

White Hacker Cloud Security Fundamentals

[Date] – Day 7

[Trainer]





hello



About our last session



Today's agenda



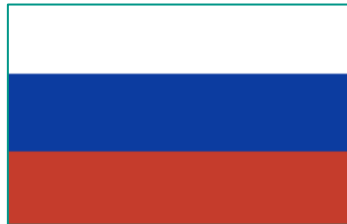
What are we going to learn today ?

Logging & Monitoring

- Finalization for all: help each other

Monitoring & Logs analysis

- Log reporting to Azure log analytics
- Run custom actions on event





[Name]' team





Briefing time

Your challenge

Monitoring & Logs analysis

*Report and share
vocabulary words not understood & the sources used*

- Many accounts of Becloud have been hacked recently
- Your mission will be to automate the following actions on each risky sign-ins, or when a user is flagged as risky and to setup rules avoiding logins from China and Russia since none of our employees are working in these countries.
 1. Reset password to a secure one
 2. Kill all active sessions
 3. Enable MFA
 4. Produce an audit log of the actions that the user took

At the end of this challenge you should be able to

- I. log reporting to Azure log analytics
- II. run custom actions on event



Your challenge

Monitoring & Logs analysis







**Did you enjoy
your lunch ?**



be The Dilbert of the day



Dilbert.com DilbertCartoonist@gmail.com



5-25-12 © 2012 Scott Adams, Inc. / Dist. by Universal Uclick



be
≤/

**After Steve last
week...**

**the Cloud vision
of Intel in...
2010**

3 min 11 sec



<https://www.youtube.com/watch?v=gpzM6Mask80>



9 AM



2PM





**Sorry in advance
for those who
missed
9 AM or 2 PM
photo, we had to
find a
“substitute” ;-)**



Let's go...

9 AM



2 PM



9 AM



2 PM



9 AM



2 PM



9 AM



2 PM



9 AM



2 PM



9 AM



2 PM



9 AM



2 PM



9 AM

2 PM



9 AM

2 PM



9 AM

2 PM



**Last but
not least...
your
today's coach**

9 AM



2 PM



The agenda of our next session

```
ay}}}},{key:"backspace",value:function(t,e){var s=this;if(
is.toggleBlinking(!1);var n=this.humanizer(this.backSpeed);
smartBackspace){var i=s.strings[s.arrayPos+1];i&&n===i.subs
s.strings.length?(s.arrayPos=0,s.options.onLastStringBacksp
complete",value:function(){this.options.onComplete(this),thi
=s,this.pause.curString=t,this.pause.curStrPos=e}},{key:"to
ng=t;var e=t?"infinite":0;this.cursor.style.animationIterat
gsIfNeeded",value:function(){this.shuffle&&(this.sequence=t
this;return this.el.className+=" "+this.fadeOutClass,this.c
length>t.arrayPos?t.typewrite(t.strings[t.sequence[t.arrayP
.attr?this.el.setAttribute(this.attr,t):this.isInput?this.el
}},{key:"bindFocusEvents",value:function(){var t=this;this.i
e){t.el.value&&0!==t.el.value.length||t.start()}}),{key:"i
"),this.cursor.className="typed-cursor",this.cursor.innerHTML
})();e["default"]=a,t.exports=e["default"]},function(t,e,s){
Error("Cannot call a class as a function")}Object.defineProperty
ts[e];for(var n in s)Object.prototype.hasOwnProperty.call(s,
.enumerable||!1,n.configurable=!0,"value"in n&&(n.writable=
n(a),l=function(t){i(this,t)}return o(t,[{key:"
ut="input"===t.el.tagName.toLowerCase(),t.attr=t.opt
t.startDelay=t.options.cursorChar,t.cursorBlinking=10,t
t.startDelay=t.options.startDelay,t.fadeOutClass,t.
ns.stringsElem
```

What are we going to learn in the next session ?

Monitoring & Logs analysis

- Log reporting to Azure log analytics
- Run custom actions on event

Module 3 Security & Operations

VPN

- Create a Point to Point VPN
- Create a site to site VPN



CERRADO

y por nosotros estaría siempre abierto

De V