough Walkie Talkies](http://redteamalliance.com)
“Can You Hear Me Now?”
Too Many Voices
Different Roles
3. Culture
Missing Locks Should Be Reported
Missing Locks Should Be Reported
Missing Locks Should Be Reported
Perhaps the **Biggest** Benefit Toward Which You Can Strive...
Fight Fatigue
<table>
<thead>
<tr>
<th>Event Description</th>
<th>Time</th>
<th>Date</th>
<th>ID Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Door Command Issued - Door Used</td>
<td>4:20 PM</td>
<td>6/21/2018</td>
<td>IDF-5-LNL-2000</td>
</tr>
<tr>
<td>Relay Contact Activated</td>
<td>4:20 PM</td>
<td>6/21/2018</td>
<td>EP-1502-42A</td>
</tr>
<tr>
<td>Relay Contact Deactivated</td>
<td>4:20 PM</td>
<td>6/21/2018</td>
<td>EP-1502-42A</td>
</tr>
<tr>
<td>DHO Door 21-J</td>
<td>4:21 PM</td>
<td>6/21/2018</td>
<td>IDF-6-LNL-1000</td>
</tr>
<tr>
<td>DFO Door 45-A</td>
<td>4:22 PM</td>
<td>6/21/2018</td>
<td>IDF-3-LNL-2100</td>
</tr>
<tr>
<td>Unlock Mode Disabled</td>
<td>4:23 PM</td>
<td>6/21/2018</td>
<td>none</td>
</tr>
<tr>
<td>DHO Door 21-J</td>
<td>4:25 PM</td>
<td>6/21/2018</td>
<td>IDF-6-LNL-1000</td>
</tr>
<tr>
<td>Biometric Mismatch</td>
<td>4:26 PM</td>
<td>6/21/2018</td>
<td>IDF-5-LNL-1000</td>
</tr>
<tr>
<td>DHO Door 21-J</td>
<td>4:32 PM</td>
<td>6/21/2018</td>
<td>IDF-6-LNL-1000</td>
</tr>
<tr>
<td>DFO Door 45-A</td>
<td>4:37 PM</td>
<td>6/21/2018</td>
<td>IDF-3-LNL-2100</td>
</tr>
<tr>
<td>DHO Door 21-J</td>
<td>4:42 PM</td>
<td>6/21/2018</td>
<td>IDF-6-LNL-1000</td>
</tr>
<tr>
<td>DFO Door 45-A</td>
<td>4:51 PM</td>
<td>6/21/2018</td>
<td>IDF-3-LNL-2100</td>
</tr>
<tr>
<td>Open Door Command Issued - Door Used</td>
<td>5:02 PM</td>
<td>6/21/2018</td>
<td>IDF-5-LNL-2000</td>
</tr>
<tr>
<td>DFO Door 45-A</td>
<td>5:14 PM</td>
<td>6/21/2018</td>
<td>IDF-3-LNL-2100</td>
</tr>
<tr>
<td>DFO Door 45-A</td>
<td>5:34 PM</td>
<td>6/21/2018</td>
<td>IDF-3-LNL-2100</td>
</tr>
<tr>
<td>Open Door Command Issued - Door Unused</td>
<td>5:49 PM</td>
<td>6/21/2018</td>
<td>IDF-5-LNL-3400</td>
</tr>
<tr>
<td>DFO Door 45-A</td>
<td>5:53 PM</td>
<td>6/21/2018</td>
<td>IDF-3-LNL-2100</td>
</tr>
<tr>
<td>Open Door Command Issued - Door Used</td>
<td>5:59 PM</td>
<td>6/21/2018</td>
<td>IDF-5-LNL-2000</td>
</tr>
<tr>
<td>Event Description</td>
<td>Time</td>
<td>Date</td>
<td>ID/Location</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Open Door Command Issued - Door Used</td>
<td>4:20 PM</td>
<td>6/21/2018</td>
<td>IDF-5-LNL-2000</td>
</tr>
<tr>
<td>Relay Contact Activated</td>
<td>4:20 PM</td>
<td>6/21/2018</td>
<td>EP-1502-42A</td>
</tr>
<tr>
<td>Relay Contact Deactivated</td>
<td>4:20 PM</td>
<td>6/21/2018</td>
<td>EP-1502-42A</td>
</tr>
<tr>
<td>DHO Door 21-J</td>
<td>4:21 PM</td>
<td>6/21/2018</td>
<td>IDF-6-LNL-1000</td>
</tr>
<tr>
<td>DFO Door 45-A</td>
<td>4:22 PM</td>
<td>6/21/2018</td>
<td>IDF-3-LNL-2100</td>
</tr>
<tr>
<td>Unlock Mode Disabled</td>
<td>4:23 PM</td>
<td>6/21/2018</td>
<td>none</td>
</tr>
<tr>
<td>DHO Door 21-J</td>
<td>4:25 PM</td>
<td>6/21/2018</td>
<td>IDF-6-LNL-1000</td>
</tr>
<tr>
<td><strong>Biometric Mismatch</strong></td>
<td><strong>4:26 PM</strong></td>
<td>6/21/2018</td>
<td><strong>IDF-5-LNL-1000</strong></td>
</tr>
<tr>
<td>DHO Door 21-J</td>
<td>4:32 PM</td>
<td>6/21/2018</td>
<td>IDF-6-LNL-1000</td>
</tr>
<tr>
<td>DFO Door 45-A</td>
<td>4:37 PM</td>
<td>6/21/2018</td>
<td>IDF-3-LNL-2100</td>
</tr>
<tr>
<td>DHO Door 21-J</td>
<td>4:42 PM</td>
<td>6/21/2018</td>
<td>IDF-6-LNL-1000</td>
</tr>
<tr>
<td>DFO Door 45-A</td>
<td>4:51 PM</td>
<td>6/21/2018</td>
<td>IDF-3-LNL-2100</td>
</tr>
<tr>
<td>Open Door Command Issued - Door Used</td>
<td>5:02 PM</td>
<td>6/21/2018</td>
<td>IDF-5-LNL-2000</td>
</tr>
<tr>
<td>DFO Door 45-A</td>
<td>5:14 PM</td>
<td>6/21/2018</td>
<td>IDF-3-LNL-2100</td>
</tr>
<tr>
<td>DFO Door 45-A</td>
<td>5:34 PM</td>
<td>6/21/2018</td>
<td>IDF-3-LNL-2100</td>
</tr>
<tr>
<td><strong>Open Door Command Issued - Door Unused</strong></td>
<td><strong>5:49 PM</strong></td>
<td>6/21/2018</td>
<td><strong>IDF-5-LNL-3400</strong></td>
</tr>
<tr>
<td>DFO Door 45-A</td>
<td>5:53 PM</td>
<td>6/21/2018</td>
<td>IDF-3-LNL-2100</td>
</tr>
<tr>
<td>Open Door Command Issued - Door Used</td>
<td>5:59 PM</td>
<td>6/21/2018</td>
<td>IDF-5-LNL-2000</td>
</tr>
</tbody>
</table>
Fight Fatigue
Fight Fatigue
And Don’t Be Afraid to Call-In and Report Strange Things!
Thank You Very Much!