BVGROUP

The state of information security in universities

Harnessing the power of open-source CERT & research collaboration

Lt Cdr Kieren Nicolas Lovell RNorN RTD

Agenda

1. Introduction
2. Problem
3. Research Problem
4. OpenSource CERT
5. Future

Introduction

- HMS Vengeance TSSBN
- MCMV
- Royal Norwegian Navy Frigate Weapon
- SNMG1
- Head of CERT
  University of Cambridge
- Head of InfoSec - Pipedrive
  Pembroke College, Cambridge
  IR - Cranfield University
  COO - SensusQ

Problem

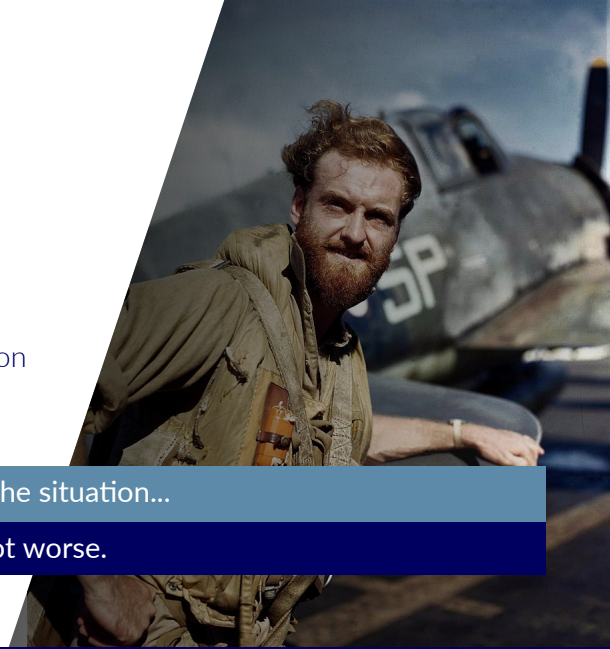
The problem is as old as time:

- Too much information
- Looking for a needle stack for hay...
- Cybersecurity "magic boxes" that fix all of your issues

Information

"We are drowning in information but starved for knowledge."[1]

- The technology jump from 1944 - 2021 is a giant leap
- It would be easy to assume information management has got better.



If anything, the situation...

...has got worse.

[1] John Naisbitt

Problem - Comparison

Operation	Overlord (1944)	Herrick (2014)
Personnel	250,000	10,000
Administrators	10,000	86,000
Bandwidth	50 baud	1.8 Mb
Average Speed of Comms	***15 minutes***	***8 - 12 hours***

Table: Communications speed and requirements comparison

Problem

So we are drowning in data, each team is in their Silo

- Risk
- Compliance
- Incident Response
- CISO
- Helpdesk
- Users

But a Threat Actor only needs to find a single weakness.... of which we have many.

Research Problem

Researchers more and more need access to large datasets to conduct research.

Conducting research on older datasets reduces the time for academics to see what is going on within the world.

Universities are amazingly unique

- Thousands of students that use as their home connection
- Academics focused purely on their task, and not always focused on security
- Finance and IT Operations areas that are more focused on security
- ... it is like a mini country.

Introducing the OpenSource CERT

First introduced at TalTech University

- OS SOAR/SIEM that scales (theHIVE, CorTex, ElasticStack)
- Cuckoo as a seperate VM conducting malware analytics on demand
- MISP (A Malware Intelligence Sharing Platform)
- Direct Sentinel connection into the feed available
- Able to process GCP, AWS, Azure logging
- Able to process SSO logs

But what about GDPR?

Good question:

- Recital 49 (GDPR processing is allowed as a CERT)
- Allow two ”Cores” of your CERT Team.
  - Primary CERT - Paid for employees of the University
  - Reserve CERT - Researchers that are like the Reserves
- Of course, you need a DPIA, and to talk to your DPO
- Removing PII is of course is important.

Benefits

We bridge the app between research and operational services

- Increased research capabilities for the University
- Works technically using Kubernates so it scales
- It is sooooooooo much cheaper
- No vendor lock-in

OpenCERT Expansion

You can also start to bring on
more proactive opensource tooling
to really increase your oversight.
For example, we will now go through
Spiderfoot

Spiderfoot

Spiderfoot is a platform that:

- Opensource
- Allows you to scan whole organisations and name-spaces so you can connect parts of your infra you didn't even know you've had
- Can run on a laptop or on a very small VM
- Lets have a look!

But most of all....

Research and operations need to bring the gap.
We should help each other.
But more importantly, we should change the way we work:

- SOC Manuals,
- Infrastructure documentation Diagrams
- Incident Response Plans,
- Threat Data
- Together we are stronger, we are weaker apart.

Need to Know

With a Responsibility to Share

Future

The fix, like it always has been, is not going to be security magic boxes. There are many tools, but it is how we use these tools - to process the vast amount of data we have to turn it into information... and in turn... make it **intelligence**.

- Use the knowledge and experience inhouse
- Be creative
- Reduce costs but increase ability to scale
- Reduce vendor lock-in
- Contribute to the Open Source Community
- Be the ”Moodle” of cybersecurity frameworks

Conclusion

If we use our resources internally,
if we break down our silos, and move
to a ”responsibility to share model”...

We can end up being one step behind hackers.
Which is a lot better than being ten
steps behind.

Thank you for listening!