Hunting the Bad Guys: Approaches to Threat Detection

Peter Glock, Managing Director EMEA



Before we start...



"When a meeting, or part thereof, is held under the **Chatham House Rule**, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."



5 questions to ask before we get to 'threat detection'





Contents

- An exercise in trust and risk
- What do I want to protect?
- Defining and discovering assets
- Threats, risks and security controls
- Smoke alarms for security and privacy



Who and what do you trust?



Rīgas konference 2018 norisināsies Latvijas Nacionālajā bibliotēkā, 28.- 29. septembrī, apvienojot gandrīz 800 dalībniekus no visas pasaules. Latvijas Transatlantiskās Organizācijas rikotā konference, sadarbībā ar Latvijas Republikas Ārlietu ministriju, un Latvijas Republikas Azsardzības ministriju, ir viedojusi ārlietu politikas debašu ietvaru Baltijas jūras reģionā kopš 2006. gada.

riga-airport.com/en





Demonstration – wireless insecurity





What do you want to protect?



Information Assets



Jim Schwar @jimiDFIR

Following

 \sim

Replying to @MalwareJake

CISO: How many windows hosts do we have? AV Guy: 7864 Desktop Management: 6321 EDR Team: 6722 CMDB Team: 4848 SIEM Team: 9342

5:55 AM - 8 Feb 2018



And what about?:

- Client data
- Personnel files
- Supply chain details

02

Demonstration – unsexy asset management





Threats, risks, security controls



The Process in a Nutshell





Architecture and Integration Role Based Access ThreatModeler External Tools Executive RealTime Dashboard/ Threat CISO/CIO/VP Top 10 Threats Intelligence Threat BugTracking IT Risk & Console Security 0 Security Policy Single Sign On **DeveloperIDE** Configuration Compliance Policies IT Security **ThreatModeler** New Application + Secure Security Enhancements SDLC Requirements/ Application Abuse Cases Inventory/ Architects Change Mgmt Secure Coding Secure Code Policies Snippets/ GRC Developers Abuse Cases Threat Metadata

hreatModeler Security Starts Here Source: ThreatModeler

4

Demonstration – VAST Threat Modelling





Smoke alarms

OCymmetria

A word about supply chains

Your data is spread throughout your supply chain

- Github
- Unprotected network shares (s3, DropBox...)
- Shadow IT

...and maybe by the bad guys

- Pastebin
- Dark Web

You need a 'smoke alarm' for the supply chain



Smoke Alarm – a breach of your own defenses

Leverage the fact attackers are predictable

// start with spearphishing, and
then ...

```
while ( !TargetFound )
```

/* compromise endpoint →
escalate privileges → recon
(mimikatz, net use, etc.) →
lateral movement */
}





Controlling the attackers

Attackers use **information they find in our networks** to make lateral movement and attack targets in the organization.

Deception feeds them **reallooking information** that causes them to follow a **defendercontrolled path**.

Once they hit a **deception target**, their *modus operandi* is exposed and their attacks are **detected and prevented**.



Threat Hunting - the surgical approach

Surgical approach – as opposed to "spray and pray"

- Better at catching attackers, including advanced attackers
- Lower friction with IT, as well as lower total cost (compared to other deception approaches)



Conclusion – detect threats throughout the SDLC

- It's much more efficient to build security controls and mitigate threats during development
- Test the effectiveness of your security controls at each step (Red Teams...)
- Don't trust your own controls, set up some smoke alarms for breaches



5 questions to ask





Next step?

Come talk to us!

