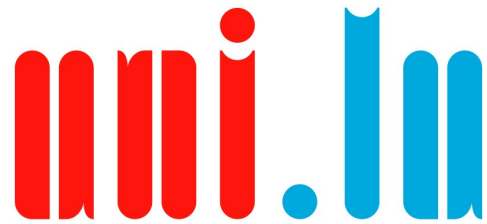




UNIVERSITÉ DU
LUXEMBOURG



UNIVERSITÉ DU
LUXEMBOURG

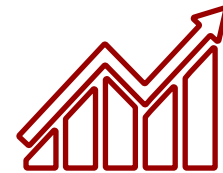
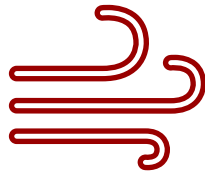
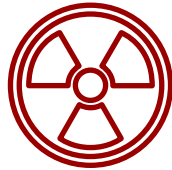
***From logging to next generation detection
and response, and other models
of countermeasures***

Threats, Attacks and Countermeasures

Master in Information System Security Management

How do you approach your risks ?









Risk = Threat * Vulnerability * Impact







Threat landscape

2021/2022

Luxembourg CyberWeather (Q3 2022)

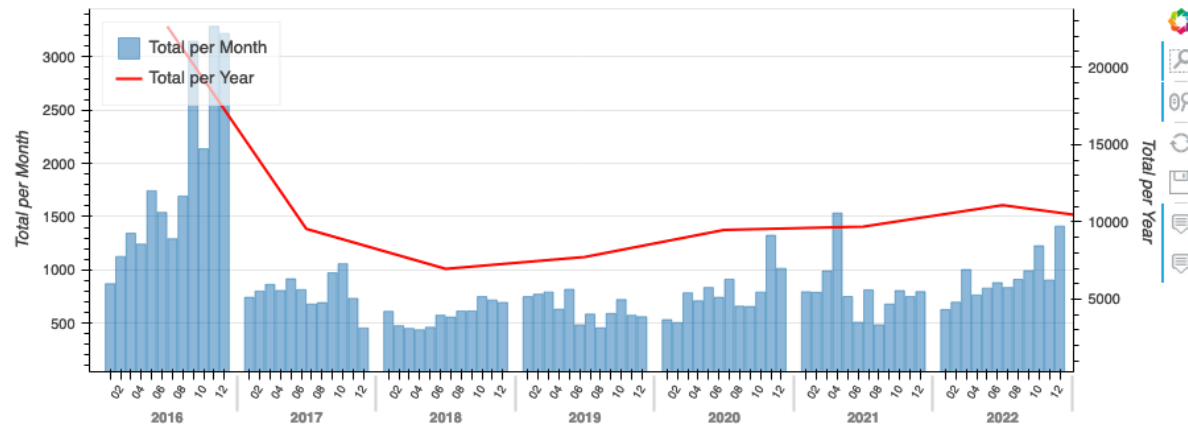
| Category | Status |
|--------------------|---|
| Malware |  |
| Availability |  |
| Phishing and scams |  |
| Intrusions |  |
| Vulnerabilities |  |
| IoT |  |
| eID |  |
| APT |  |

| 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 |  |

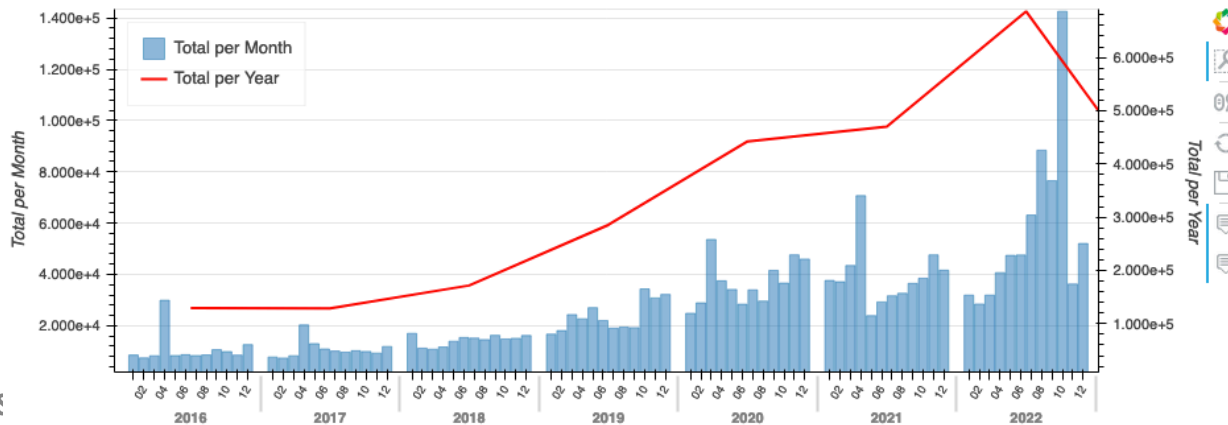
<https://www.govcert.lu/en/cyberweather/>

Luxembourg Operational statistics

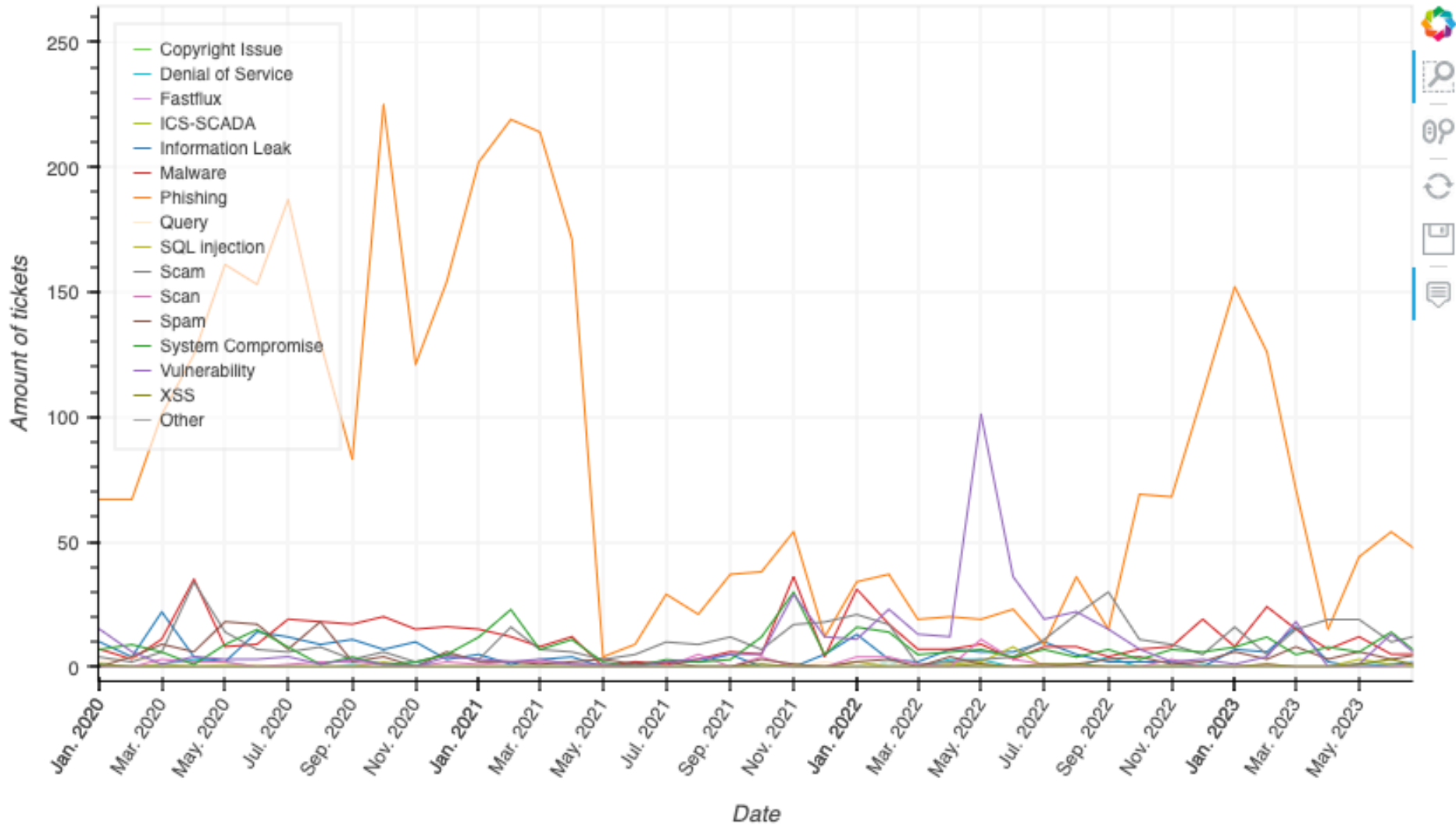
Manual tickets over time



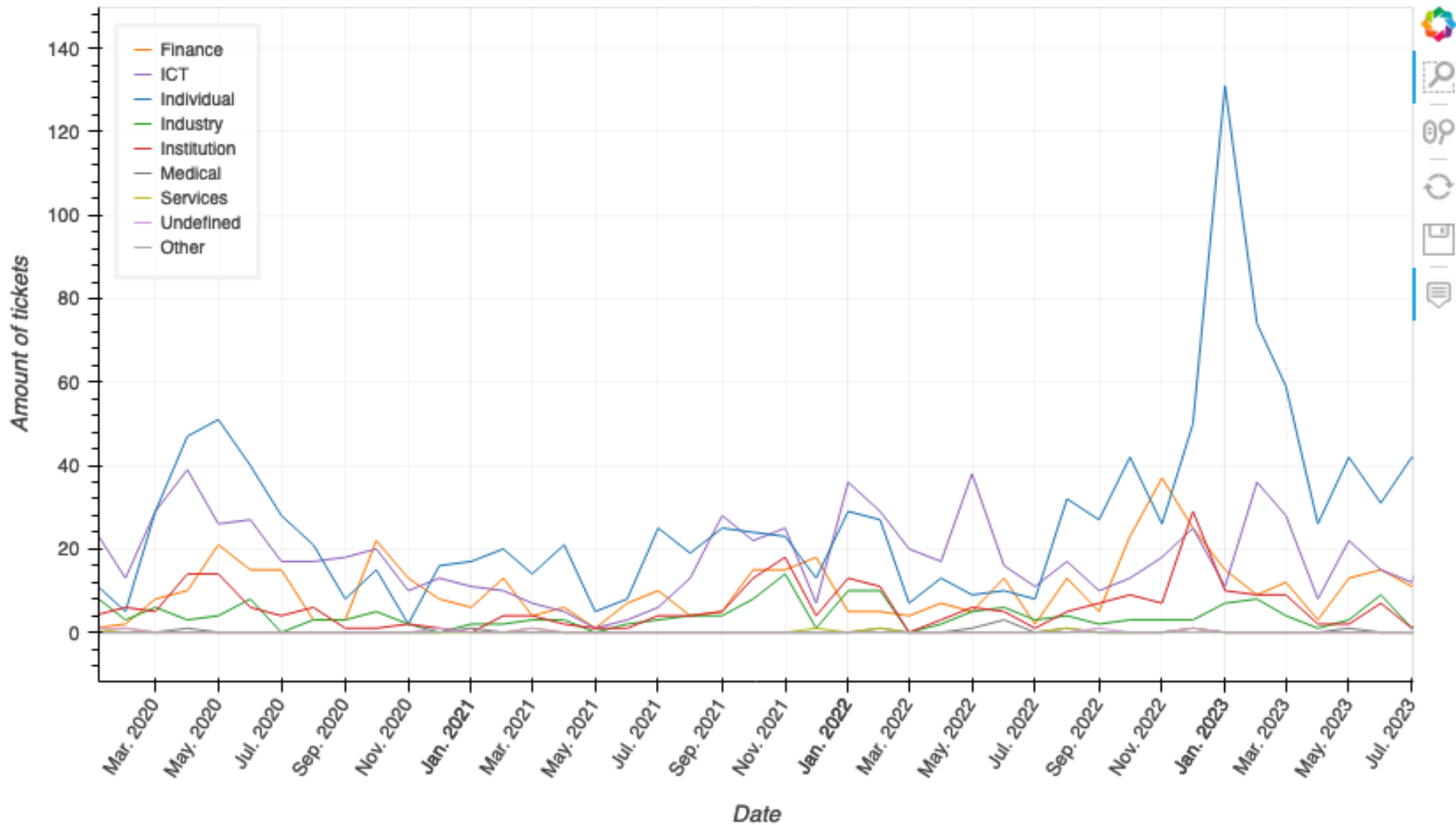
Automatic tickets over time



Manual Ticket Classification over time

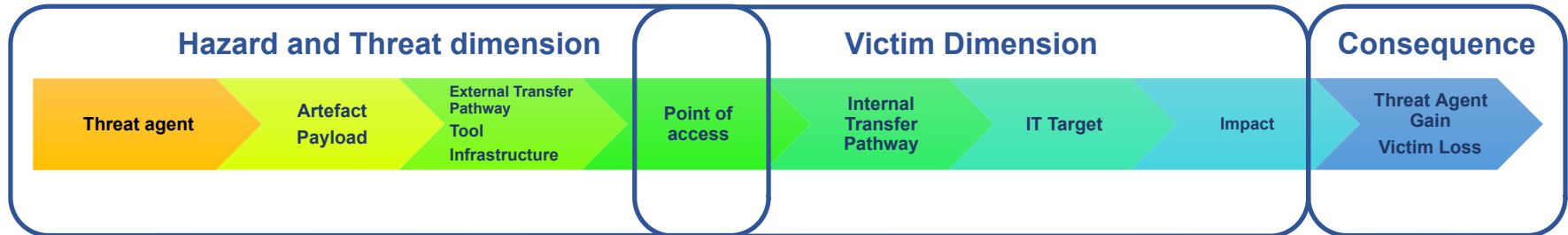


Manual Ticket by Sector over time



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

NC3 TOP – Threat Observatory Platform



| | | nc3.lu National Cybersecurity Competence Center LUXEMBOURG | | BULLETIN Qtr4 | | LTC Luxembourg House of Cybersecurity | |
|--------------------------------------|-------------|---|-------------|------------------|-------|---|--|
| THREAT ACTOR | | | | | | | |
| | Qtr3 | | Qtr4 | | Trend | | |
| | # | % | # | % | | | |
| APT38 | 0 | 0,00% | 1 | 0,07% | ↑ | | |
| FIN7 | 0 | 0,00% | 2 | 0,14% | ↑ | | |
| Gamaredon Group | 5 | 0,34% | 4 | 0,28% | ↓ | | |
| Kimsuky | 12 | 0,82% | 2 | 0,14% | ↓ | | |
| Lazarus Group | 11 | 0,75% | 1 | 0,07% | ↓ | | |
| Mustang Panda | 0 | 0,00% | 1 | 0,07% | ↑ | | |
| OPERA1ER | 0 | 0,00% | 2 | 0,14% | ↑ | | |
| Sandworm Team | 0 | 0,00% | 1 | 0,07% | ↑ | | |
| Silent Librarian | 5 | 0,34% | 1 | 0,07% | ↓ | | |
| Turla | 1 | 0,07% | 2 | 0,14% | ↑ | | |
| Number of attributed events | 48 | 3,28% | 17 | 1,18% | ▼ | | |
| Number of unattributed events | 1417 | 96,72% | 1427 | 98,82% | = | | |
| Attribution Rate | 3,3% | | 1,2% | | ▼ | | |

| | | nc3.lu National Cybersecurity Competence Center LUXEMBOURG | | BULLETIN Qtr4 | | LTC Luxembourg House of Cybersecurity | |
|--------------------------------------|--------------|---|--------------|------------------|-------|---|--|
| EXTERNAL TRANSFER PATHWAY | | | | | | | |
| | Qtr3 | | Qtr4 | | Trend | | |
| | # | % | # | % | | | |
| Attack | 12 | 0,82% | 7 | 0,48% | ↓ | | |
| Brute Force Attack | 0 | 0,00% | 2 | 0,14% | ↑ | | |
| DDoS | 1 | 0,07% | 2 | 0,14% | ↑ | | |
| Defense Evasion | 1 | 0,07% | 2 | 0,14% | ↑ | | |
| DNS Hijacking | 0 | 0,00% | 1 | 0,07% | ↑ | | |
| Espionage | 1 | 0,07% | 2 | 0,14% | ↑ | | |
| Execution | 25 | 1,71% | 35 | 2,42% | ↑ | | |
| Malicious Network Activity | 4 | 0,27% | 11 | 0,76% | ↑ | | |
| Malspam | 5 | 0,34% | 9 | 0,62% | ↑ | | |
| Phishing | 429 | 29,28% | 485 | 33,59% | ↔ | | |
| Smishing | 18 | 1,23% | 121 | 8,38% | ↑ | | |
| Number of attributed events | 499 | 34,06% | 677 | 46,88% | ▲ | | |
| Number of unattributed events | 966 | 65,94% | 767 | 53,12% | ▼ | | |
| Attribution Rate | 34,1% | | 46,9% | | ▲ | | |

<https://nc3.lu/pages/b2022/q4/b2022q4.html>

Europe

Top threats, majors trends



<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>

Figure 1: ENISA Threat Landscape 2022 - Prime threats



Figure 5: EU breakdown of number of threats by threat group

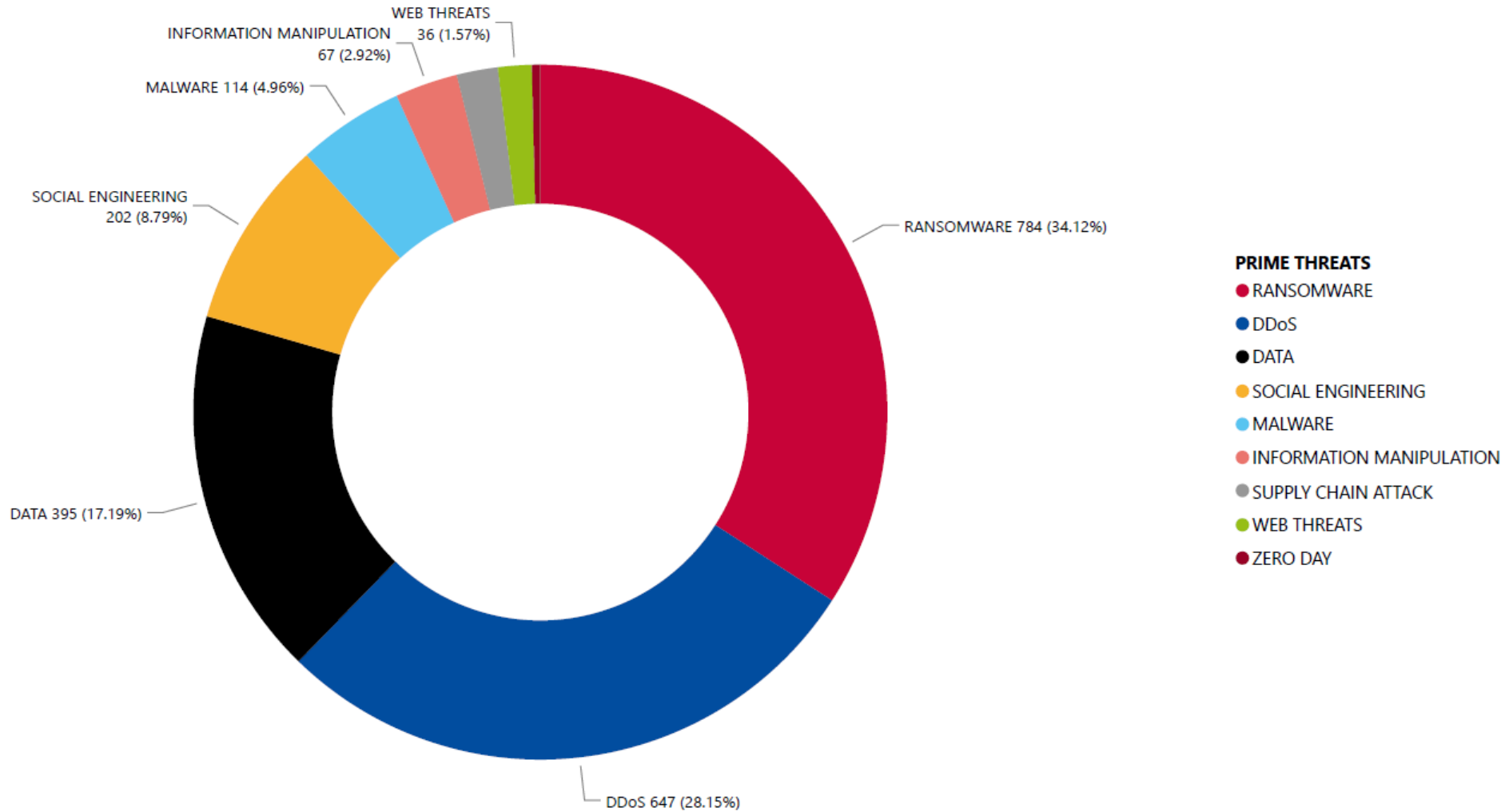
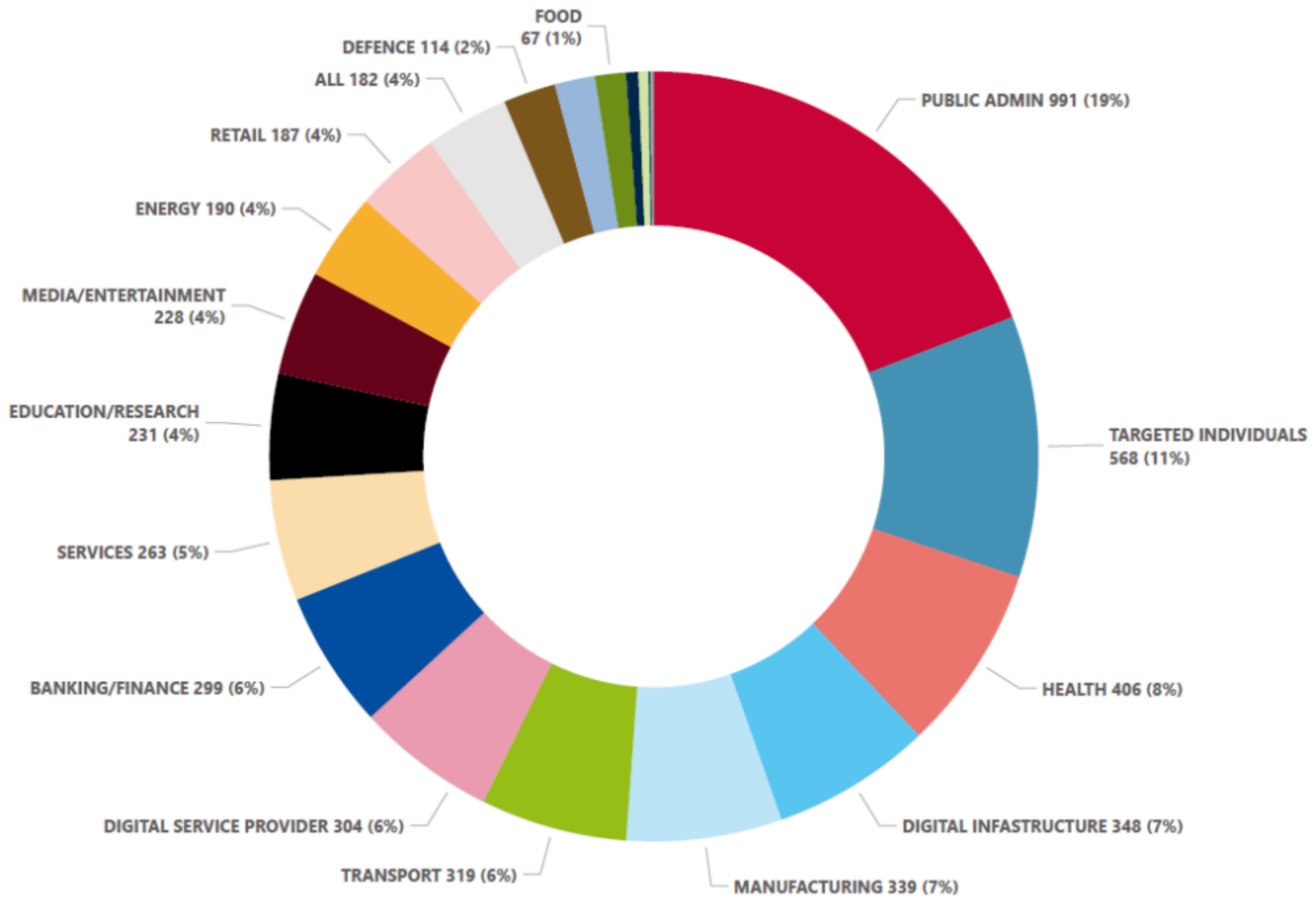


Figure 6: Targeted sectors per number of incidents (July 2022 - June 2023)



Europe (main findings)

- **Ransomware and threats against availability ranked at the top during the reporting period.**
- **Resourceful threat actors have been observed to misuse legitimate tools** primarily to prolong their cyber espionage operations . Their aim was to evade detection for as long as possible and obscure their activities by using widely available software from most systems which makes it more challenging for defenders to identify them. Maximizing their chances of success when it comes to an intrusion by not arousing victim' suspicions
- **Geopolitics continue to have a strong impact on cyber operations.**
- **Several threat actors further professionalised** their As-a-Service programmes. They not only used novel tactics and methods to infiltrate environments but also delved into alternative approaches to pressure and extort victims, all the while advancing their illicit enterprises.
- **By Using Extortion Only Techniques** criminal organisations have been progressively blending extortion methods that almost invariably incorporate some form of data theft. Double extortion has witnessed a notable rise, with certain groups even relying solely on the act of stealing information.
- **Increased operations by law enforcement**, such as the takedown of Hive ransomware group's IT infrastructure or Trickbot.
- **CI0p rose** in the first half of 2023 with the weaponisation of two zero-days.
- **One of the biggest malware threats is still information stealers** such as Agent Tesla, Redline Stealer and FormoBook.
- **There is a steady decline in classic mobile malware**, with adware remaining in numbers of occurrences the most prevalent threat to mobile devices while in terms of impact spyware can be seen as the most prevalent threat to mobile devices.



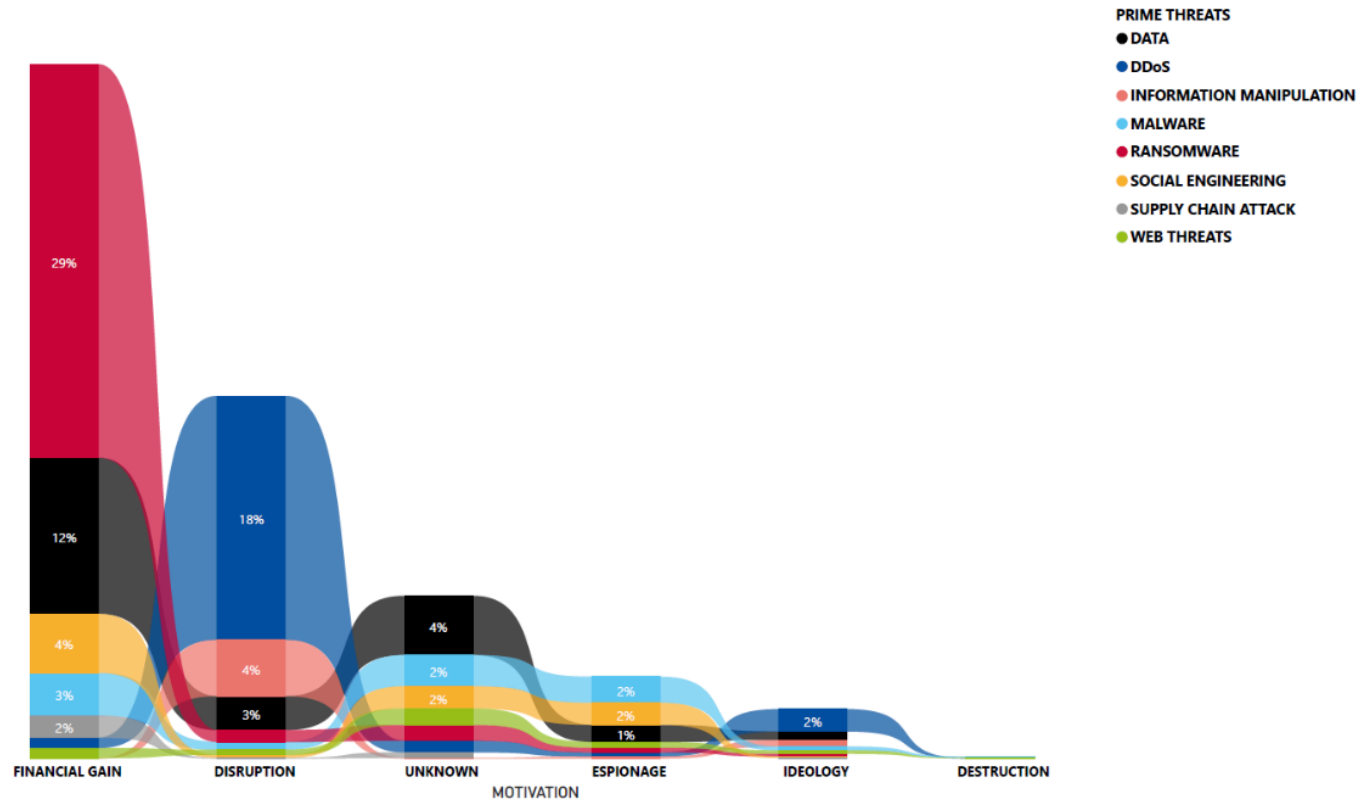
Europe (main findings cont'd)

- **Hacktivists are increasingly claiming that they target OT environments** but public reporting indicate they often **overestimate** or do not **substantiate** their claims.
- **Phishing is once again the most common vector** for initial access. But a new model of social engineering is also emerging, an approach that consists of **deceiving victims in the physical world**.
- **Business e-mail compromise (BEC, VEC) remains** one of the attacker's favourite means for obtaining financial gain.
- **The move from Microsoft macros to ISO , Onenote and LNK files is continuing**, a shift towards the use of LNK and ISO/ZIP files as well as Onenote files in response to Microsoft's macro changes.
- **Data compromise increased in 2023**. There was a rise in data compromises leading up to 2021, and although this trend remained relatively stable in 2022, it began to increase once more in 2023.
- **There has been a Surge in AI Chatbots impacting the cybersecurity threat landscape**. The disruptive impact and the exponential adoption of generative artificial intelligence chatbots such as OpenAI ChatGPT, Microsoft Bing and Google Bard are changing the way in which we work, live and play, all built around data sharing and analysis.
- **DDoS attacks are getting larger and more complex, are moving towards mobile networks and IoT and are being used in the context of** being used in support of additional means in the context of a conflict.
- **Internet shutdowns are at an all-time high**. Internet availability threats are keeping up their momentum, especially in the post-covid era, due to the increasing reliance of human activities and society on Internet technologies.
- **Information manipulation is a key element of Russia's war of aggression against Ukraine**. Information manipulation has been an essential and well-established component of Russia's security strategies^{16 17}. The number of analysed events for the reporting period has also grown significantly.
- **'Cheap fakes' and AI-enabled manipulation of information** continues to be a cause for concern. In the past months, the debate on the use of AI to manipulate information has heated up both within and beyond the circle of industry professionals.
- **Threat groups have an increased interest in supply chain attacks and exhibit an increasing capability by using employees as entry points**. Threat actors will continue to target employees with elevated privileges, such as developers or system administrators



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)

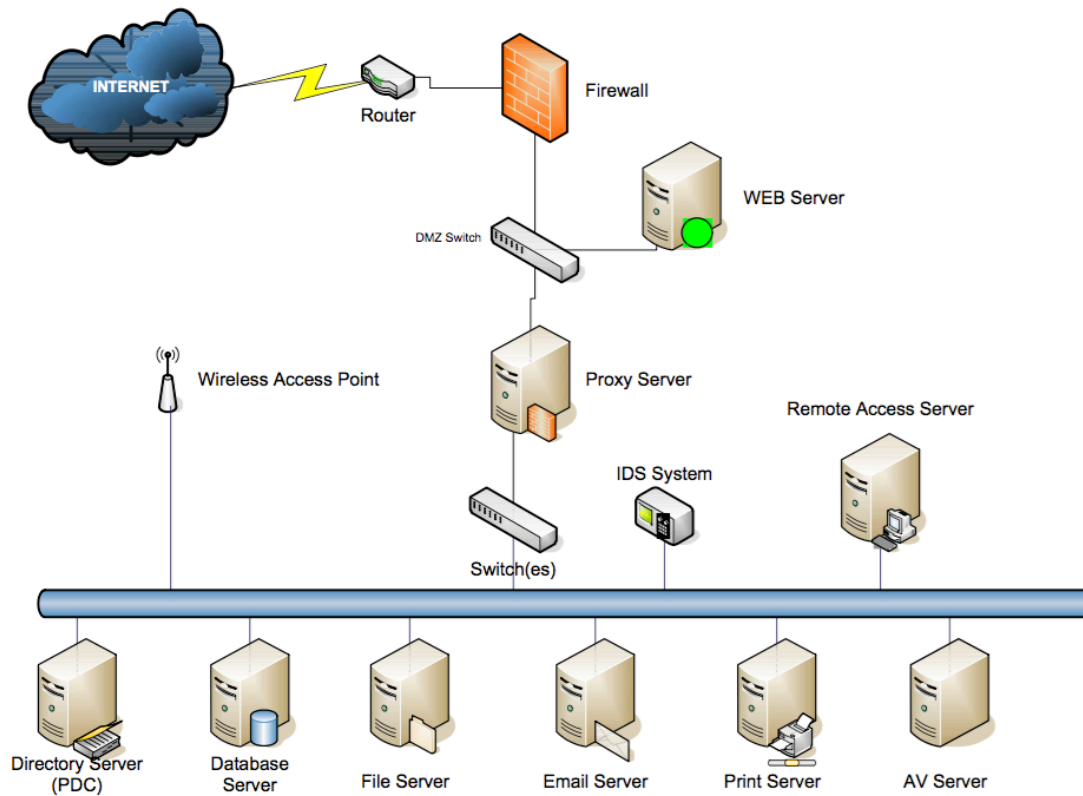


What are logs ?

- **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**)

```
2015-07-21T20:02:
ch-2.3.1/var/log/
2015-07-21T20:02:
.1/var/run/opensv
2015-07-21T20:02:
.1/var/run/opensv
opened datapath o
2015-07-21T20:02:
circulation
2015-07-21T20:02:
gth probed as 3
2015-07-21T20:02:
65534
2015-07-21T20:02:
t failed (No such
2015-07-21T20:02:
3344
2015-07-21T20:02:
2015-07-21T20:02:
2015-07-21T20:02:
t failed (No such
2015-07-21T20:02:
onds
2015-07-21T20:02:
```

Where to find logs?



Logs are everywhere

Types

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

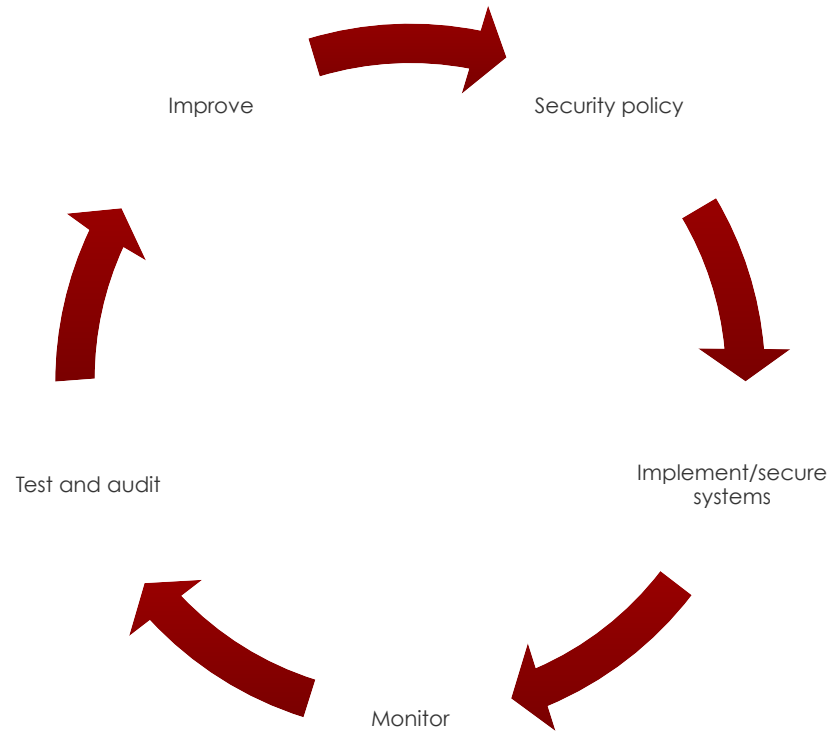
Location

- 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

TCP source port of the client is missing.

```
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)""
```

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

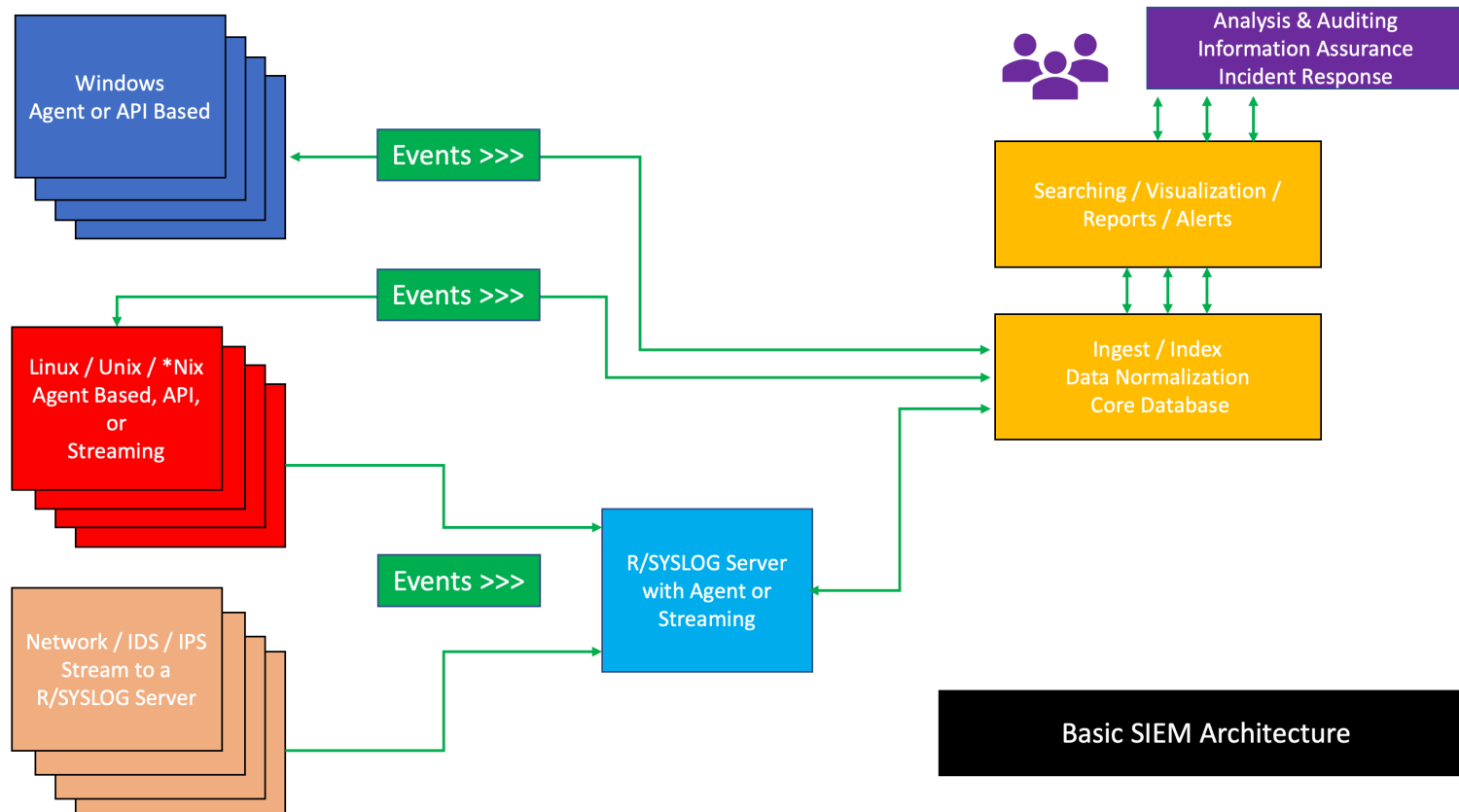
Automation or how can computers help us ?

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

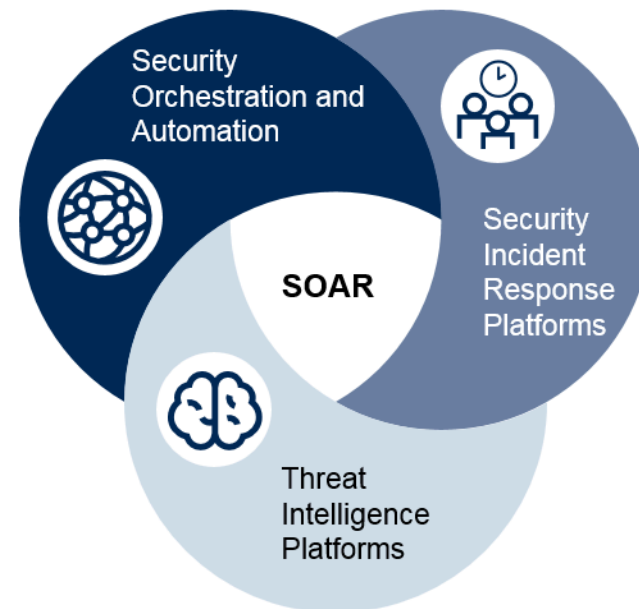
Ok, your SIEM alerted you
about an attack or intrusion,
what's next?

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

SOAR (?)

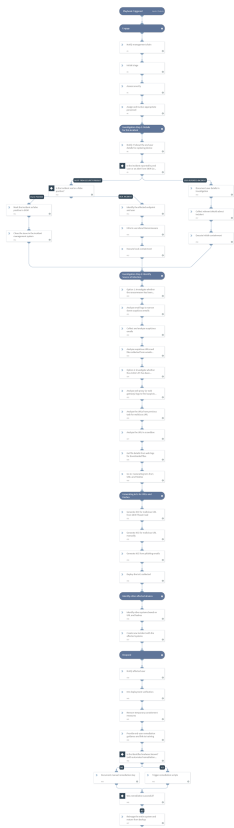
Technology and Workflows to do *Security*...

- **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



Dr. Anton Chuvakin ✓

@anton_chuvakin

#SIEM is too hard. **#SOAR** is too hard. **#EDR** is too hard. Now, if you combine them all into **#XDR**, now that ... that would be simple?! Duh. Obviously. Why didn't anybody think about it before? **#ironic**

11:32 PM · Nov 10, 2021 · Twitter Web App

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*



| | Identity | Device | Network / Environment | Application Workload | Data |
|---|---|--|---|--|---|
| Traditional | <ul style="list-style-type: none"> • Password or multifactor authentication (MFA) • Limited risk assessment | <ul style="list-style-type: none"> • Limited visibility into compliance • Simple inventory | <ul style="list-style-type: none"> • Large macro-segmentation • Minimal internal or external traffic encryption | <ul style="list-style-type: none"> • Access based on local authorization • Minimal integration with workflow • Some cloud accessibility | <ul style="list-style-type: none"> • Not well inventoried • Static control • Unencrypted |
| | <p style="text-align: center;">← Visibility and Analytics Automation and Orchestration Governance →</p> | | | | |
| | Advanced | <ul style="list-style-type: none"> • MFA • Some identity federation with cloud and on-premises systems | <ul style="list-style-type: none"> • Compliance enforcement employed • Data access depends on device posture on first access | <ul style="list-style-type: none"> • Defined by ingress/egress micro-perimeters • Basic analytics | <ul style="list-style-type: none"> • Access based on centralized authentication • Basic integration into application workflow |
| <p style="text-align: center;">← Visibility and Analytics Automation and Orchestration Governance →</p> | | | | | |
| Optimal | <ul style="list-style-type: none"> • Continuous validation • Real time machine learning analysis | <ul style="list-style-type: none"> • Constant device security monitor and validation • Data access depends on real-time risk analytics | <ul style="list-style-type: none"> • Fully distributed ingress/egress micro-perimeters • Machine learning-based threat protection • All traffic is encrypted | <ul style="list-style-type: none"> • Access is authorized continuously • Strong integration into application workflow | <ul style="list-style-type: none"> • Dynamic support • All data is encrypted |
| <p style="text-align: center;">← Visibility and Analytics Automation and Orchestration Governance →</p> | | | | | |

Figure 2: High-Level Zero Trust Maturity Model



















| | Identity | Device | Network / Environment | Application Workload | Data |
|-------------|---|--|---|--|---|
| Traditional |  |  |  |  |  |
| | <ul style="list-style-type: none"> • Password or multifactor authentication (MFA) • Limited risk assessment | <ul style="list-style-type: none"> • Limited visibility into compliance • Simple inventory | <ul style="list-style-type: none"> • Large macro-segmentation • Minimal internal or external traffic encryption | <ul style="list-style-type: none"> • Access based on local authorization • Minimal integration with workflow • Some cloud accessibility | <ul style="list-style-type: none"> • Not well inventoried • Static control • Unencrypted |
| |  | | | | |
| Advanced |  |  |  |  |  |
| | <ul style="list-style-type: none"> • MFA • Some identity federation with cloud and on-premises systems | <ul style="list-style-type: none"> • Compliance enforcement employed • Data access depends on device posture on first access | <ul style="list-style-type: none"> • Defined by ingress/egress micro-perimeters • Basic analytics | <ul style="list-style-type: none"> • Access based on centralized authentication • Basic integration into application workflow | <ul style="list-style-type: none"> • Least privilege controls • Data stored in cloud or remote environments are encrypted at rest |
| |  | | | | |
| Optimal |  |  |  |  |  |
| | <ul style="list-style-type: none"> • Continuous validation • Real time machine learning analysis | <ul style="list-style-type: none"> • Constant device security monitor and validation • Data access depends on real-time risk analytics | <ul style="list-style-type: none"> • Fully distributed ingress/egress micro-perimeters • Machine learning-based threat protection • All traffic is encrypted | <ul style="list-style-type: none"> • Access is authorized continuously • Strong integration into application workflow | <ul style="list-style-type: none"> • Dynamic support • All data is encrypted |
| |  | | | | |

Figure 2: High-Level Zero Trust Maturity Model

Thank you
for your attention