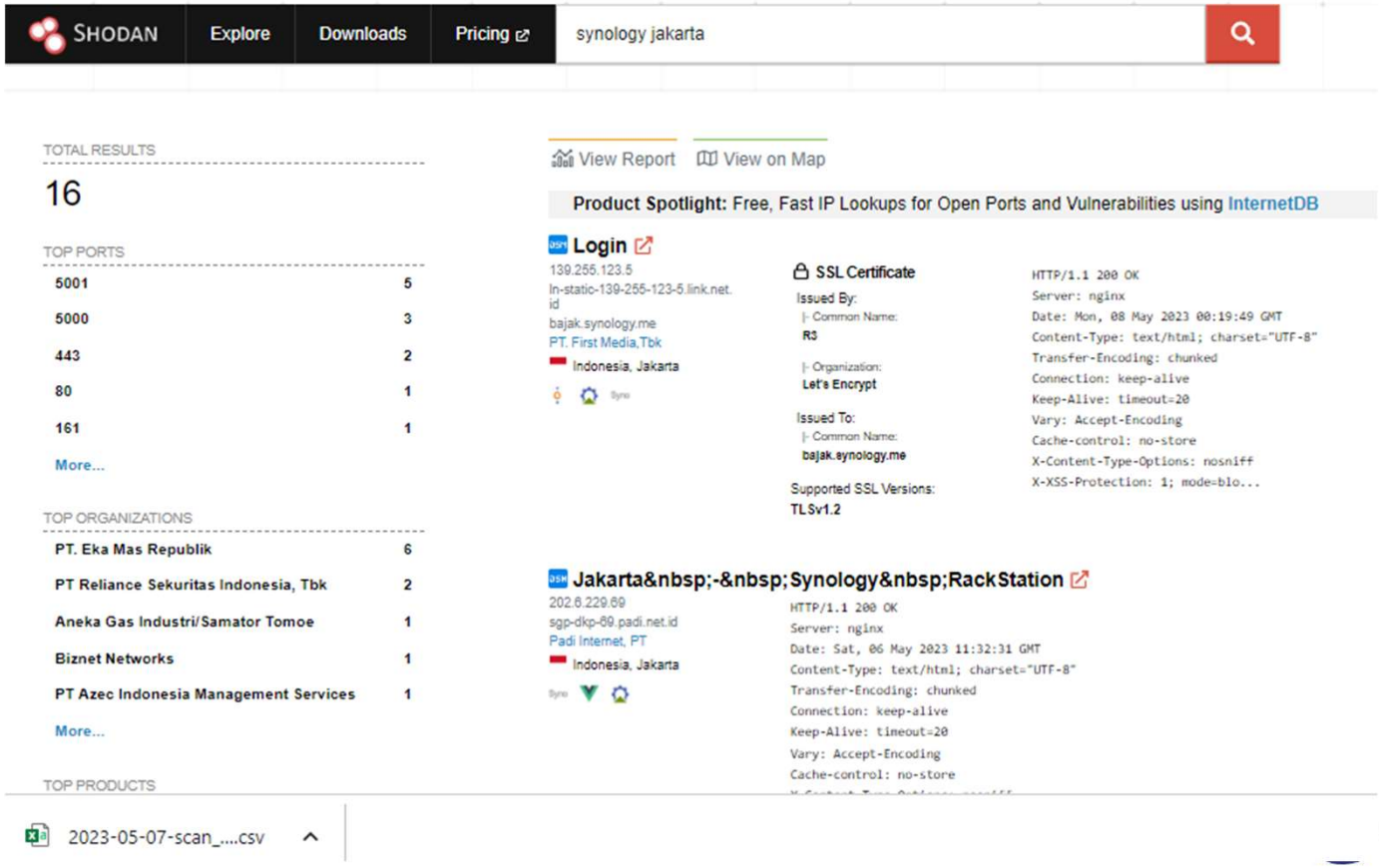
CrowdSecure

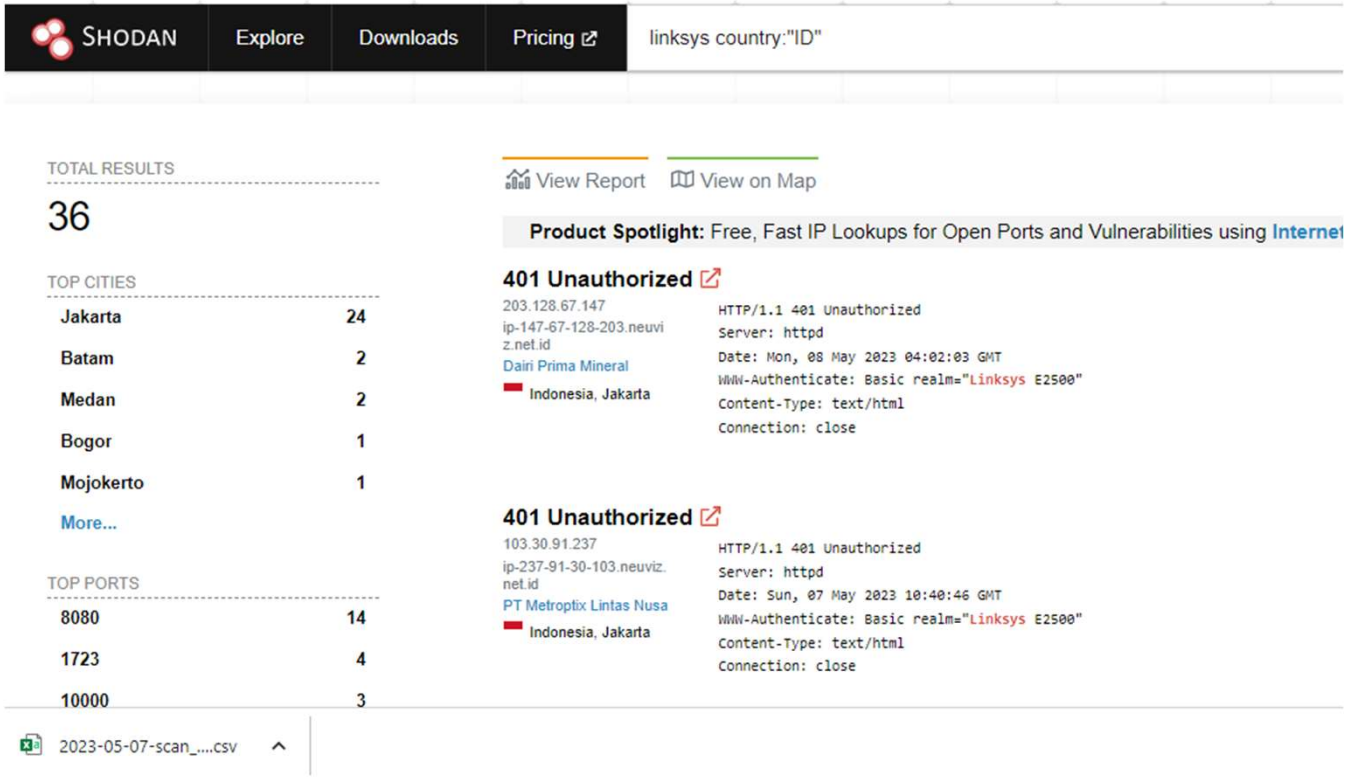
Protecting your Company from Cyber Attacks: A Pragmatic Approach

Richard Iau, CISO

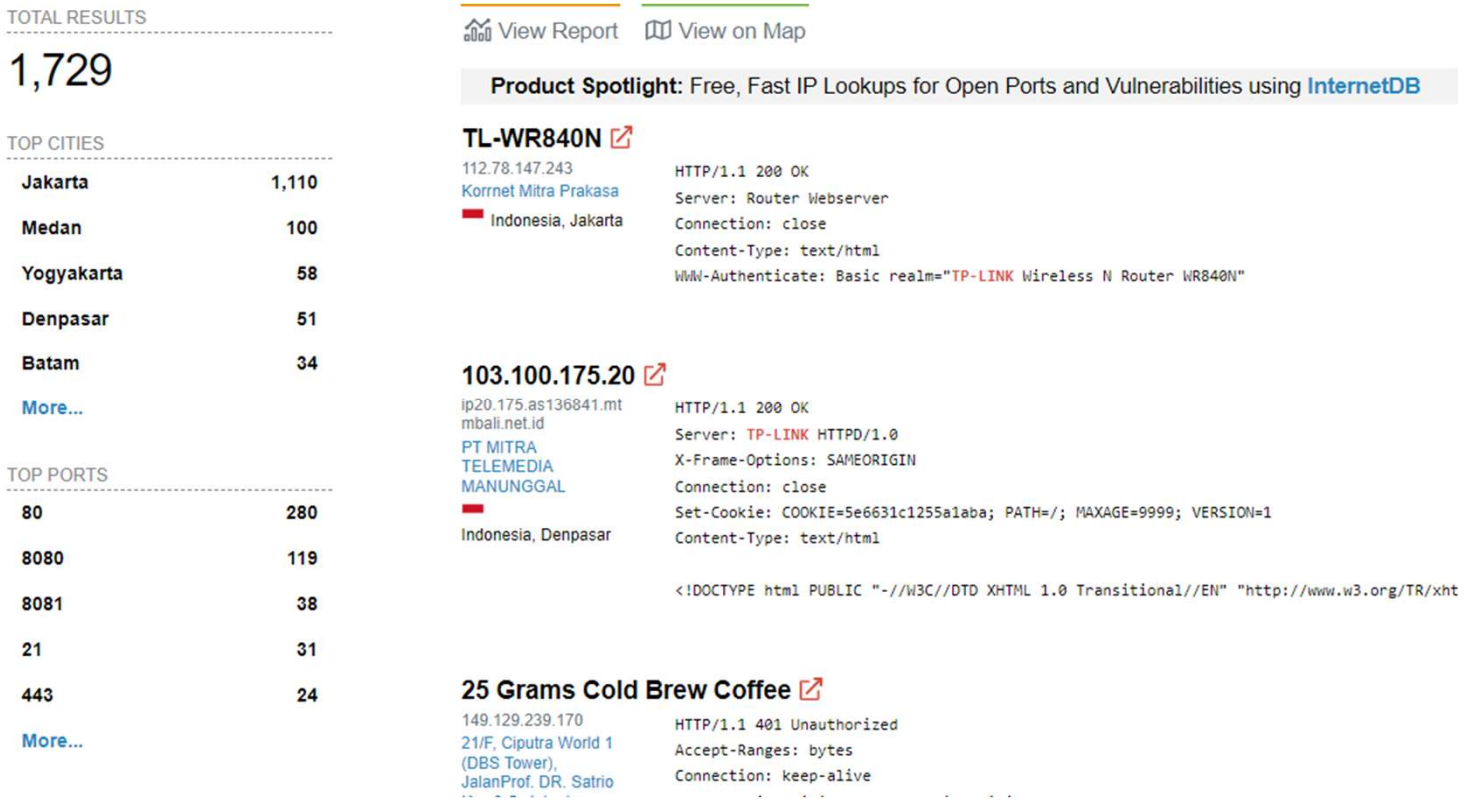
Hacking is an organized business



Hacking is an organized business



Hacking is an organized business



TOTAL RESULTS

1,729

TOP CITIES

Jakarta	1,110
Medan	100
Yogyakarta	58
Denpasar	51
Batam	34

More...

TOP PORTS

80	280
8080	119
8081	38
21	31
443	24

More...

View Report View on Map

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

TL-WR840N

112.78.147.243
Kornet Mitra Prakasa
Indonesia, Jakarta

```
HTTP/1.1 200 OK
Server: Router Webserver
Connection: close
Content-Type: text/html
WWW-Authenticate: Basic realm="TP-LINK Wireless N Router WR840N"
```

103.100.175.20

ip20.175.as136841.mtmbali.net.id
PT MITRA TELEMEDIA MANUNGGAL
Indonesia, Denpasar

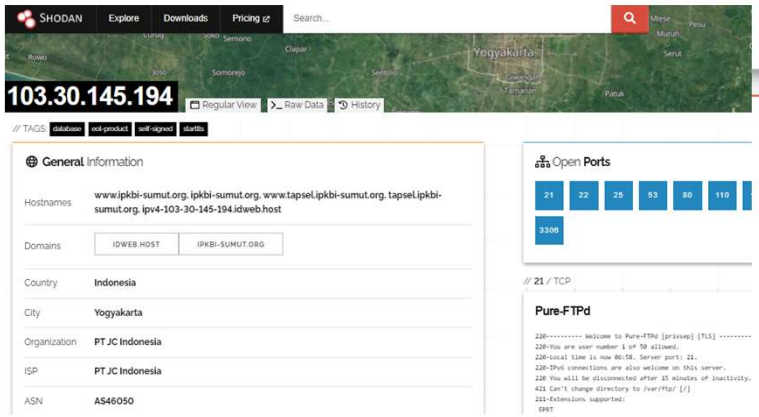
```
HTTP/1.1 200 OK
Server: TP-LINK HTTPD/1.0
X-Frame-Options: SAMEORIGIN
Connection: close
Set-Cookie: COOKIE=5e6631c1255a1aba; PATH=/; MAXAGE=9999; VERSION=1
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xht
```

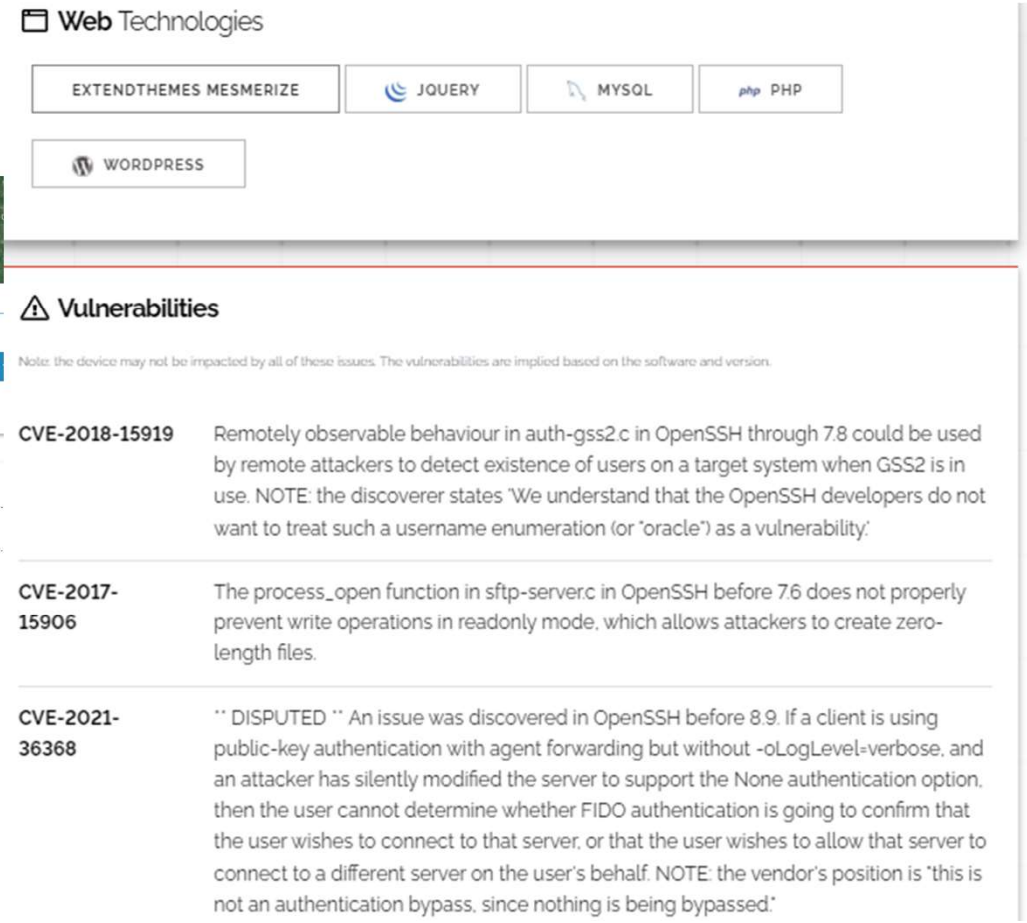
25 Grams Cold Brew Coffee

149.129.239.170
21/F, Ciputra World 1 (DBS Tower), JalanProf. DR. Satrio

```
HTTP/1.1 401 Unauthorized
Accept-Ranges: bytes
Connection: keep-alive
```

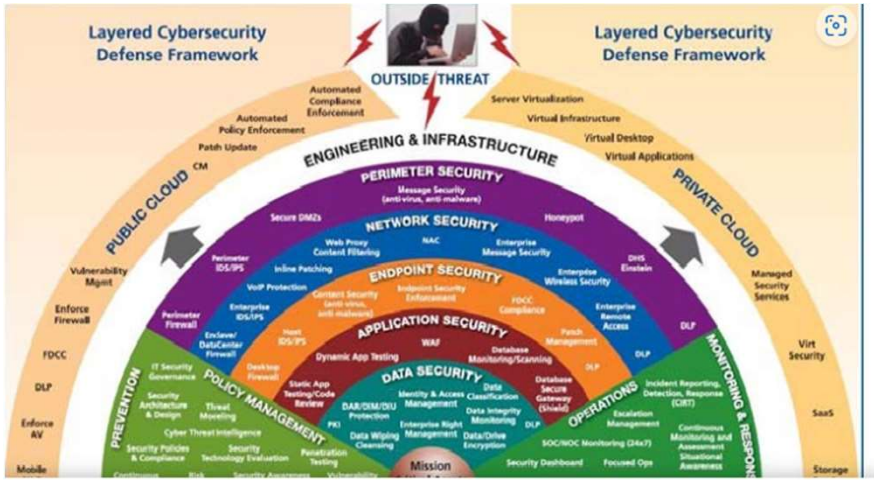
Hacking is an organized business





Background

- **Cybersecurity is too complex for Small Medium Business with little Cyber skills:** attackers are monetizing data theft, so everyone is constantly attacked, regardless of size
- **ISO27000 is too high-level for effective security:** cyber risk conversations provide no assurance that the company is adequately protected
- **Pragmatic approach is needed**: effective and inexpensive so that management know they are adequately protected and can focus on the business



Examples of ISO27000 Controls

- **Log Reviews:** companies are asked to review regularly (?daily) privilege account activity, firewall & AV logs. Many perform this manually Is this effective?
- **Maintain Asset Inventory, Perform inventory reconciliation:** with on-demand cloud infrastructure changes can happen daily. Manual update of the inventory list is time consuming is there a smarter way?
- **Reporting and Assessing Security events**: 45% of security events (Ponemon study) are false positives. Wasteful consumption of scarce resource.

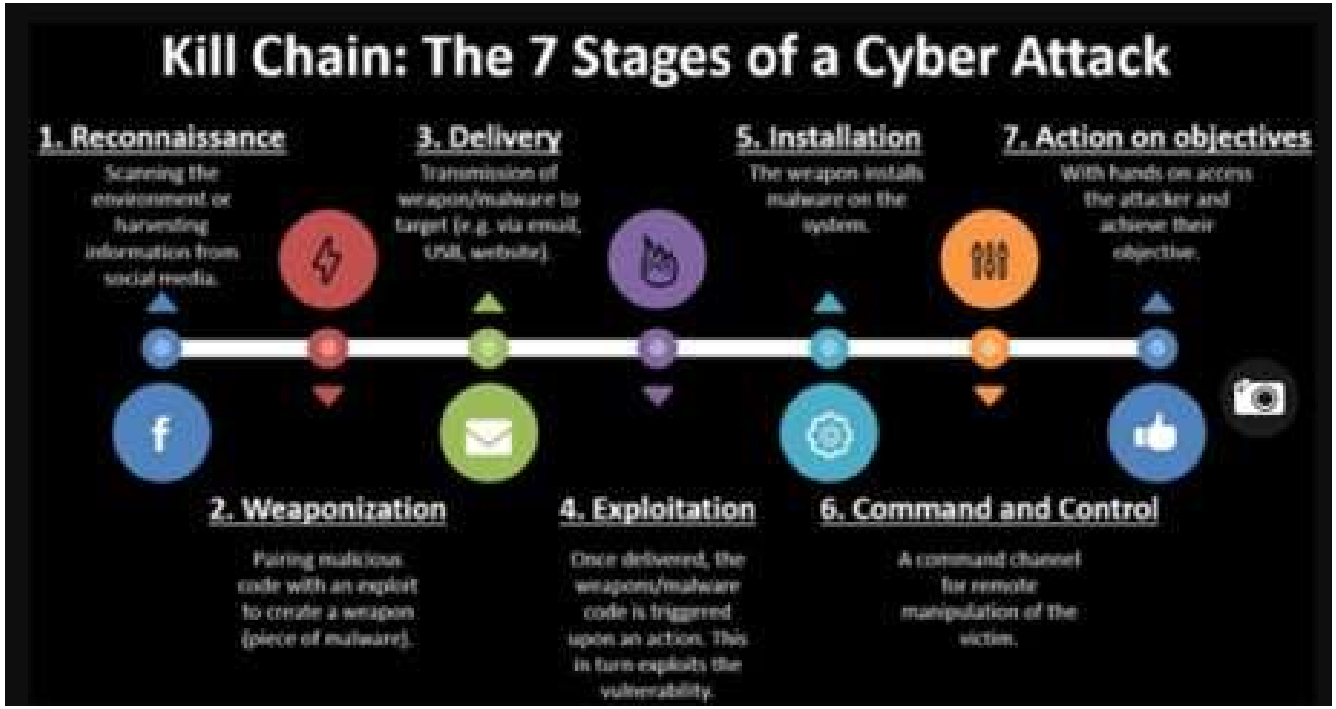
Security Operations Challenges

- **Too many tools:** companies have implemented technologies to counter cyber threats, these run in siloed stacks and the increased complexity hinders timely response
- **Lack of automation:** too many manual process
- **Volume of alerts:** masks threats and alert fatigue sets-up
- **Skills shortage:** struggle to retain and acquire senior level staff

Do I need a SOC?
Answer:Yes if you are concerned about security events and want timely detection

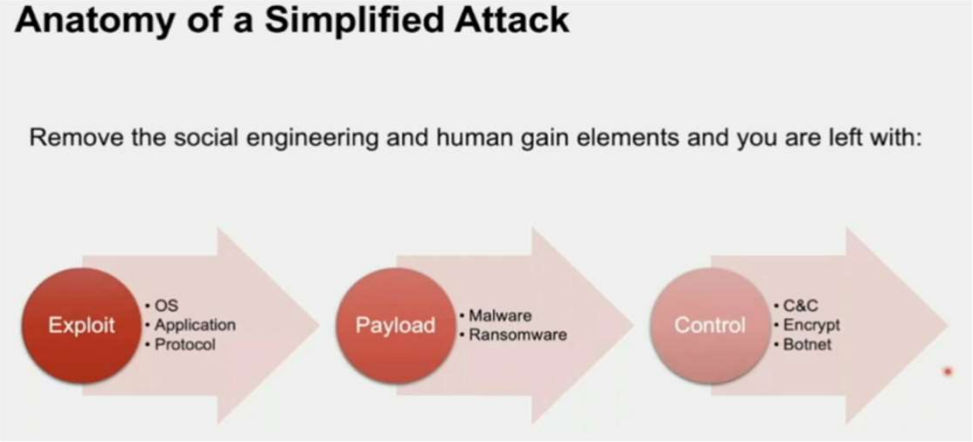
Cyber Attack Stages

- **Defend Better:** if we know the stages of attack.
- We can reduce risk of attack by putting in measures to disrupt any attack
- Attacks will happen and response is critical



How do Hackers succeed: 2 key areas

- **Exploit Vulnerabilities:** penetrate through defences and the attack starts
- **Gain Privilege Access:** social engineering, attacking the weakest link: human element
- This can be partly solved with regular awareness training, phishing campaigns to validate staff know-how

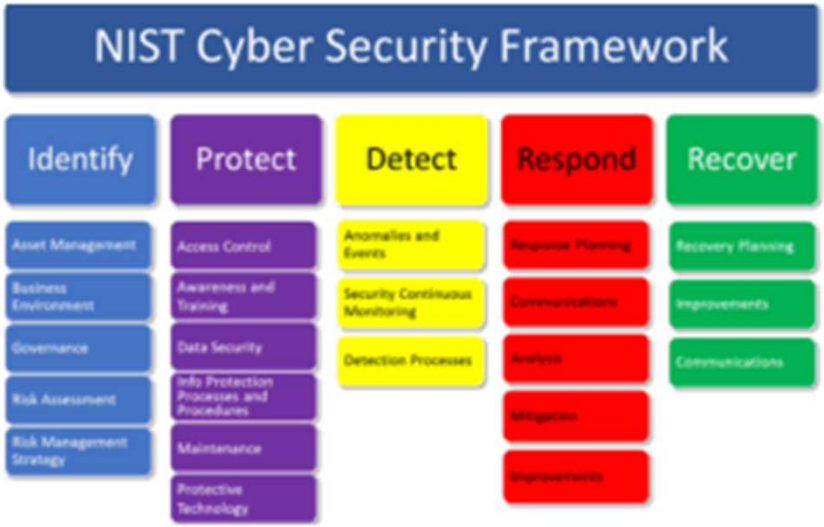


Any effective defence strategy needs to reduce this attack surface

Pragmatic Security Strategy

- **Identify**: know your assets, identify which are the critical assets, protect accordingly
  - Many online tools to finger-print network
  - Your NAS server could be a critical asset

- **Protect:**
  - End-point protected: Anti-virus and End-point Detection and Response (EDR)
  - perform regular Back-ups of critical assets
  - update systems regularly
  - implement Multi-factor Authentication, &
  - conduct regular Awareness training

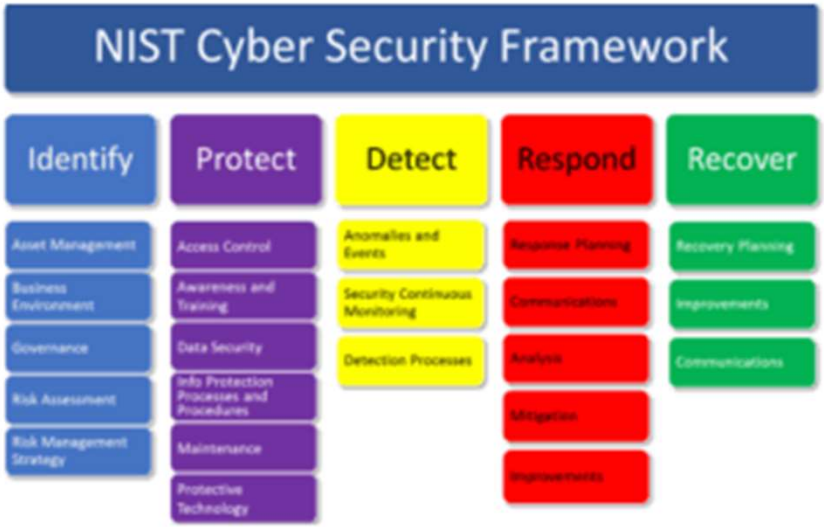


How do I get the job done?
Answer: Speak with your IT partner, these tasks should require est.10 man-days

Pragmatic Security Strategy

- **Detect:** from your security logs, suspicious events which are continuous monitored 24/7 through a Security Operations Centre (SOC) to protect against attack. Some arrangements:
  - In-house, outsourced or
  - Jointly by embed staff into provider team

- Most companies out-source or have staff embedded with their vendors as SOCs are resource and skills intensive



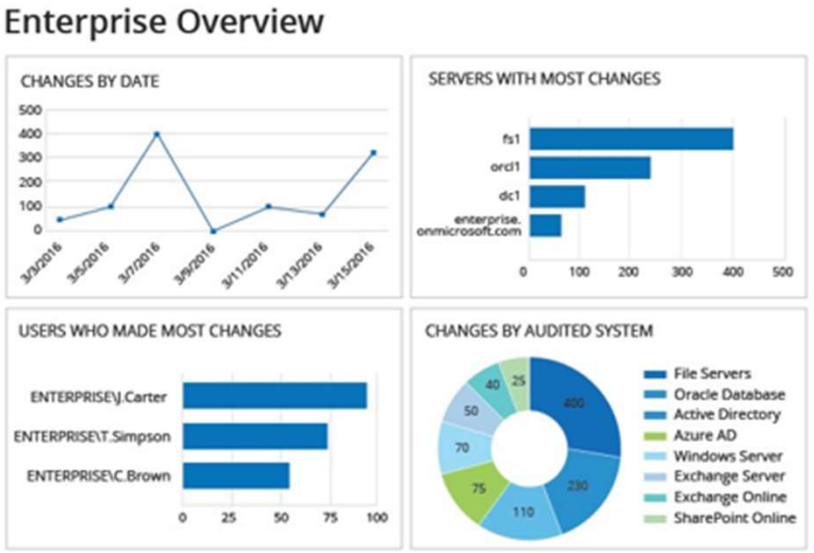
How much to spend on security?
Answer: 8% to 10% of IT budget

Security Operations Centre (SOC)

- **Managed Security Service Providers (MSSP):** typically cloud hosted to achieve economies of scale, a minimum set of security tools and who's logs are captured and analysed for attack indicators
- **Dashboards** provide management at-a-glance views to track cyber defence effectiveness and to direct resources and improve controls where needed

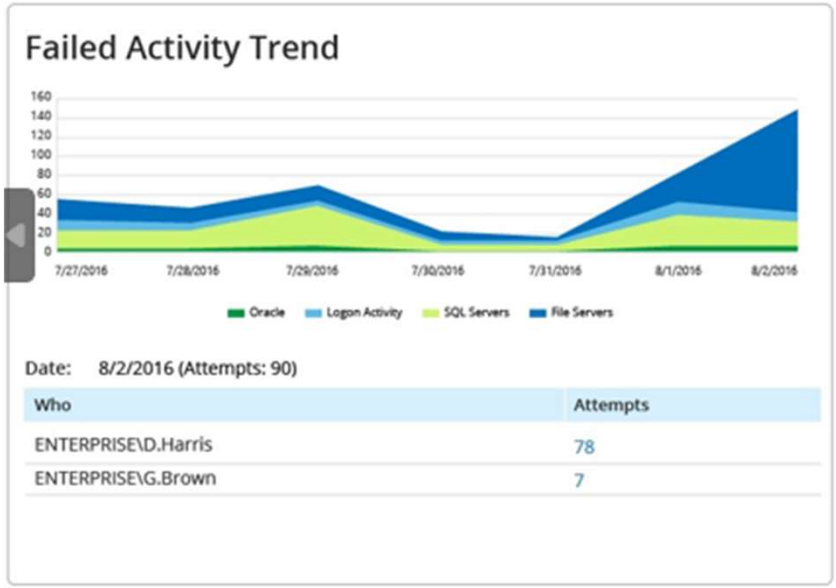
Dashboards: Enterprise View

- **Track Changes**: provide the CIO an overview of changes occurring in the infrastructure
- Helps focus attention to anomalies that suggest potential security incidents
- **Data Sources:** Critical assets such as AD, Database, Firewall, Admin activity
- E.g. Failed Login, Admin Group Member Change,



Dashboards: Importance of Trends

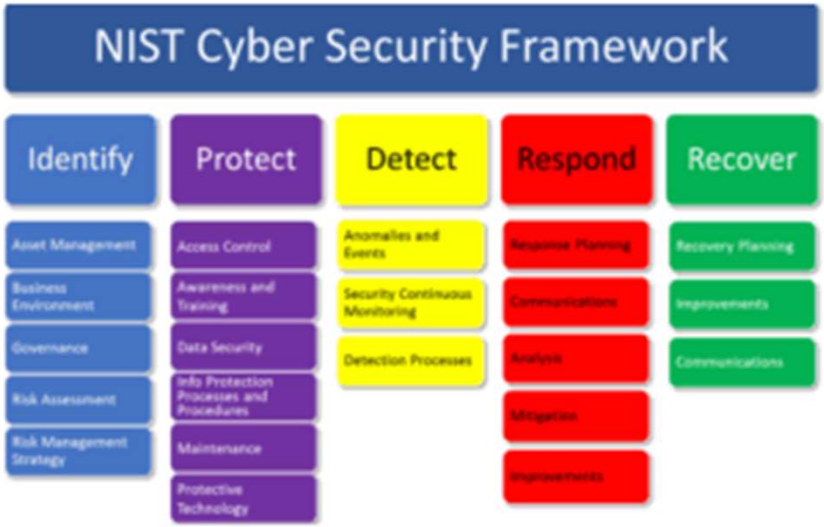
- **Trends**: power of visual representation to drive call for action
- Helps focus attention to Acceptable Levels Vs Unusual Behaviour as signs of compromise
- **Data Attributes:** Volume count, Change Time of Day, Geographic Location of Change,



These are examples, dashboard should be customized to reflect key performance indicators

Pragmatic Security Strategy

- **Respond & Recover**:
  - expect to be attacked, so its important to have a plan and exercise it regularly to protect your business and reputation
  - Run table-top exercises with external consultants or partners to test plans
  - Make sure that the recovery SOP is easily understood, such that anyone can take the SOP and execute the plan!



Summary: recap Key initiatives

- **Identify**
  - Know your assets, critical asset
- **Protect:**
  - Encrypt critical assets, e.g. NAS
  - Patch regularly
  - Implement 2FA
  - Back-up data
  - Train staff
- **Detect:**
  - Monitor for suspicious events, automate as much as possible
- **Response & Recover**
  - Recovery SOP that anyone can execute, table-top exercise

Summary

- **Business Owner, IT Managers starting on cyber journey:**
  - Start small and focus on the few important areas to protect your company,
  - Have these done properly
- **You have implemented cyber security and still getting breached:**
  - Change is always hard work
  - Ask if existing deployments can be improved walkthrough People-Process-Technology
  - Identify areas to improve and boldly implement them, e.g. upgrade Anti-virus to a AV with EDR, buy services for quicker improvements

Useful Security tools

- **Basic Health check for website and email**
  - https://ihp.csa.gov.sg/
  - Created by Singapore Agency for SMEs to perform health check. Call for Action

- **Check if you are on the hit list**
  - Sites that regularly scan for vulnerabilities that hackers check for targeted attacks
  - https://www.shodan.io/
  - https://www.shadowserver.org/

ATSOC Value Proposition

Why ATSOC

- ATSOC has been built with leading SIEM tools with strong data analytics capability. ATSOC is supported by a team with experience building SOCs for clients in Singapore Gov, Utility and Transport Agencies and Multinationals
- Automate important tasks that small IT teams struggle to perform, such as monitoring & alerting on suspicious activity, abuse of privilege accounts, resource utilization thresholds
- Summarize key indicators aligned to ISO27000 or NIST so that management and team are aligned to drive targeted improvements
- Virtual CISO advisory service available to advise management

Use Cases: Privilege Account Review

- **Challenge**: Client has no resources to review Admin activity, manager resorts to monthly sign-offs of print outs, which is an ineffective measure
- **Solved** by understanding what are unauthorised privilege account activities, **ATSOC** helps to reduce the review requirements by filtering out routine changes so that the manager need only focus on the exceptions E.g. Time of change, matching with Change Ticket, sensitive command use

Automating the review process improved control effectiveness and demonstrated management oversight.

Use Cases: Insider Threat

- **Challenge**: Insider Theft is a problem that many organizations ignore. Events such as leaking sensitive customer data, pricing, contact lists, and theft of company intellectual property and erode competitiveness and hurt the business.
- **Solved** by controlling and monitoring access to critical data defends against insider attacks, **ATSOC** helps to detect such attacks by reporting suspicious activity E.g. activation of dormant accounts database level data transfers,

Critical data needs to be access controlled and monitored for unauthorized access. Automating the monitoring and detection is essential for its protection.

Use Cases: Critical Resource Monitoring

- **Challenge**: Client has no 24/7 capability to monitor and alert Support Teams when critical resources exceed safe operating thresholds
- **Solved** by capturing in real time, performance telemetry data, and setting auto-alerts, **ATSOC's** 24/7 service keeps a constant watch on key indicators such as CPU, Memory, Storage, WAN Usage levels, and client agreed protocol to alert Support Teams to support client Service Levels

Active 24/7 monitoring of only the key resource indicators, ensure service continuity and proactive security management