
uni.lu
UNIVERSITÉ DU
LUXEMBOURG

From logging to next generation and new models of countermeasures

Threats, Attacks and Countermeasures

Master in Information System Security Management

Threat landscape

2021/2022

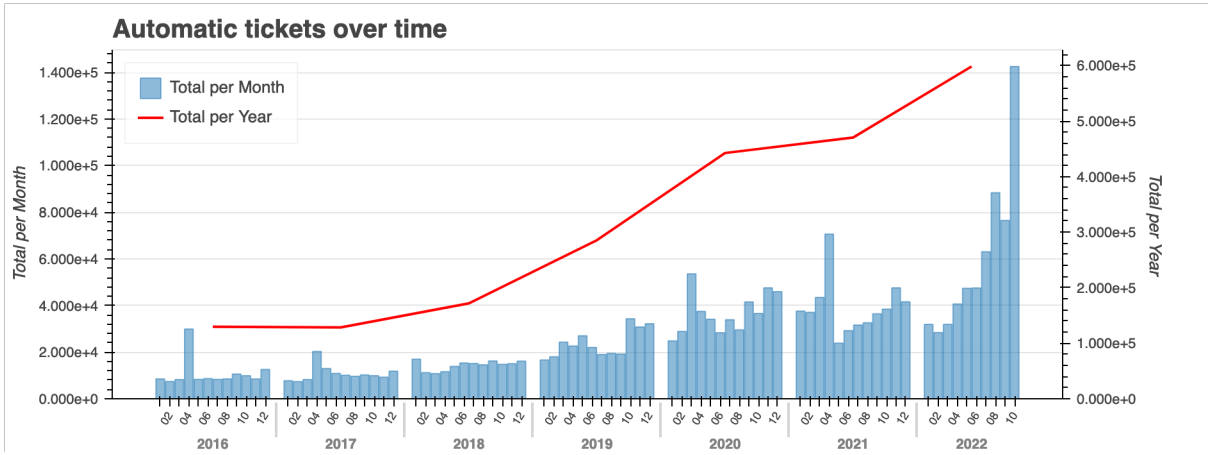
Luxembourg CyberWeather – Q1 2022

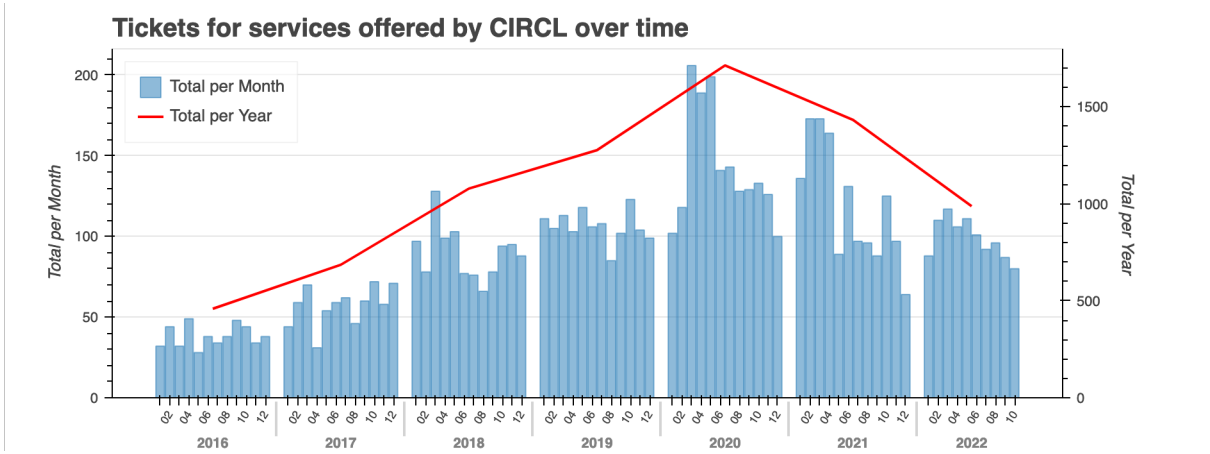
Category	Status
Malware	
Availability	
Phishing and scams	
Intrusions	
Vulnerabilities	
IoT	
eID	
APT	

Symbol used	Explanation
0 - 15% of teams indicating this type of incident	
16 - 50% of teams indicating this type of incident	
51 - 85% of teams indicating this type of incident	
86 - 100% of teams indicating this type of incident	

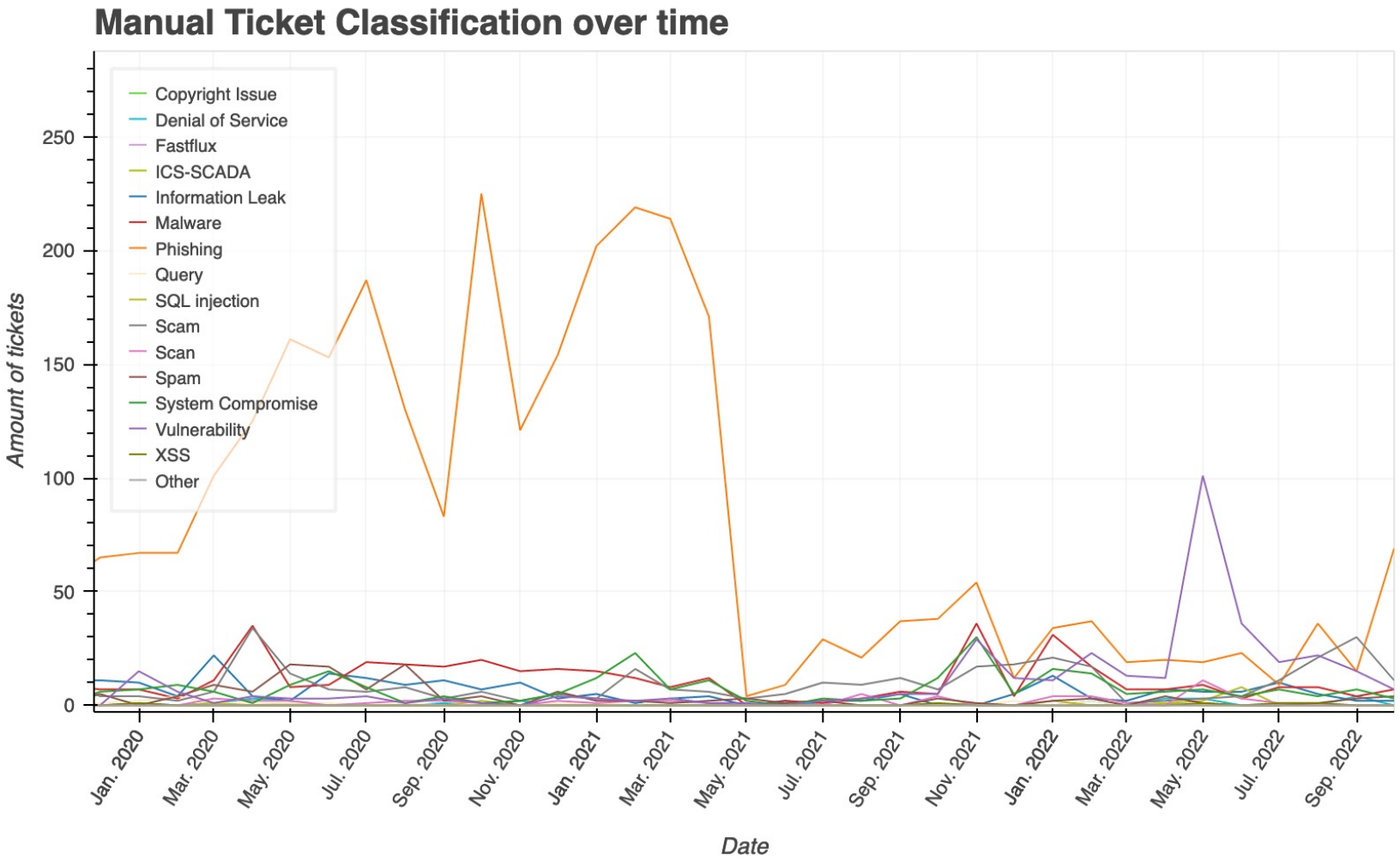
https://www.govcert.lu/en/cyberweather/

Luxembourg Operational statistics

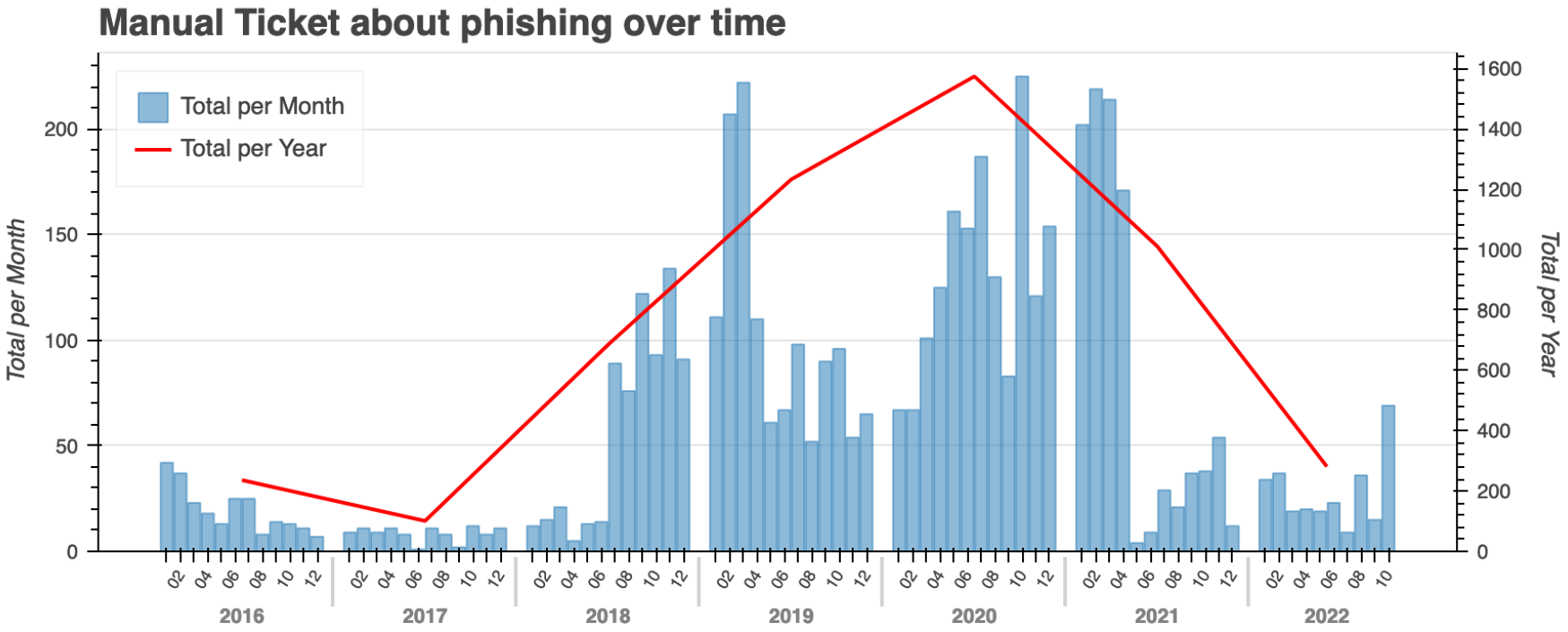




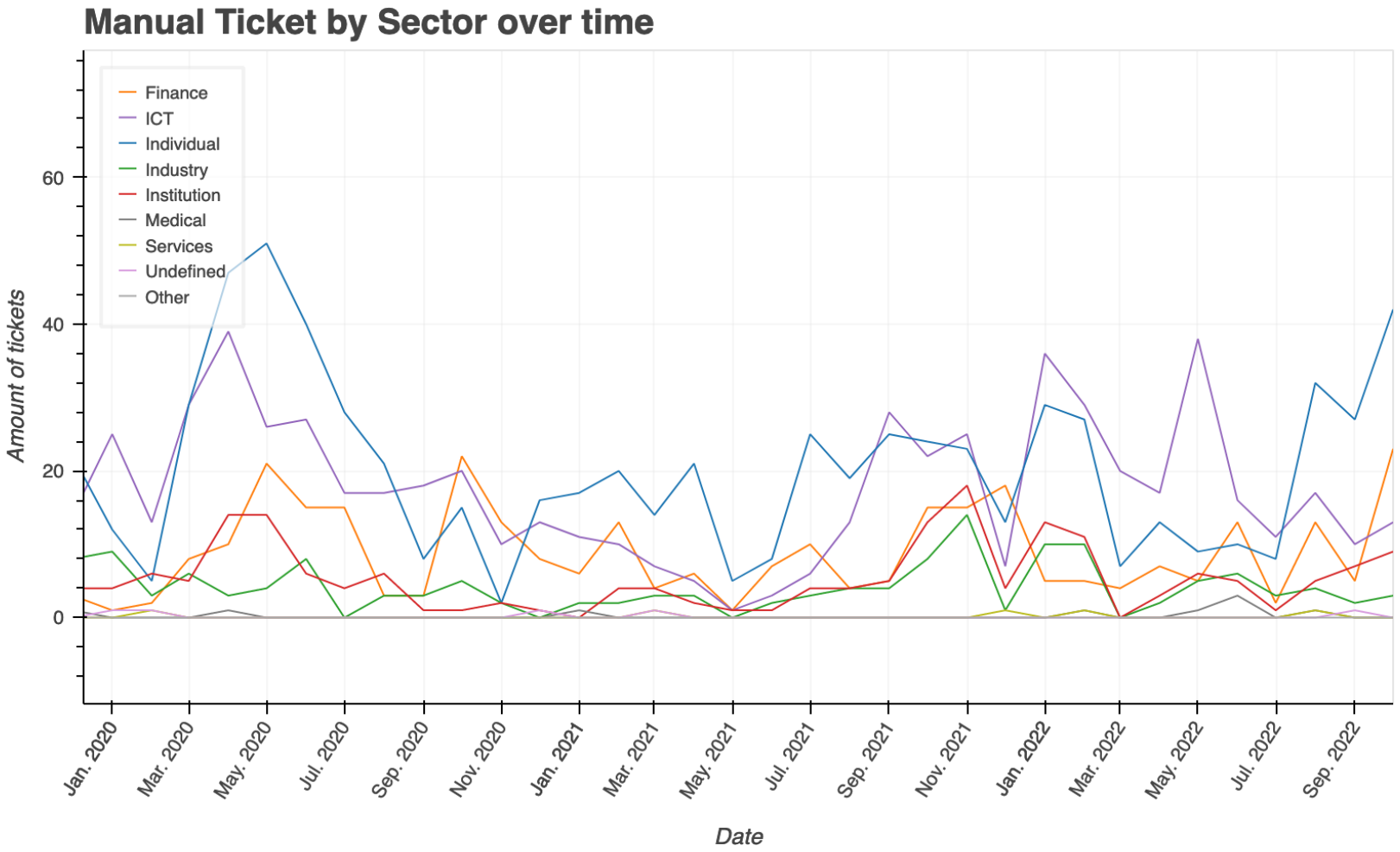
circl.lu


Manual Ticket Classification over time
Copyright Issue
Denial of Service
Fastflux
ICS-SCADA
Information Leak
Malware
Phishing
Query
SQL injection
Scam
Scan
Spam
System Compromise
Vulnerability
XSS
Other
Amount of tickets
0
50
100
150
200
250
Jan. 2020
Mar. 2020
May. 2020
Jul. 2020
Sep. 2020
Nov. 2020
Jan. 2021
Mar. 2021
May. 2021
Jul. 2021
Sep. 2021
Nov. 2021
Jan. 2022
Mar. 2022
May. 2022
Jul. 2022
Sep. 2022
Date

circl.lu


Manual Ticket about phishing over time
Total per Month
Total per Year
Total per Month
Total per Year
0
50
100
150
200
0
200
400
600
800
1000
1200
1400
1600
2016
2017
2018
2019
2020
2021
2022

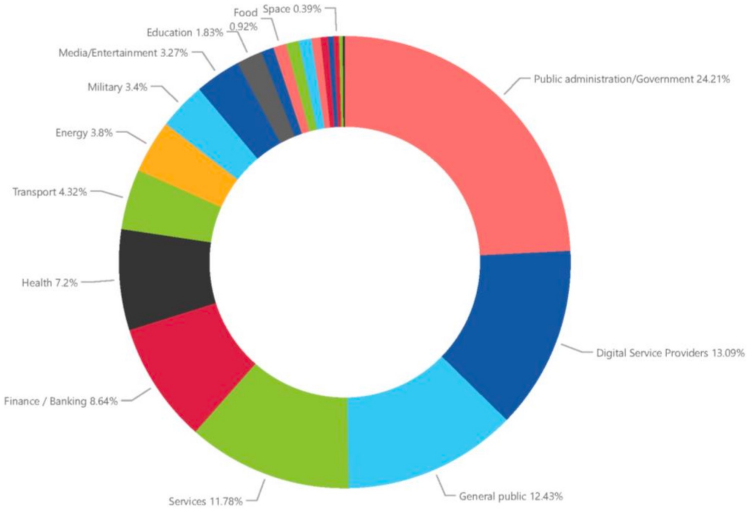
circl.lu



https://www.circl.lu/opendata/statistics/

circl.lu

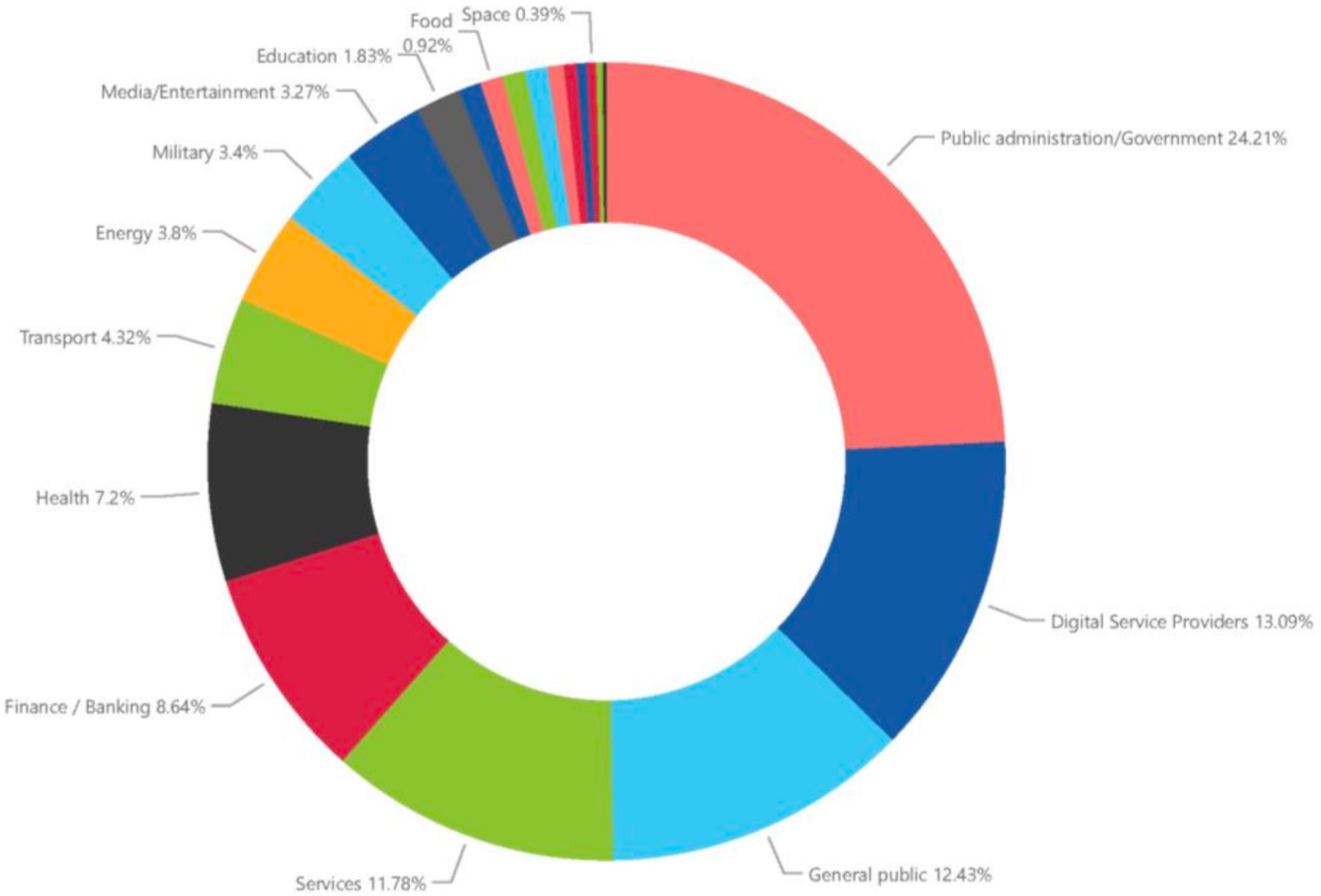
Europe
Top threats, majors trends



https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Figure 1: ENISA Threat Landscape 2022 - Prime threats

Figure 4: Targeted sectors per number of incidents (July 2021-June 2022)



Europe (main findings)

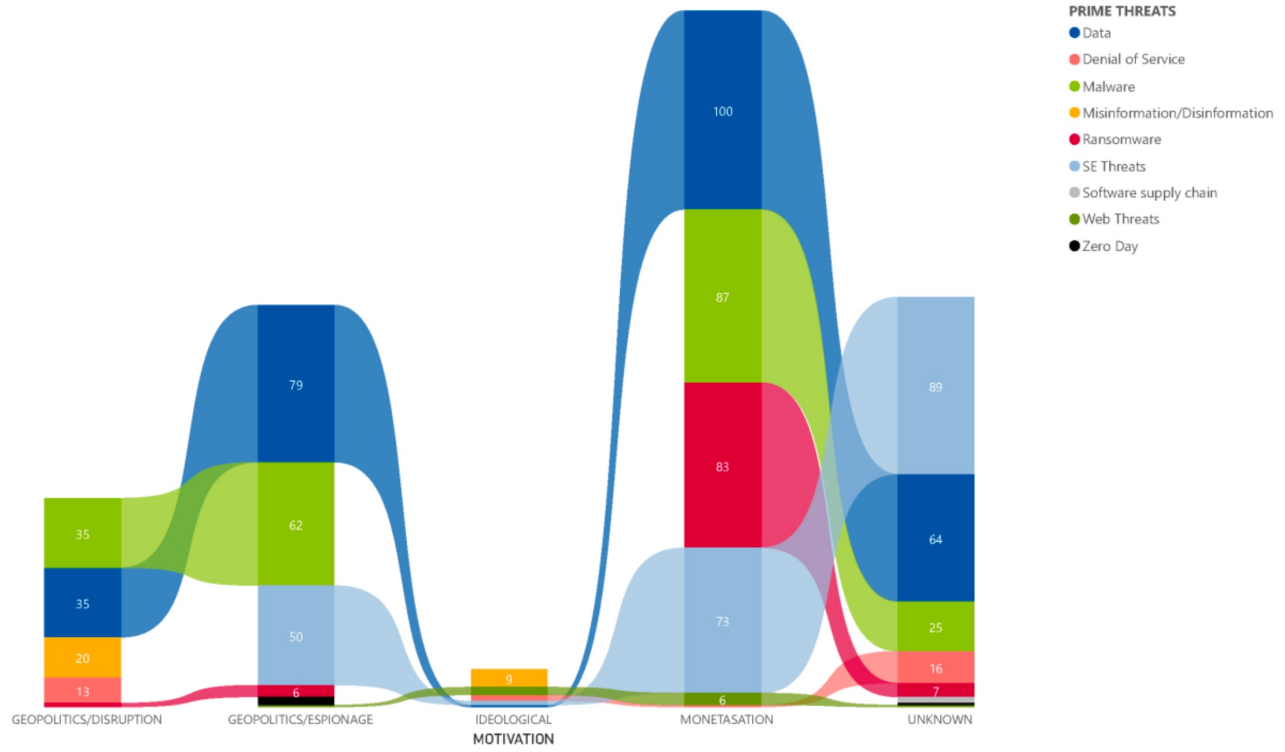
- **Ransomware and threats against availability rank at the top during the reporting period.**
- **Geopolitics continue to have strong impact on cyber operations.**
- **Destructive attacks are a prominent component of the operations of state actors.** During the Russia-Ukraine conflict, cyber actors were observed conducting operations in concert with kinetic military action20.
- **Continuous 'retirements' and the rebranding of ransomware groups** is being used to avoid law enforcement and sanctions.
- **Hacker-as-a-service business model** gaining traction, growing since 2021.
- **Significant rise on attacks against availability, particularly DDoS**, with the ongoing war being the main reason behind such attacks.
- **The Pegasus case triggered media coverage and governmental actions,** which also then was reflected in other cases concerning **surveillance and the targeting of civil society.**
- **A new wave of hacktivism21 has been observed** especially since the Russia-Ukraine crisis began.

Europe (main findings cont'd)

- **Phishing is once again the most common vector** for initial access. Advances in sophistication of phishing, user fatigue and targeted, context-based phishing have led to this rise.
- **Extortion techniques are further evolving** with the popular use of leak sites.
- **Malware is on the rise again** after the decrease that was noticed and linked to the COVID-19 pandemic.
- **Data compromise is increasing year on year.**
- **Machine Learning (ML) models** are at the core of modern distributed systems and are increasingly **becoming the target of attacks**.
- **DDoS are getting larger and more complex, are moving towards mobile networks and IoT and are being used in the context of cyberwarfare.**
- **State-owned Certificate Authorities (CA)** makes it easy to perform HTTPS traffic interception and man-in- the-middle attacks on its citizens thus putting internet security and privacy at risk.
- **Disinformation is a tool in cyberwarfare, including AI-enabled disinformation and deepfakes.** It was used even before the 'physical' war started as a preparatory activity for Russia's invasion of Ukraine.
- **Threat groups have an increased interest and exhibit an increasing capability in supply chain attacks and attacks against Managed Services Providers (MSPs).**

Europe (threat actors)

Figure 10 Motivation of threat actors per threat category



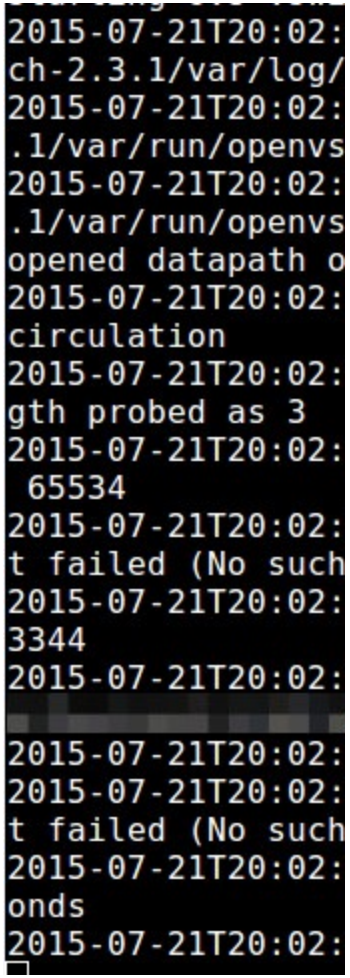
No data no defence

Log management
the good, the bad and the ugly

Security data is in the logs

- Log management generally covers:
  - Log collection
  - Log aggregation(ideally centralised)
  - Log storage and retention (long-term)
  - Log rotation
  - Log analysis (real-time or after storage)
  - Log search and reporting

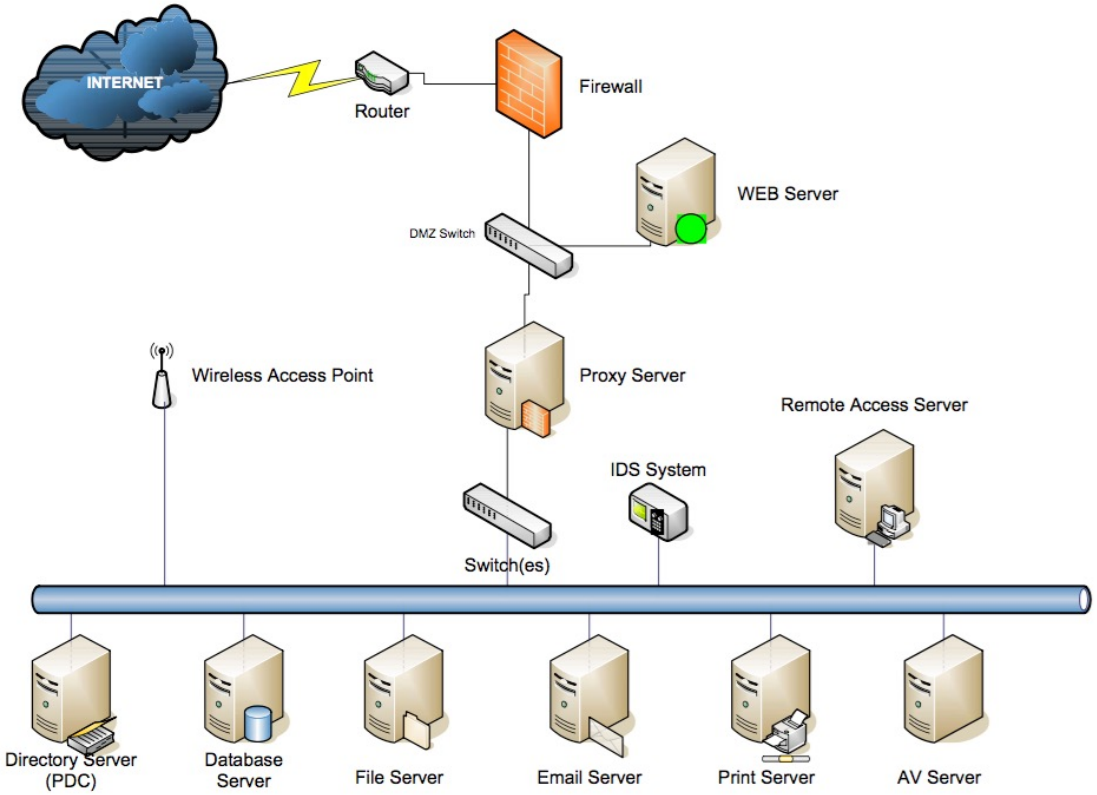
- NIST SP 800-92 (https://csrc.nist.gov/publications/detail/sp/800-92/final)
- BSI IT-Grundschutz-Compendium (OPS 1.1.5) (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2021.html)



What are logs ?

- **Historical** record of events that happened.
- Record of events and status of systems in a **time sequential** format.
- Record of **activity** on a system/network.
- **Objective**: to provide an audit trail of who done what, where, when and why (**5 Ws**)

Where to find logs?



Logs are everywhere

Types

- Audit logs
- Transaction logs
- Intrusion logs
- Connection logs
- System performance recods
- User activity logs
- Alerts and other messages

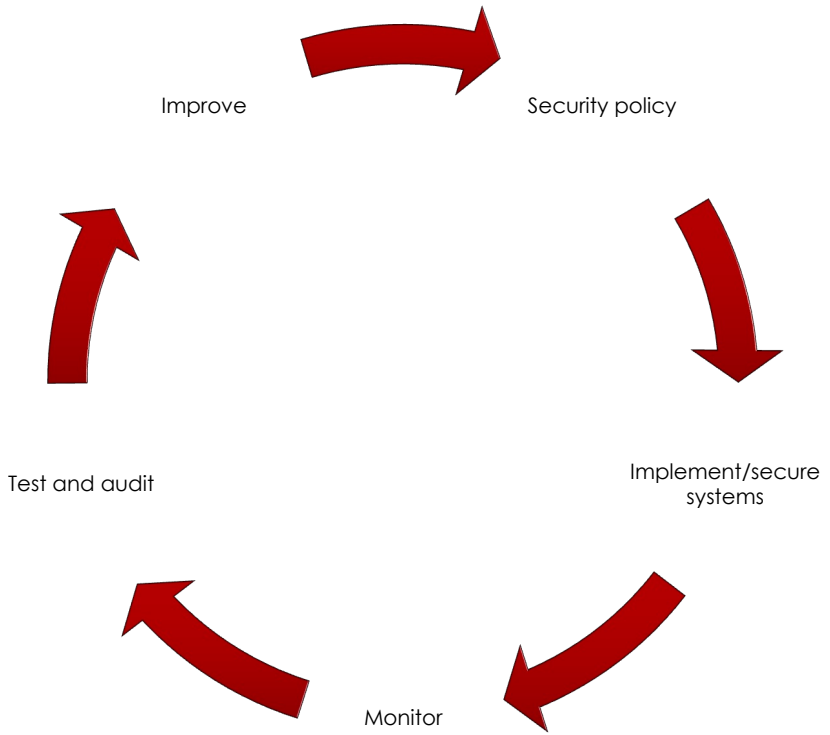
Location

- Firewalls / IPS
- Routers / Switches
- IDS / IAM
- Server, Desktop and other devices (mobile, IoT…)
- Applications
- Databases
- Anti-virus et al.
- VPNs

Why are logs important ?

- Logs assist you in determining *what happened*:
  - Threat / Intrusion detection and discovery
  - Incident response and containment
  - Forensic analysis and litigation support
  - Compliance
    - Regulatory
    - Policy
    - Audit
  - Determining the health of the network
    - Troubleshooting issues
    - Proactive maintenance
  - Proactive protection & Real-time alerts
  - Providing a network baseline

Logging/Monitoring as part of an ISMS



Top 6 mistakes with logging

1. **No logging** at all
2. Not logging **all** the logs
3. Storing logs for **too short time**
4. **Prioritising before** collection
5. **Ignoring application** logs
6. Only looking for **“kown bad”** stuff

Challenges

- Logs contain enormous amount of information
- Logs are "written" by developers
  - Format is not easy to read
  - Messages can be obscure
- Different vendors different log formats
- Identifying anomalies can be difficult
  - Probes over time
- Regulatory requirements

Challenges (2)

- Managing logs can be expensive
  - Looking at all events takes time
  - Logs can consume a lot of disk space
  - Log analysis is a quite unique skill
- Volume of information is huge
- No one size fits all
  - Each network is unique

Log analysis

HTTP access example

```
118.78.23.83 - - [18/Oct/2012:11:05:45
    +0200] ``GET /favicon.ico HTTP/1.0''
    200 4531 ``-'' ``Safari/6534.57.2
    CFNetwork/454.12.4 Darwin/10.8.0 (
    i386) (MacBookPro5%2C1)''
```

What can go wrong ? an example

```
118.78.23.83 - - [18/Oct/2012:11:05:45
  +0200] ''GET /favicon.ico HTTP/1.0''
  200 4531 ''-'' ''Safari/6534.57.2
  CFNetwork/454.12.4 Darwin/10.8.0 (
  i386) (MacBookPro5%2C1)''
```

TCP source port of the client is missing.

Without the source port, the IP address and an adequate time-stamp an ISP won't be able to find back the client if this is behind a NAT device (e.g. Internet mobile access is usually behind a carrier grade NAT device)

Destroying evidence without knowing it

- Aggregation, filtering, correlation or alerting might mean destroying evidences
- As an example, you ask for the raw HTTP logs from a proxy
- It's logged but then aggregated to produce usage report
- In incident analysis, you need the raw logs not the high-end report or simplified alert

Never logging the required evidences

- A chain of 4 reverse proxies (WAF) logging at each state but missing a single X-Forwarded-For in the chain
- If you need to rebuild an end-to-end session from logs, you need to keep track of the source IP address for each records

Time synchronization
good practice

- Have an NTP server with an external source
- Every device shall be synced against that server
- How do you check if your NTP server is really at the correct time?
- A 3 minutes drift when merging 200GB of one hour logs is a big . . .

Proprietary log-formats

- Do you need special tools to extract raw logs? Are those accessible to you ?
- Are the raw logs viable as evidence?
- How long does it take to extract the logs? (e.g. 10 days to extract 5 days)
  - Can you wait 10 days if the "remediation" solution can be found within those logs?

Everything can go wrong with logging

- Log rotation (e.g. what's on going while the rotation is performed?)
- Threshold for limiting logs size (e.g. Many vendors have hard coded values)
- Log analysis requires context (e.g. Is the access from that time period valid? or is it coming from a Malware?)
- Are you just logging denied access? or just accepted access? or both?


More Security Doesn't Make You More Secure
Better Management Does.

Good practices

- **Develop logging Policy**
- **Determine what information is relevant to you.**
  - What devices are important?
  - What events are important?
  - Don't forget to turn on logging!
  - Timing of events, e.g. user logons in morning.
  - What reports you and the business want/need?
  - Group servers into zones based on their function or criticality and prioritise events accordingly.

Good practices (2)

- **Baseline your systems & network.**
  - Determine how your network normally behaves
  - Repeat at regular intervals
  - Define context (e.g. is the event time period valid? or is it coming from a malware?)
- **Secure log files on all devices**
  - Encrypt logs
- **Ensure all devices use same time source.**
  - If using more than one time zone use UTC.
  - Use NTP protocol from a secure source to synchronise time.

Good practices (3)

- **Centralise log collection**
  - Dedicated server to collect all logs.
    - Be careful of network traffic volumes.
    - Be aware of limitations of server to process number of events.
  - Configure all devices send logs to central log server.
  - Make sure central server is secure. Secure transmission of logs.
    - e.g. Syslog uses UDP by default. Consider using IPSec or next generation Syslog (Syslog-NG)

Good practices (4)

- **Normalise the data**
  - All events should be normalised into same format.
- **Review the Logs**
  - Ensure logs are regularly reviewed
    - Manually
    - Automatically

Good practices (5)

- **Log Rotation**
  - Determine time schedule
  - Based on volume of data
  - Develop meaningful naming convention
  - Move data to rotated file
- **Log Retention**
  - May be regulatory requirements
  - Archive onto WORM (Write-Once-Read-Many) type devices and store in secure area

Good practices (6)

- **Using logs for investigation**
  - List and train people to extract logs (and also to read them)
  - Try to manually reconstruct a chain of events from logs
  - Test your log exports (e.g. you ask your local CSIRT/CERT to make a test request)
  - Storing raw logs is usually simpler than creating "aggregated" logs
    - Make sure raw logs are readable by standard text-processing tools
  - Use beacon logs to ensure the effectiveness of your log processing (eg. SIEM)

In a nutshell

- logging is good, log everything
- define the scope of coverage
- define what events constitute a threat
- detail what should be done about them in what time frame
- document when they occurred and what was done
- document where both the events and follow up records can be found
- document how long events and tickets are kept

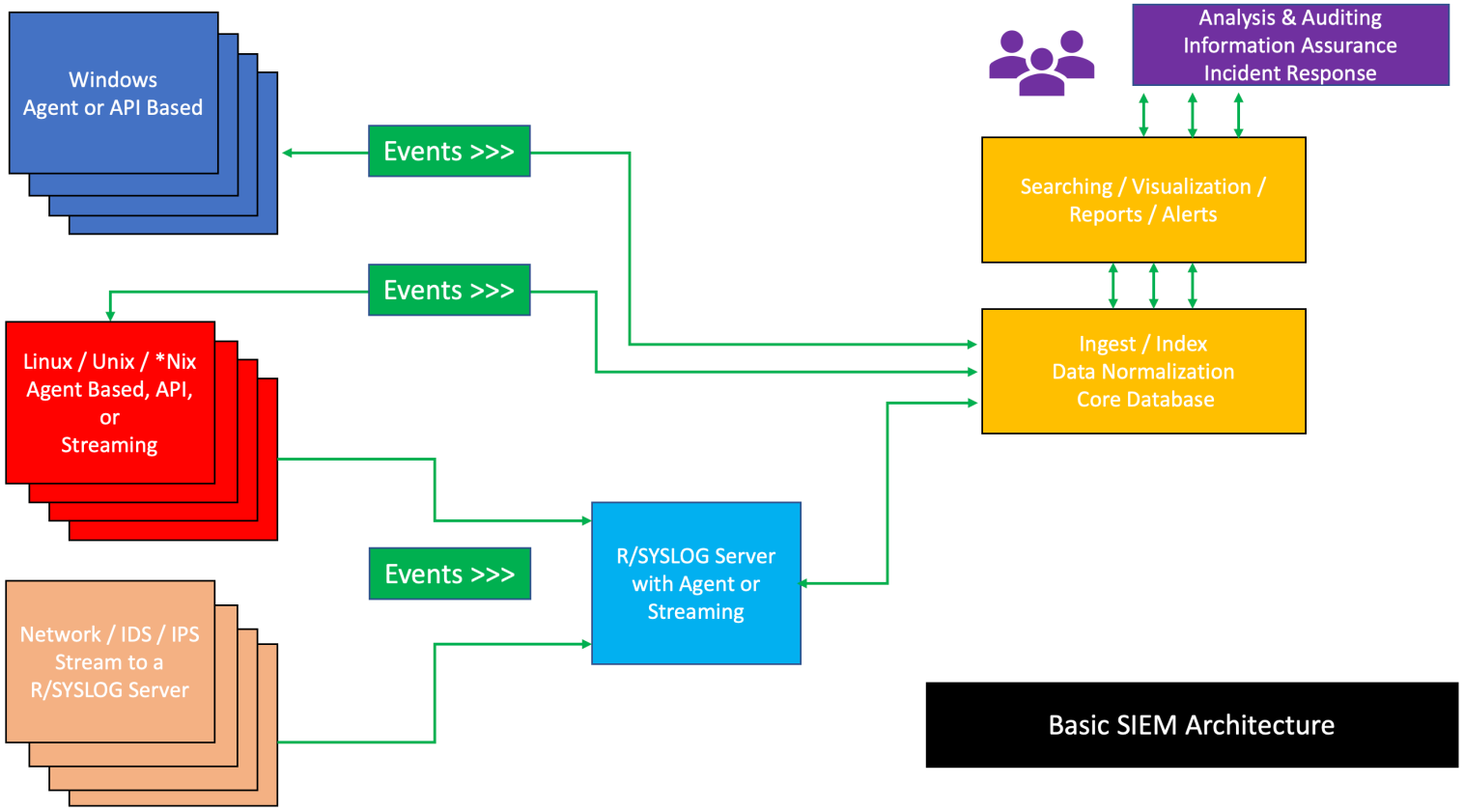
Logging for Detection and Response

Automation or how can computers help us ?

Terminology

- ***Log management*** – Focus on simple collection and storage of log messages and audit trails
- ***SIM (Security information management)*** – Long-term storage as well as analysis and reporting of log data
- ***SEM (Security event manager)*** – Real-time monitoring, correlation of events, notifications and console views
- ***SIEM (Security information and event management)*** – Combines SIM and SEM and provides real-time analysis of security alerts generated by network hardware and applications
- ***SOAR (Security orchestration, automation and response)*** – In SOAR one uses security "playbooks" to automate and coordinate workflows that may include any number of disparate security tools as well as human tasks.
- **EDR (Endpoint Detection and Response) / XDR (eXtended Detection and Response) / MDR (Managed Detection and Response)** done by a MSSP or SOC

SIEM – basic architecture



SIEM – capabilities & components

Capabilities

- **Data aggregation**
- **Correlation**
- **Alerting**
- **Dashboards**
- **Compliance**
- **Retention**
- **Forensic analysis**

Components

- A **data collector** forwards selected audit logs from a host
- An **ingest** and **indexing** point **aggregation** point for parsing, correlation, and data **normalization**
- A **search** node that is used to for **visualization**, queries, **reports**, **alerts** and **analysis**

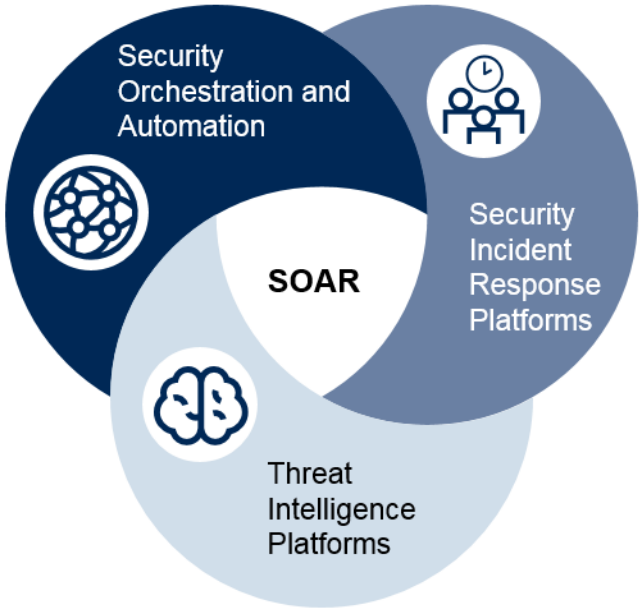
Ok, your SIEM alerted you about an attack or intrusion, what's next?

After the detection comes response,
can we automate this as well?

SOAR (?)

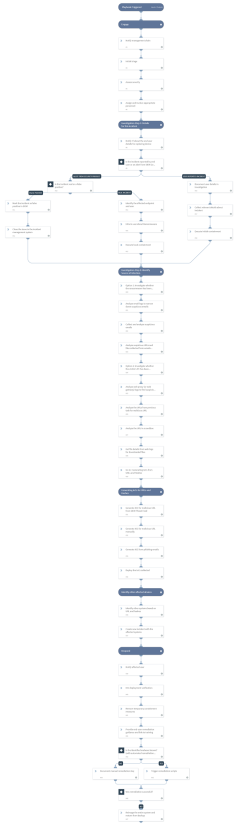
Technology and Workflows to do *Security*…

- **Orchestration:** putting tools together to work with one another, bringing out the full value of each and allowing teams to more effectively respond to threats
- **Automation:** automatic execution of security tasks without human intervention
- **Response:** a structured methodology for handling security incidents, breaches, and cyber threats



SOAR = SOA + SIR + TIP

Ransomware playbook (an example)



- Automate
- Execute
- Coordinate
- People
- Systems

What about the endpoint?

Especially during covid-19, endpoints became quite crucial to manage and secure well

Well there are systems like: *Anti-virus, anti-spam, anti-malware, firewall, HIDS/IPS, etc. etc.*

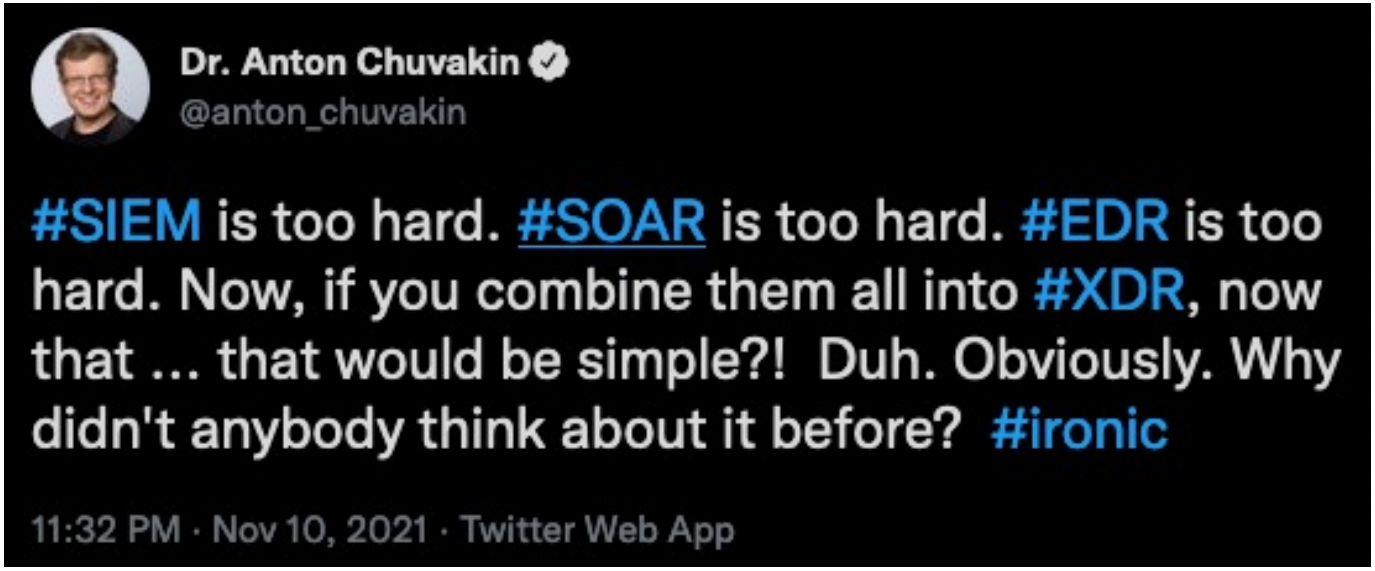
- Bah, that's "old school"!
- Now we go for **EDR**
  - *Endpoint Detection and Response*

EDR – Endpoint Detection and Response

- Monitor and collect activity data from endpoints that could indicate a threat
- Analyse this data to identify threat patterns
- Automatically respond to identified threats to remove or contain them, and notify security personnel
- Forensics and analysis tools to research identified threats and search for suspicious activities

EDR? no, today we are XDR

- XDR brings a proactive approach to threat detection and response.
- Blocks known and unknown attacks
- Uses AI-based analytics to automatically detect sophisticated attacks
- Eradicate threats without business disruption
- Restore hosts to a clean state
- Understand threats and actors with MITRE ATT&CK integration
- Supercharge your security team



https://twitter.com/anton_chuvakin/status/1458563366025265153

What if you don't have a dedicated security team ?

- **MDR** is your friend

Managed detection and response (MDR) services offer dedicated personnel and technology to improve the effectiveness of security operations in threat identification, investigations and response.

The path to *Zero Trust*

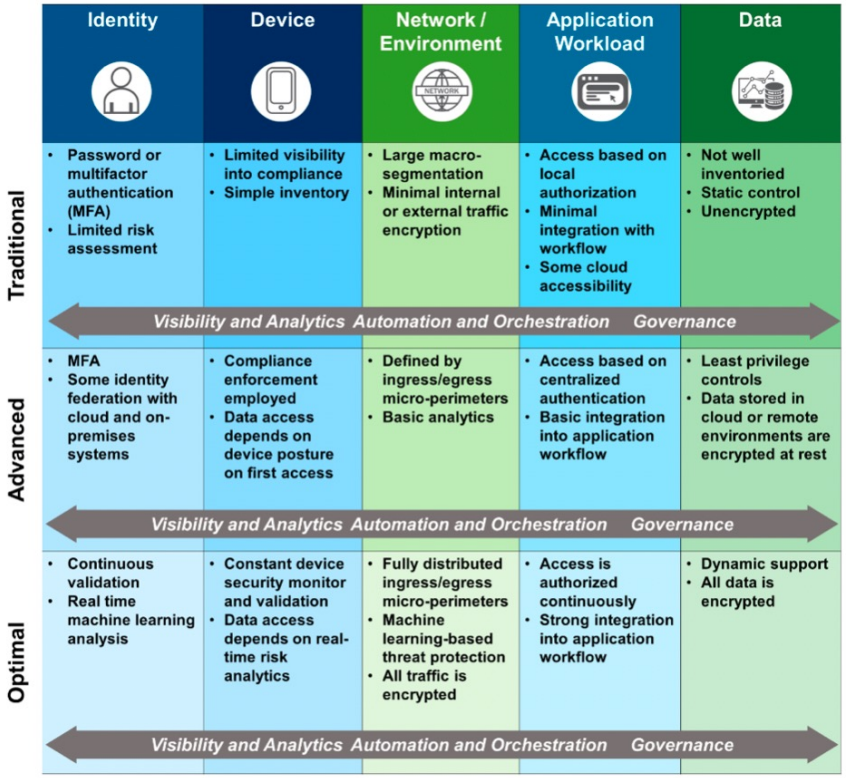


Figure 2: High-Level Zero Trust Maturity Model

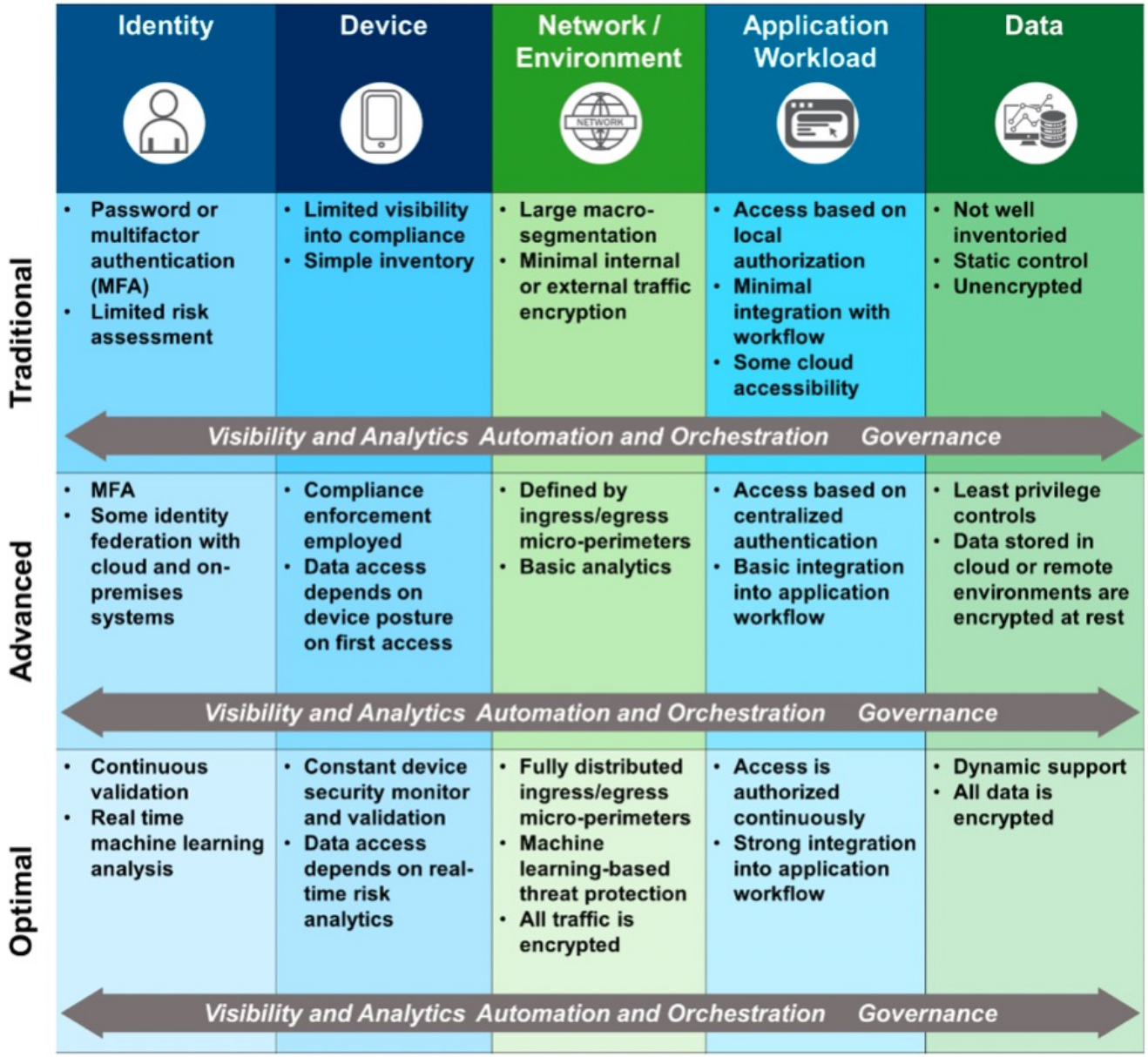


Figure 2: High-Level Zero Trust Maturity Model

Thank you for your attention