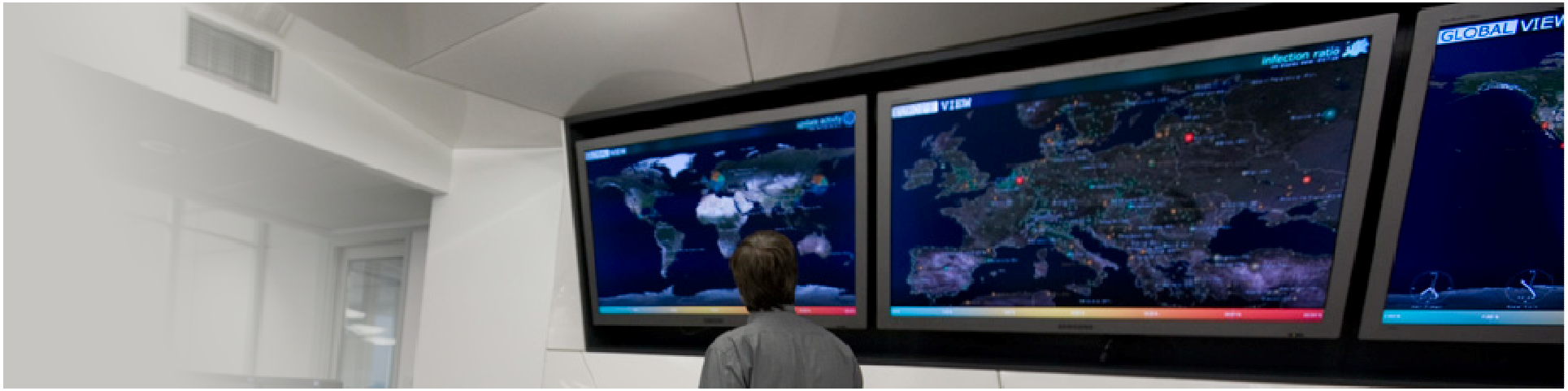


Čo robí ESET

Peter Košinár
kosinar@eset.sk

Čo u nás človek občas robí

Hasiča – hasí vzniknuté problémy.

Krotiteľa duchov – hľadá neexistujúce problémy.

Právnika – to je samostatná kapitola...

Nočníka – veci majú občas veľmi rýchly spád.

S čím sa stretávame každý deň

Detailná analýza nemožná (a často nepotrebná)

Rýchly vývoj situácie – čas, ľudské zdroje.

Priority, plánovanie času, zdrojov.

Externé vplyvy, „DoS“ od spoluhráčov.

S čím sa stretávame každý deň

300 tisíc unikátnych súborov každý deň z vlastných zdrojov.

Cudzie zdroje - exponenciálny nárast objemu dát (3x), momentálne 8TB ročne.

Ukladanie, spracovávanie, rozhodovanie...

Automatizácia sa robí ťažko.

S čím sa stretávame každý deň

Dobro vs. Zlo = sémantický problém.

window.gbar={};(function(){function g(a,b,e){var c="on"+b; if(a.addEventListener)a.addEventListener(b,e,false);
else if(a.attachEvent)a.attachEvent(c,e);else{var f=a[c];a[c]=function(){var i=f.apply(this,arguments),
d=e.apply(this,arguments);return i==undefined?d:d==undefined?i:d&&i}};var j=window.gbar,k,l,m;function
n(a){m=a}function o(a){var b=m&&window.encodeURIComponent&&encodeURIComponent(m());if(b)
a.href=a.href.replace(/([?&]continue=)[^&]*/,"$1"+b)}function p(a){if(window.gApplication)a.href=
window.gApplication.getTabUrl(a.href)}j.qs=p;j.setContinueCb=n;j.pc=o;function q(a,b,e,c,f,i){var
d=document.getElementById(a),h=d.style;if(d){h.left=c?"auto":b+"px";h.right=c?b+"px":"auto";h.top=e+"px";
h.visibility=l?"hidden":"visible";if(f){h.width=f+"px";h.height=i+"px"}else{q(k,b,e,c,d.offsetWidth,d.offsetHeight);l=
l?"":a}}}j.tg=function(a){a=a||window.event;var b=a.target||a.srcElement;a.cancelBubble=true;
if(!k){a=document.createElement(Array.every||window.createPopup?"iframe":"div");a.frameBorder="0";a.src="j
avascript:"";k=b.parentNode.appendChild(a).id="gbs";g(document,"click",j.close);if(j.alld){j.alld(function(){r(b)});r
eturn}}r(b)};function r(a){var b=0,e,c=window.navExtra;if(a.className!="gb3")a=a.parentNode;var
f=a.getAttribute("aria-owns")||"gbi",i=a.offsetWidth,d=a.offsetTop>20?46:24,h;do
b+=a.offsetLeft||0;while(a=a.offsetParent);if(f=="gbi")for(a=document.getElementById(f);c&&(e=c.pop());)a.inse
rtBefore(e,a.firstChild).className="gb2";else h=b=(document.documentElement.clientWidth||
document.body.clientWidth)-b-i;l!=f&&j.close();q(f,b,d,h)}j.close=function(){l&&q(l,0,0)}})();function e(id){return
document.getElementById(id)}function v(id){return e(id).value}function vs(id,val){e(id).value=val}function
d0(id){e(id).style.display="none"}function d1(id){e(id).style.display=""}function u(v){return typeof
v=="undefined"}

Moderné technológie – zlé i dobré

Generovanie kódu za behu – Javascript, VBscript konštrukcie typu eval().

Facebook, Myspace, Twitter - nové zraniteľnosti

Unicode konštrukcie (vizuálna podobnosť)

IDN - http://пример.испытание

Vzdelávanie a právo zaostáva.

Čo dá človeku škola

Kódovanie – šifrovanie, pakovanie

Algoritmy – triedenie, vyhľadávanie

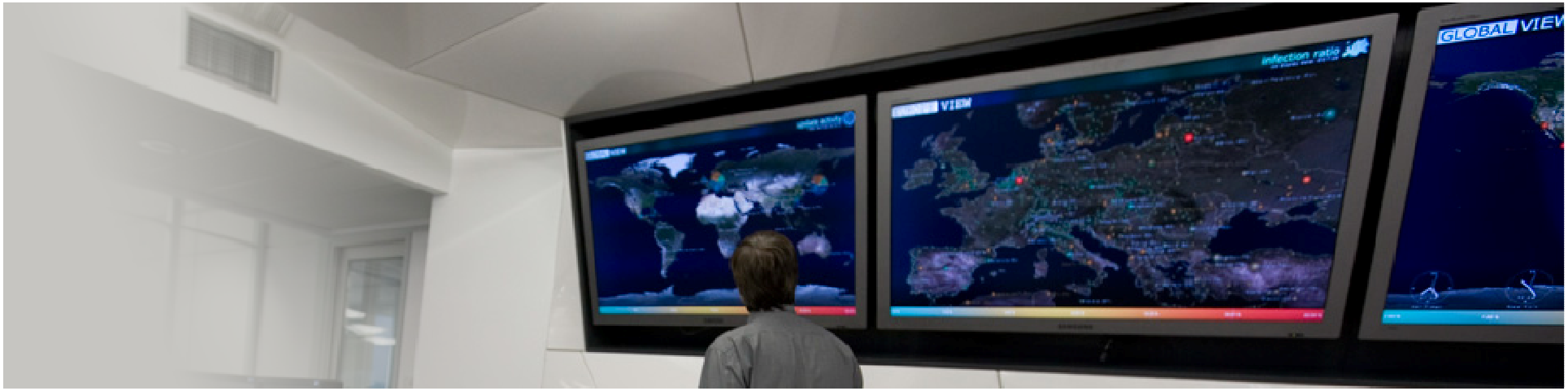
Štatistika – spracovávanie dát, odhady

Čo človeku škola NEdá

Systémko – reverzné inžinierstvo

Strednoúrovňové záležiosti - <OS> internals

Nízka úroveň – cache, GPU, siete



Otázky?

Peter Košinár <kosinar@eset.sk>