

# Defensible Security Architecture

Design principles and ATT&CK

Säkerhetskryssningen 2019





# Mattias Almeflo

## The Security Engineer

2018



- **Principal Security Consultant**

2017



- **Senior Information Security Architect**
  - Specializing in military security frameworks
  - Threat driven IT-security implementations

2016



- **Team Leader | Information Security Architect**
  - Part of the founding team of Saab Cyber Security Division
- **Systems Integrator | Information Security Architect | Team Leader**
  - IT security, Systems Engineering, Team Leader

2010



- **Thesis Worker | Software Developer**
  - Databases, .NET software development

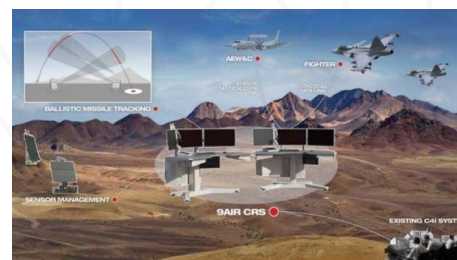
# Mattias Almeflo

## And the domains of warfare

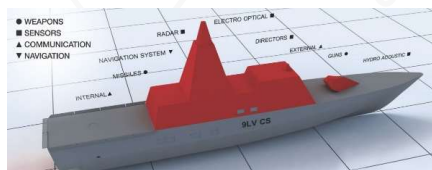
2017 –  
Development  
Environments (H/S)



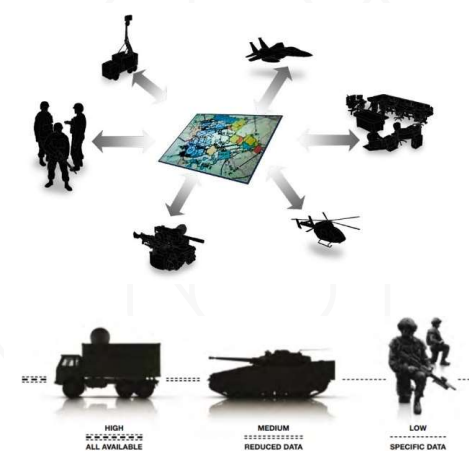
2016 – 2017: **Cyber**  
R&D Defensive Cyber Warfare



2013 – 2015: **Air**  
Windows Security in L16  
Backbone (H/S, NS)



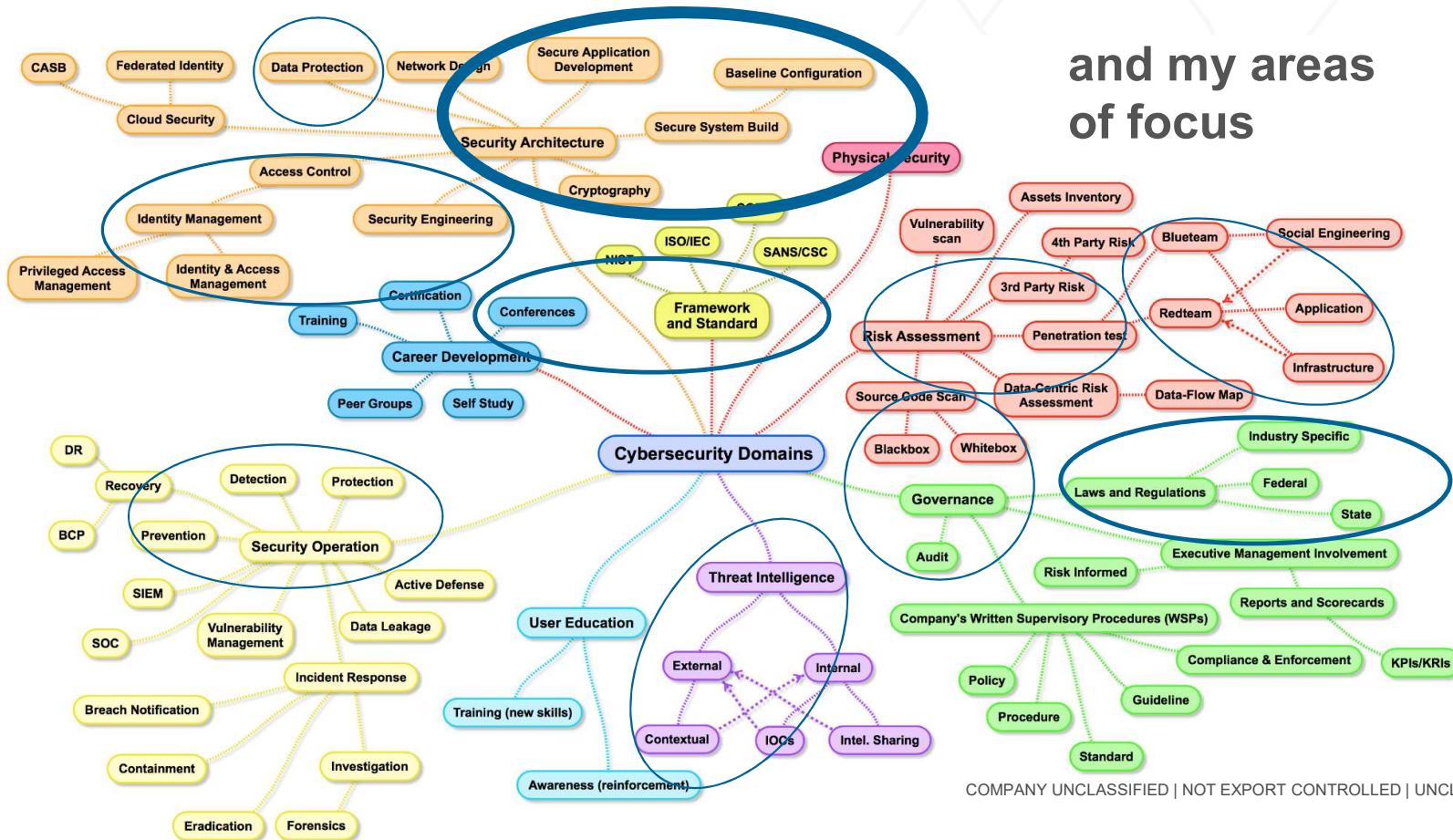
2015 – 2016: **Naval**  
Dock Security in naval  
systems (H/S)



2010 – 2013: **Land**  
Created the Secure  
Operating Environment  
(SOE) for the Swedish  
Army (H/R)

# The complexity of the domain is staggering

and my areas of focus



COMPANY UNCLASSIFIED | NOT EXPORT CONTROLLED | UNCLASSIFIED

nixu



# Trusted go-to partner for cybersecurity services

Sweden Finland

**Vision:**  
Keeping the digital  
society running



**Mission:**  
Be the best workplace for  
cyber security  
specialists



**400**  
approx

**Cyber security  
specialists**



**11**

**Locations**

Finland, Sweden,  
Netherland, US,  
Denmark  
Romania and  
Australia and more



**Cyber security services  
from board decisions to  
deep forensic investigations**



Founded in  
**1988**  
publicly listed  
**2014**



**98%**  
of our clients  
recommend Nixu

# Defensible Security Architecture

## SANS SEC530

- Traditional Security Architecture Deficiencies
- Defensible Security Architecture
- Threat, Vulnerability, and Data Flow Analysis
- Layer 1 Best Practices
- Layer 2 Best Practices
- NetFlow

# Defensible Security Architecture

SANS SEC530.1

- **Defensible Security Architecture**
  - Mindset
  - Models
  - Virtual Networking / Software-defined Networking
  - Micro-Segmentation
- **Threat, Vulnerability, and Data Flow Analysis**

# Two types of threats

## Non actor driven (not antagonistic) threat

- Possible, unwanted event with a negative outcome for operations, which isn't caused by a human actors deliberate actions.
- Generally speaking non-antagonistic threats can be divided into three categories:
  - Natural phenomena (natural disasters, disease)
  - Errors in technical systems (bugs, malfunction )
  - Non-intentional actions by human actors (accidents, negligence)



# Two types of threats

## Actor driven (antagonistic) threat

- Threat driven by an actor in the form of an individual, group, network, organisation, state etc.
- Actor driven threats are normally intentional.

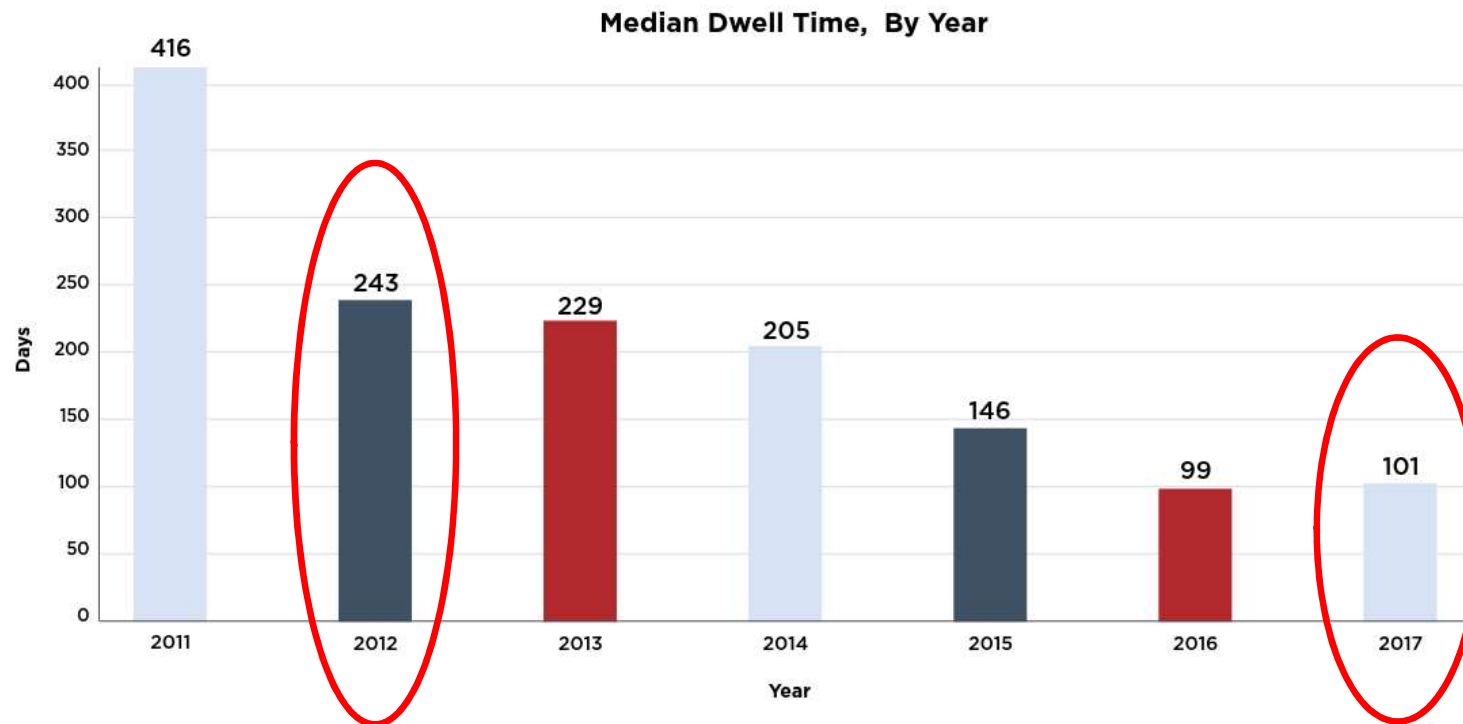
# The post-breach / “assume breach” age

"High-risk enterprises should assume that they are already compromised  
- there is no product or combination of products that provides 100% protection"

- 2012, NSS Labs Analysis,  
Brief – Cybercrime Kill Chain vs. Defense Effectiveness

# The post-breach / “assume breach” age

Dwell time – Mandiant/FireEye M-Trends 2018 report



# MITRE's “assume breach” initiative

## and the rise of the ATT&CK framework

### History:

- 2010 - researching data sources and analytic processes for detecting APTs more quickly through the use of endpoint telemetry data
- 2013 - developed a process for modeling an adversary's post-compromise behavior at a granular level. This model is named ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).
- **2015** - ATT&CK methodology is released to the world
- 2018 - The first dedicated ATT&CK conference

# ATT&CK – A more scientific way

## Adversarial Tactics, Techniques, and Common Knowledge

An empirical/curated knowledge base that helps model cyber adversaries' tactics and techniques – and then shows how to detect or stop them.

- The real hacker playbook (+200 techniques)
- Threat-informed
- Community driven
- Free



# Think like an attacker

”Think like a chef and see how well you do in the kitchen...”  
- Adam Shostack



# Threat modeling

**strategically thinking about what might go wrong**

“something you can do while preparing to deploy or build a system is to think about the threats associated with it.”

# Threat modeling

## Shostack's four questions

1. What are you deploying/building?
2. What can go wrong?
3. What are you going to do about it?
4. Did you do an acceptable job at 1-3? (For quality assurance)

# ATT&CK Matrix Use Cases

they start with the threat

- **Gap analysis** of current defences
  - Improve the security posture
- **Detection** of heavily used techniques
  - Prioritize what analysts should to look for
- **Information sharing** of observed behaviours on the network
  - Help collaboration among security teams
- **Tracking the evolution of** tactics, techniques, and procedures (TTP) over time.
  - Build adversary profiles
- **Adversary emulation**
  - More authentic red team/blue team exercises

# ATT&CK

## A moving target



John Wunder [Follow](#)

Feb 15 · 4 min read

It's been about a year since we wrote about [what was coming for ATT&CK in 2018](#)...and what a year it's been. We started from the ground up by making some big changes to ATT&CK itself, including [developing a new tactic](#) to capture how adversaries achieve [Initial Access](#). We launched a new technical infrastructure, including a [redesigned website](#) and [STIX/TAXII-based JSON API](#). We published the [ATT&CK Navigator](#) to help you visualize and explore ATT&CK, [relaunched CAR](#) to help you detect ATT&CK techniques, and conducted our first round of [ATT&CK Evaluations](#) to drive ATT&CK adoption and implementation by both vendors and end-users. We also launched this blog, with some great posts on [threat intelligence mapping](#), [finding related ATT&CK techniques](#), and [how to interpret ATT&CK Evaluation detections](#). I think I speak for the team when I say our high point was meeting so many of you in person at our first [ATT&CKcon](#).

1

NEW TACTIC

58

NEW TECHNIQUES

29

NEW GROUPS

122

NEW SOFTWARE

2018 ATT&CK Changes

# APT groups aka advance threat actors

Advanced Persistent Threat groups came to light in 2013

Currently the ATT&CK framework have 78 different threat actors in its catalogue.

## **Roughly 43% are attributed to countries**

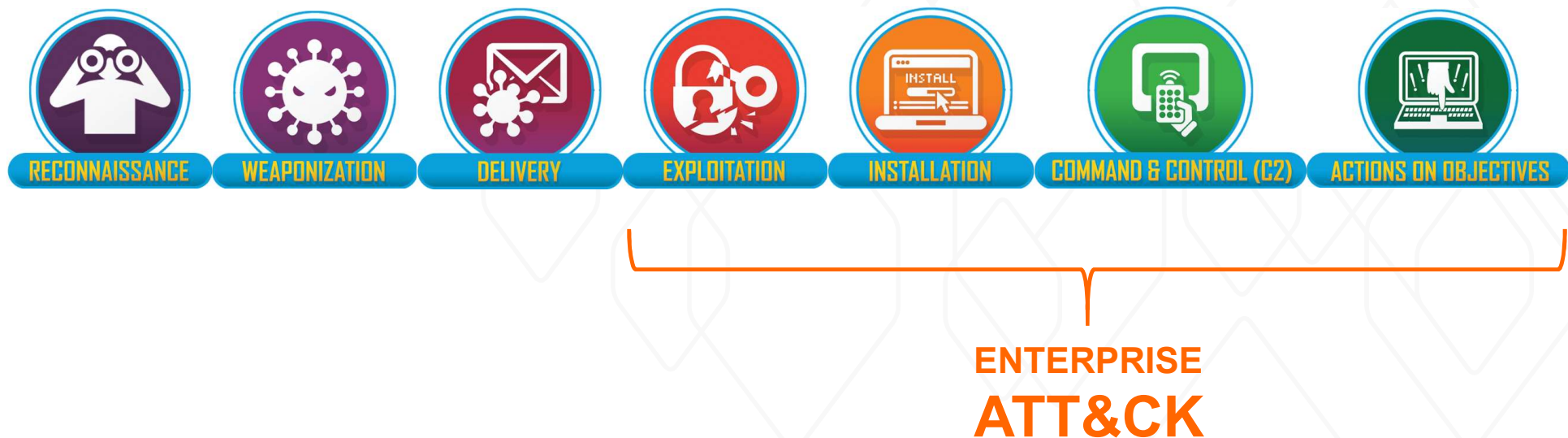
- 13 are presumed to be Chinese-based
- 12 are presumed to be Iranian-based
- 7 are presumed to be Russia-based
- 2 are presumed to be North Korea-based

# The cyber kill chain and ATT&CK

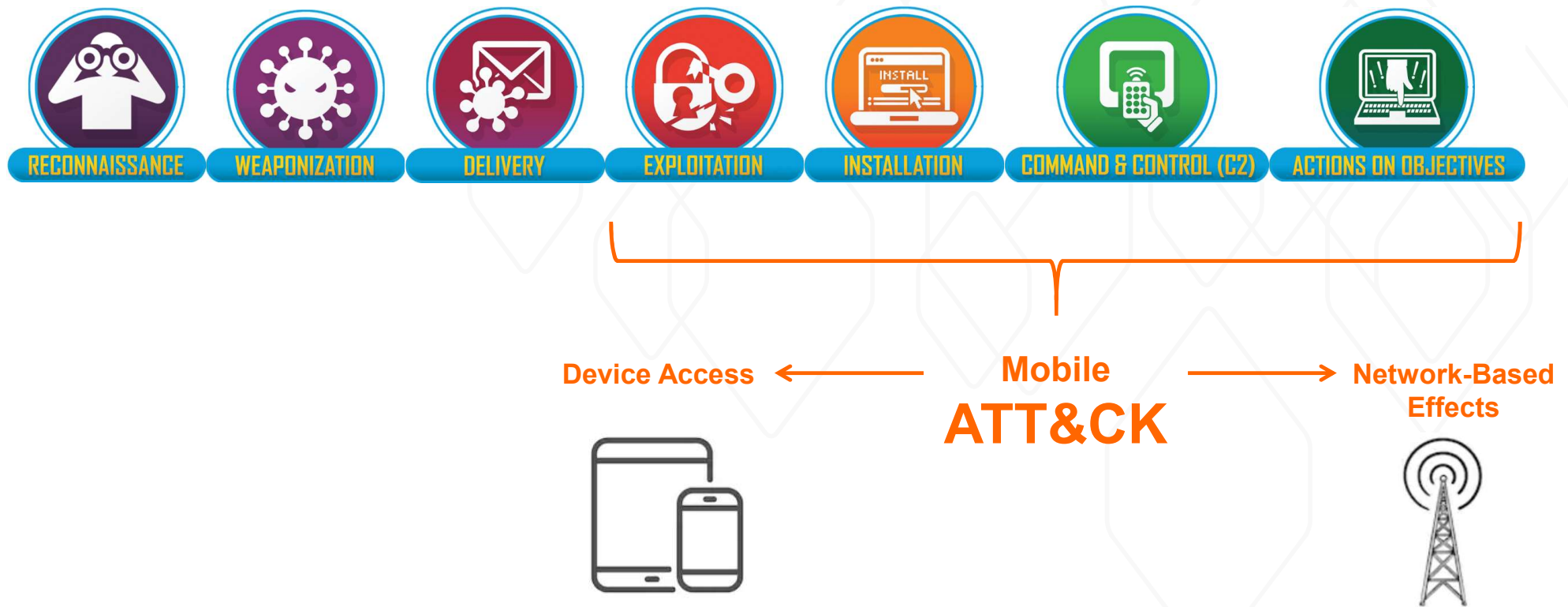




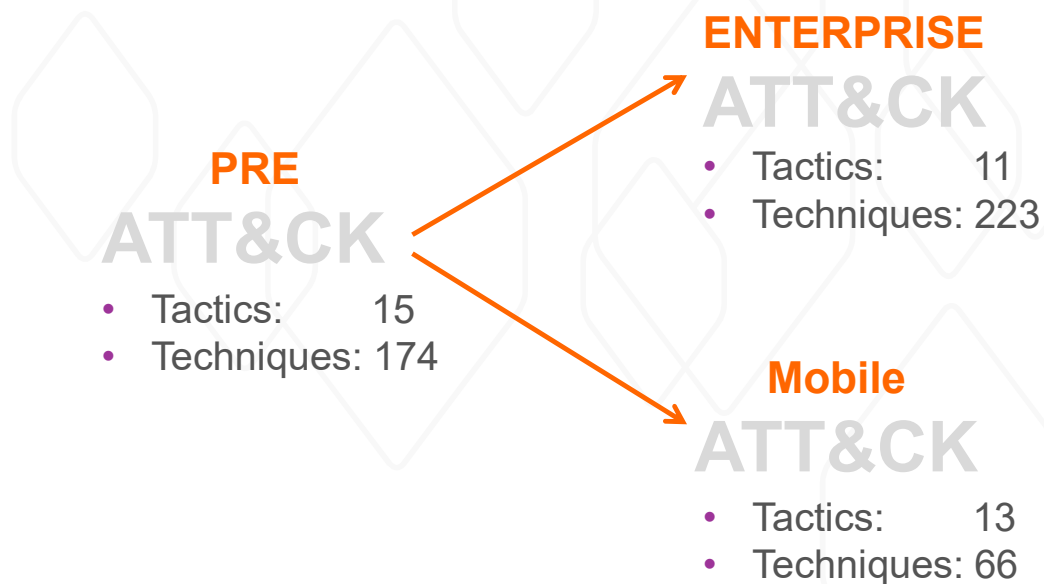
# The cyber kill chain and ATT&CK



# The cyber kill chain and ATT&CK



# The ATT&CK Matrices



# Enterprise ATT&CK focus areas (tactics)

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

**ENTERPRISE  
ATT&CK**

- Linux
- macOS
- Windows

# The post-breach / “assume breach” age

and how ATT&CK can help you leverage what you already have

1. “Think like an attacker”  
by studying their blueprints
2. Fighting the digital sleeper  
agents of modern IT-systems  
by behaviour monitoring  
through Tactics, Techniques  
and Procedures (TTP)



# The digital sleeper agents of modern IT-systems

## or the rise of Living Of the Land Binaries (LOLBins)

Living of the land binaries:

- **Authorized, trusted applications** that are used by malicious actors
- Usually never writes to disk (they are already there)
  - **Live in memory**
- **Be one with the network**
  - Use tools already in place, use protocols already used
  - (Don't talk when the network is quiet)
  - Make their infrastructure work for you



# ATT&CK - living off the land binaries (LOLBins)

or homesteading in the enterprise with fileless attacks

*“Fileless Malware Attacks on the Rise, Microsoft Says” – 2018, october*

- LOLBins have been around in the wild since 2014
- Recently experienced explosive growth
  - 52% of non-malware attacks in 2017 involved the abuse of two legitimate programs (powershell & WMI)
    - increasing at a rate of 6.8% per month

# Simple examples of TTP

## Tactics, Techniques and Procedures

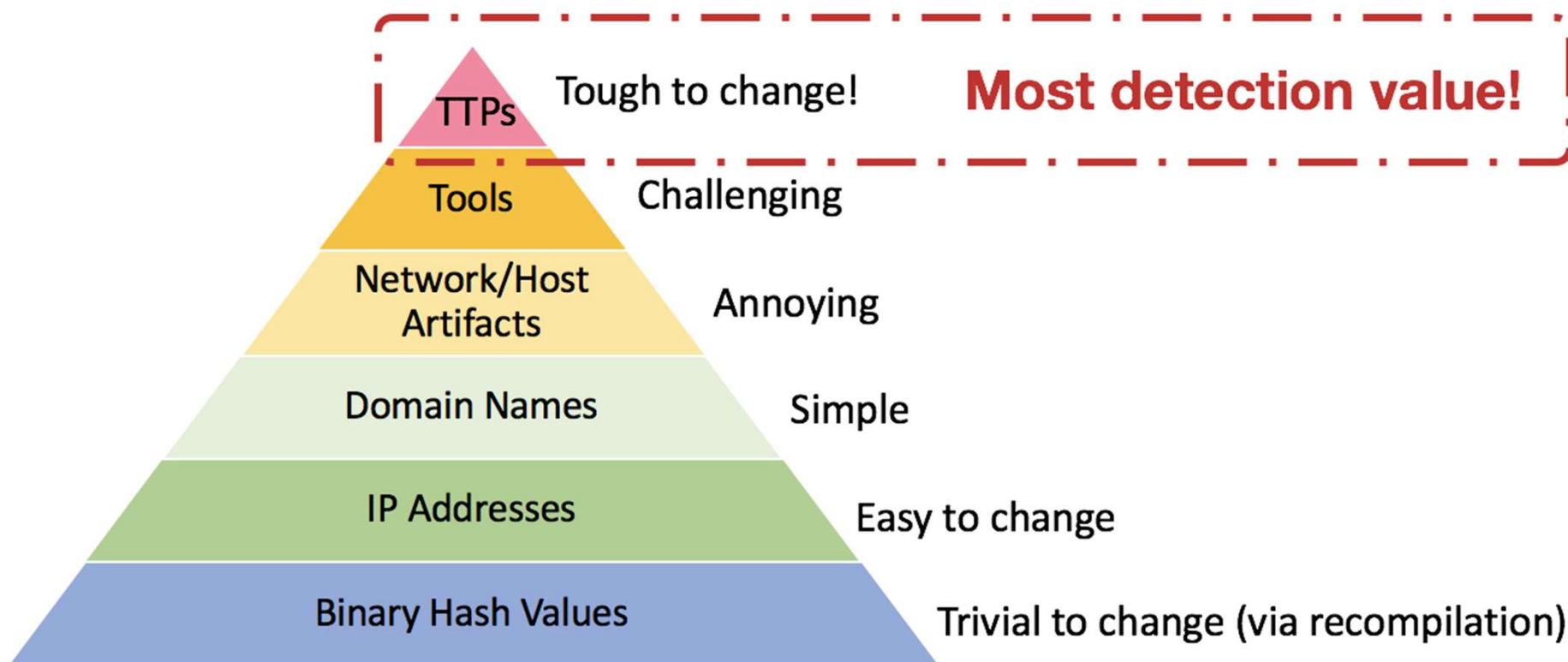
TTP in a windows environment

- “a privilege escalation via the Microsoft Connection Manager Profile Installer (CMSTP.exe) ”

Using a non-cyber analogy

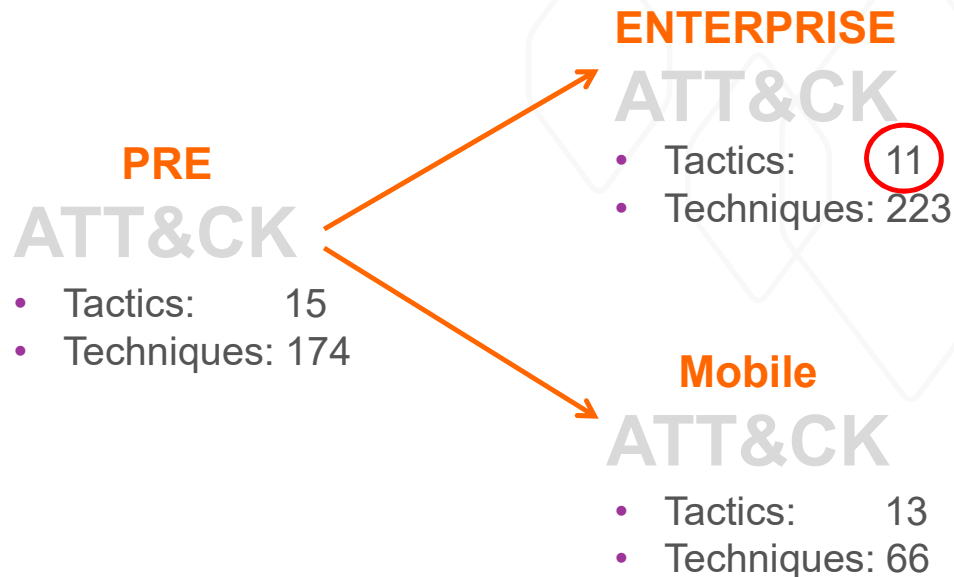
- “a specific approach to counterfeiting \$100 dollar bills can be thought of as a TTP while the specific guidance for detecting bills (wrong color, bad watermark, etc.) using this approach can be thought of as Indicators.”

# Biancos “Pyramid of Pain”



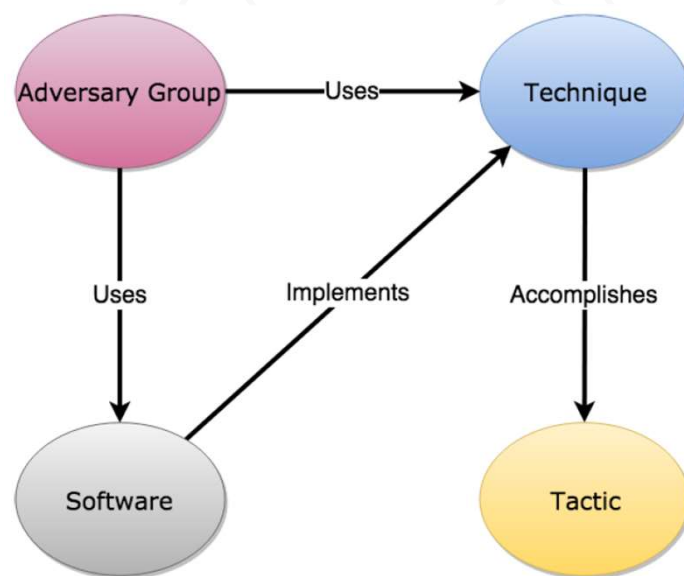
# How to start with ATT&CK

Tactics: the adversary's technical goals



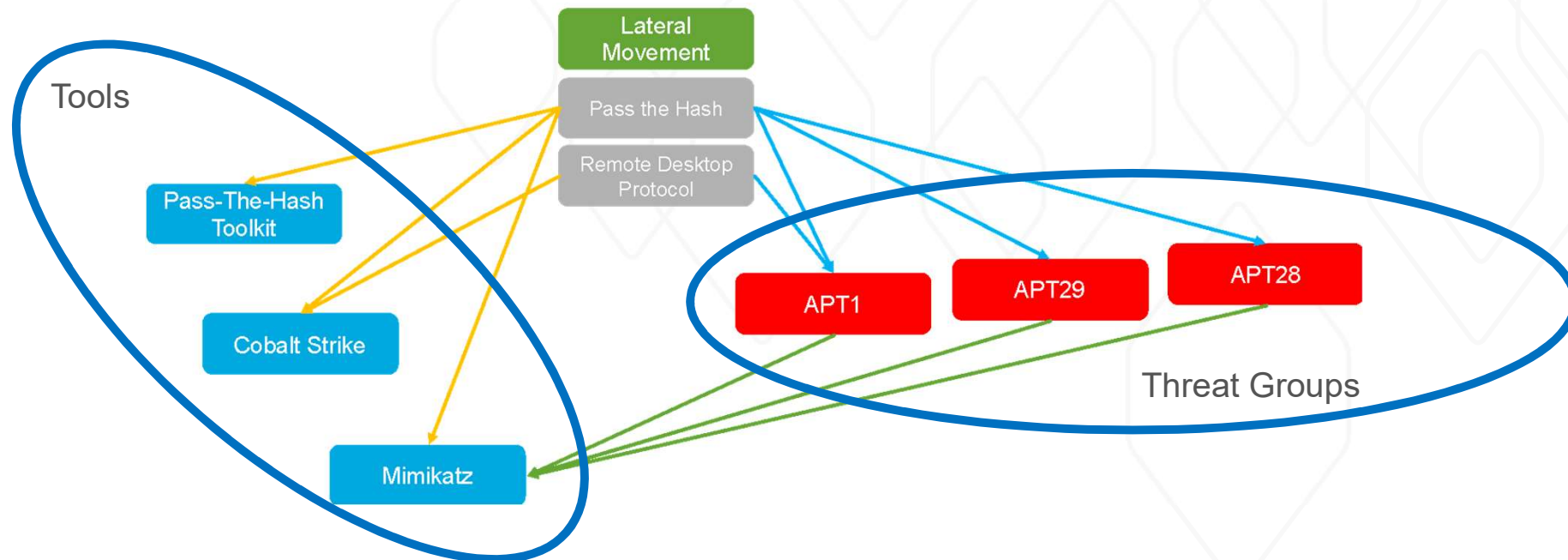
# How to start with ATT&CK

## Tactics – Techniques – Threat Groups - Tools

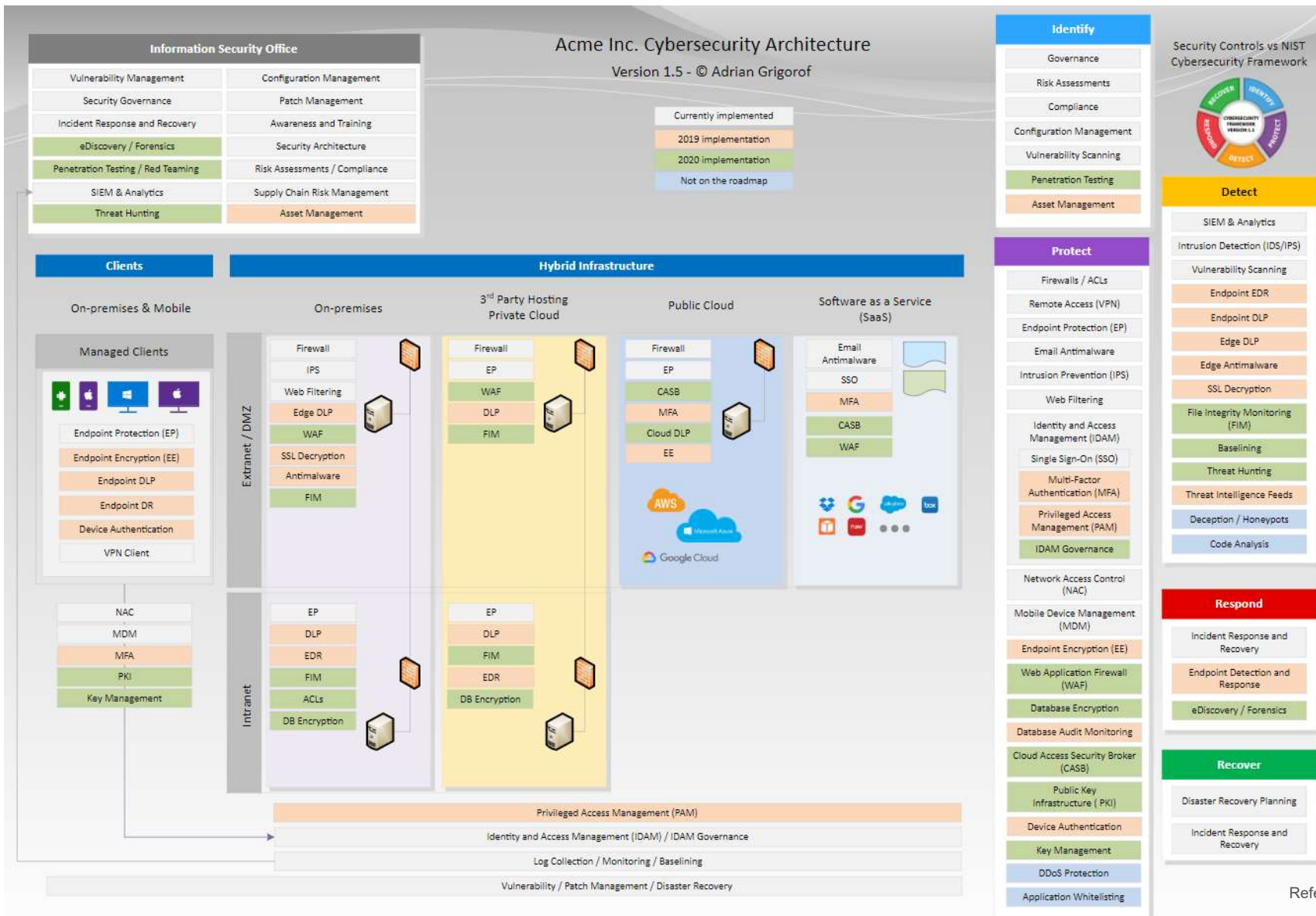


# How to start with ATT&CK

Work from tactics and break it down from there





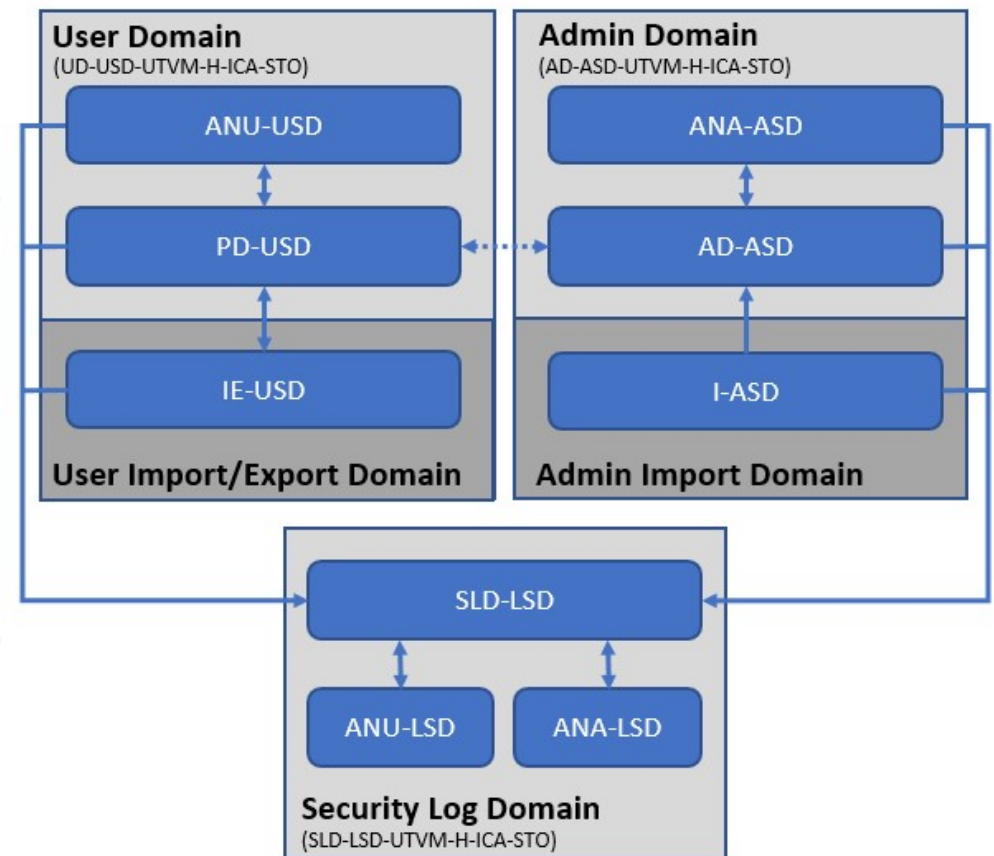


# nixu

References per slide, at the end.

# Defensible Architecture

## Separation as a security boundary



# Security Design principles

There are many sets of security design principles

They share a lot of similarities between them at a fundamental level

For defensible architecture I recommend to start with these ten (10) security design principles

# Security Design Principle

A declarative **statement**  
made with the intention of  
**guiding security design decisions**  
in order to meet the security goals of a system

# 10 design principles for defensible architecture

1. Assign the **least privilege** possible
2. Separate **responsibilities**
3. **Trust cautiously**
4. **Simplest** solution possible
5. **Audit** sensitive events
6. **Fail securely** & use **secure defaults**
7. Never rely upon **obscurity**
8. Implement **defence in depth**
9. **Never invent** security technology
10. Find the **weakest link**

# 10 design principles for defensible architecture

# 01	LEAST PRIVILEGE
Why?	Broad privileges allow malicious or accidental access to protected resources
Principle	Limit privileges to the minimum for the context
Tradeoff	Less convenient, less efficient, more complexity
Example	<ul style="list-style-type: none"><li>- Run server processes as their own users with exactly the set of privileges they require</li><li>- No root or super-admin access, ever</li></ul>

# 10 design principles for defensible architecture

# 02	SEPARATE RESPONSIBILITIES AND SYSTEM FUNCTIONS
Why?	Achieve control and accountability, limit the impact of successful attacks, make attacks less attractive
Principle	Separate and compartmentalised responsibilities, privileges and admin/user systems
Tradeoff	Development and testing costs, operational complexity, troubleshooting more difficult
Example	<ul style="list-style-type: none"><li>- System admin are separate from security log admin</li><li>- admin interfaces are not allowed to run in the same domain as user interfaces</li></ul>

# 10 design principles for defensible architecture

# 03	TRUST CAUTIOUSLY
Why?	Many security problems caused by inserting malicious intermediaries in communication paths
Principle	Assume unknown entities are untrusted, have a clear process to establish trust, validate who is connecting
Tradeoff	Operational complexity (particularly failure recovery), reliability, some development overhead. Not a trivial problem...
Example	<ul style="list-style-type: none"><li>- Two-way-authentication (client – server)</li><li>- Two-factor authentication for user auth</li><li>- Only use trusted PKI that you control</li><li>- Never share underlying HW for VMs in different sec. domains</li></ul>



# 10 design principles for defensible architecture

# 04	SIMPLEST SOLUTION POSSIBLE
Why?	Security requires understanding of the design – complex design is rarely understood – simplicity allows analysis.
Principle	Actively design for simplicity – avoid complex failure modes, implicit behaviour, unnecessary features...
Tradeoff	Hard decisions on features and sophistication. Needs serious design effort to be simple.
Example	<ul style="list-style-type: none"><li>- Fixed configuration (defined configuration as in CIS Benchmarks)</li><li>- Hardening (minimize attack surface) in terms of no unused services</li></ul>

"The price of reliability is the pursuit of the utmost simplicity"

– C.A.R. Hoare

# 10 design principles for defensible architecture

# 05	AUDIT & ANALYZE SENSITIVE EVENTS
Why?	Provide record of activity, deter wrong doing, provide a log to reconstruct the past, provide a monitoring point
Principle	Record all security significant events in a tamper-resistant store
Tradeoff	Performance, operational complexity, development cost
Example	<ul style="list-style-type: none"><li>- Record all unsuccessful login attempts, IPS/IDS events of relevance</li><li>- Use a data-diod in order to safe guard the security logs</li></ul>

# 10 design principles for defensible architecture

# 06	FAIL SECURELY & USE SECURE DEFAULTS
Why?	Default passwords, ports & rules are "open doors" Failure and restart states often default to "insecure"
Principle	Force changes to security sensitive parameters Think through failures – must be secure but recoverable
Tradeoff	Convenience
Example	<ul style="list-style-type: none"><li>- On failure don't disable or reset security controls</li><li>- Don't allow default accounts with default passwords</li></ul>

# 10 design principles for defensible architecture

# 07	NEVER RELY ON OBSCURITY
Why?	Hiding things is difficult – someone is going to find them, accidental if not on purpose
Principle	Assume attacker with perfect knowledge, this forces secure system design
Tradeoff	Designing a truly secure system takes time and effort
Example	<ul style="list-style-type: none"><li>- Use reputable crypto</li><li>- Assume that an attacker will be able to guess password encodings, port knocking etc</li></ul>

# 10 design principles for defensible architecture

# 08	DEFENCE IN DEPTH
Why?	System do get attacked, breaches do happen, mistakes are made – need to minimise the impact
Principle	Don't rely on a single point of security, secure every level, vary mechanisms, stop failures at one level propagating
Tradeoff	Redundancy of policy, complex permissioning and troubleshooting, can make recovery harder
Example	<ul style="list-style-type: none"><li>- Access control in UI, services, database, OS</li><li>- Multiple layers of authentication (HW, SW, Users)</li></ul>

# 10 design principles for defensible architecture

# 09	NEVER INVENT SECURITY TECHNOLOGY
Why?	Security technology is difficult to create – specialist job, avoiding vulnerabilities is difficult
Principle	Don't create your own security technology Always use a proven component
Tradeoff	Time to assess security technology, effort to learning it, complexity
Example	- Don't invent your own SSO mechanism, secret storage or crypto libraries. Use industry standards!

# 10 design principles for defensible architecture

# 10	SECURE THE WEAKEST LINK
Why?	"Paper Wall" problem – common when focus is on technologies not threats
Principle	Find the weakest link in the security chain and strengthen it – repeat! (Threat modelling)
Tradeoff	Significant effort required, often reveals problems at the least convenient moment
Example	<ul style="list-style-type: none"><li>- Data privacy threat met with encrypted communication but with unencrypted database storage and backups</li></ul>

# The Force Multipliers

## Technical Controls

- Strong authentication (two factor: smart cards, yubikey, sms etc)
- Separation (physical and logical)
- Security logging
- White listening
- SANS/CIS 20 Critical Security Controls



# The Force Multipliers

## Engineering

- Know your network
  - Documentation vs Implementation
- Threat modeling
  - Crown Jewels
- Think in graphs
  - Not everything is equal

# Strong authentication

**One of the few good security measures, every time!**

## Out of band authentication

- Civilian: Sms, google authenticator, mobile bank-ID
- Military: Smart cards with external num-pads

## In band authentication with physical token

- Smart cards
- Yubikeys

# Separation (physical and logical)

Separation of

- duties
- user space / kernel space
- admin console / user console
- Infrastructure management / operational management

Physical separation holds

- No virtual overlap between domains

# Security logging

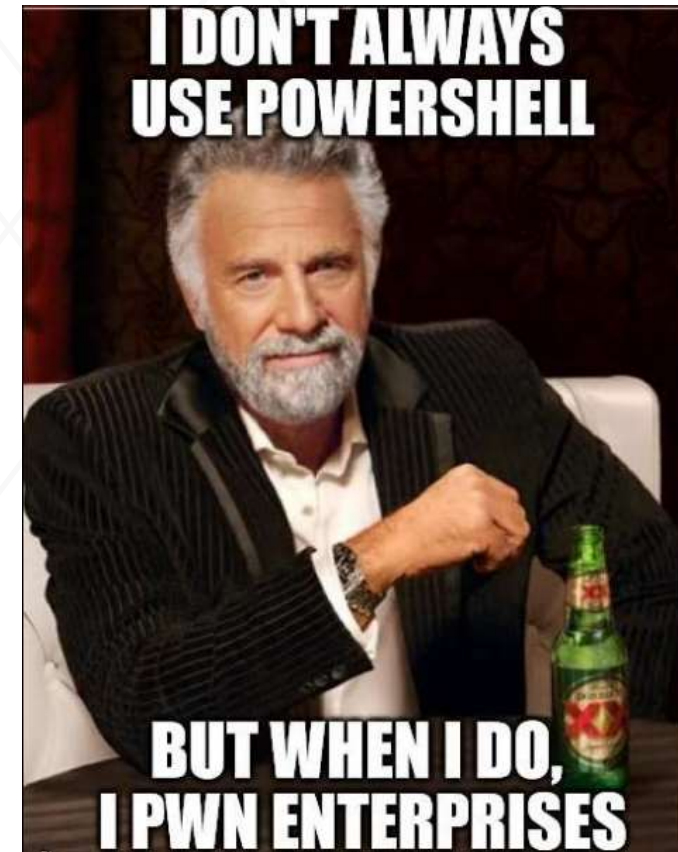
Do you even know what to log in your systems?

- Information flow diagrams
- Who's watching the results?
  - Automatic analysis
  - Manual analysis
- How do you protect your logs?
- How do you handle incident response?

# White listening

Most popular operating systems (Windows, Linux, etc.) have some sort of “deny-by-default” technology built into it:

- **Windows** has AppLocker
- In newer versions of **Linux**, using the integrity measurement architecture, module signing, and Secure Boot, it's possible to have a system where almost any change is detected. Also selinux 😊
- **NetBSD** has the Veriexec subsystem



# Graphs vs lists



Jackie Stokes  
@find\_evil

Följ

"Attackers think in graphs. Defenders think in lists." --@redteamwrangler #bsidesAugusta

RETWEET

1

GILLADE

6



08:48 - 10 sep. 2016



1



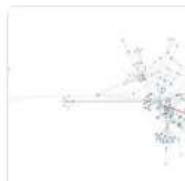
6



John Lambert  
@JohnLaTwC

Följ

@markrussinovich @melvynadam You can read more here:



**Defenders think in lists. Attackers think in graphs. As long...**

Defender Mindset A lot of network defense goes wrong before any contact with an adversary, starting with how defenders conceive of the battlefield. Most defenders focus on protecting their asse...  
[blogs.technet.microsoft.com](https://blogs.technet.microsoft.com)

RETWEETS

3

GILLADE

8

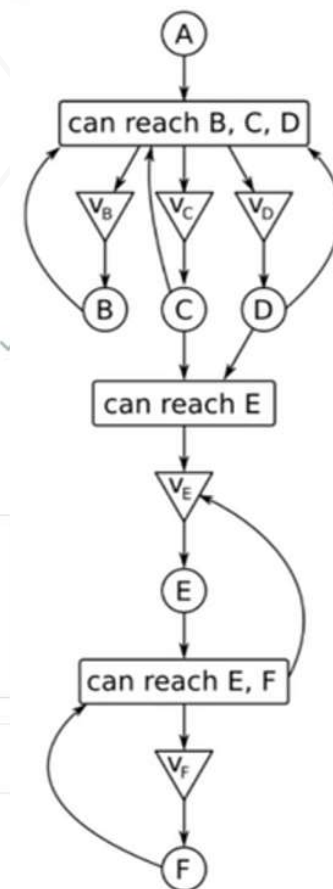


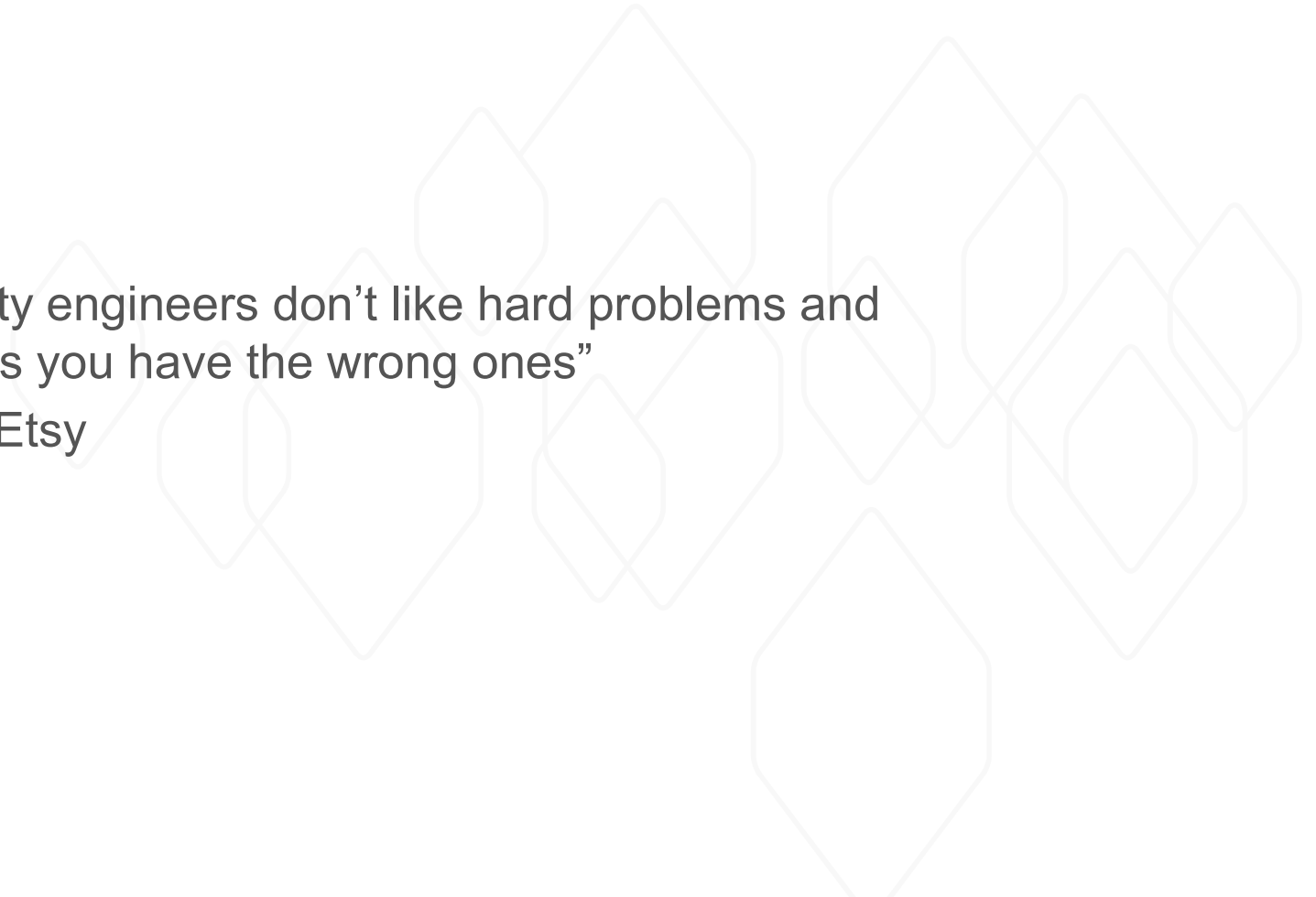
11:05 - 24 jan. 2017

1

3

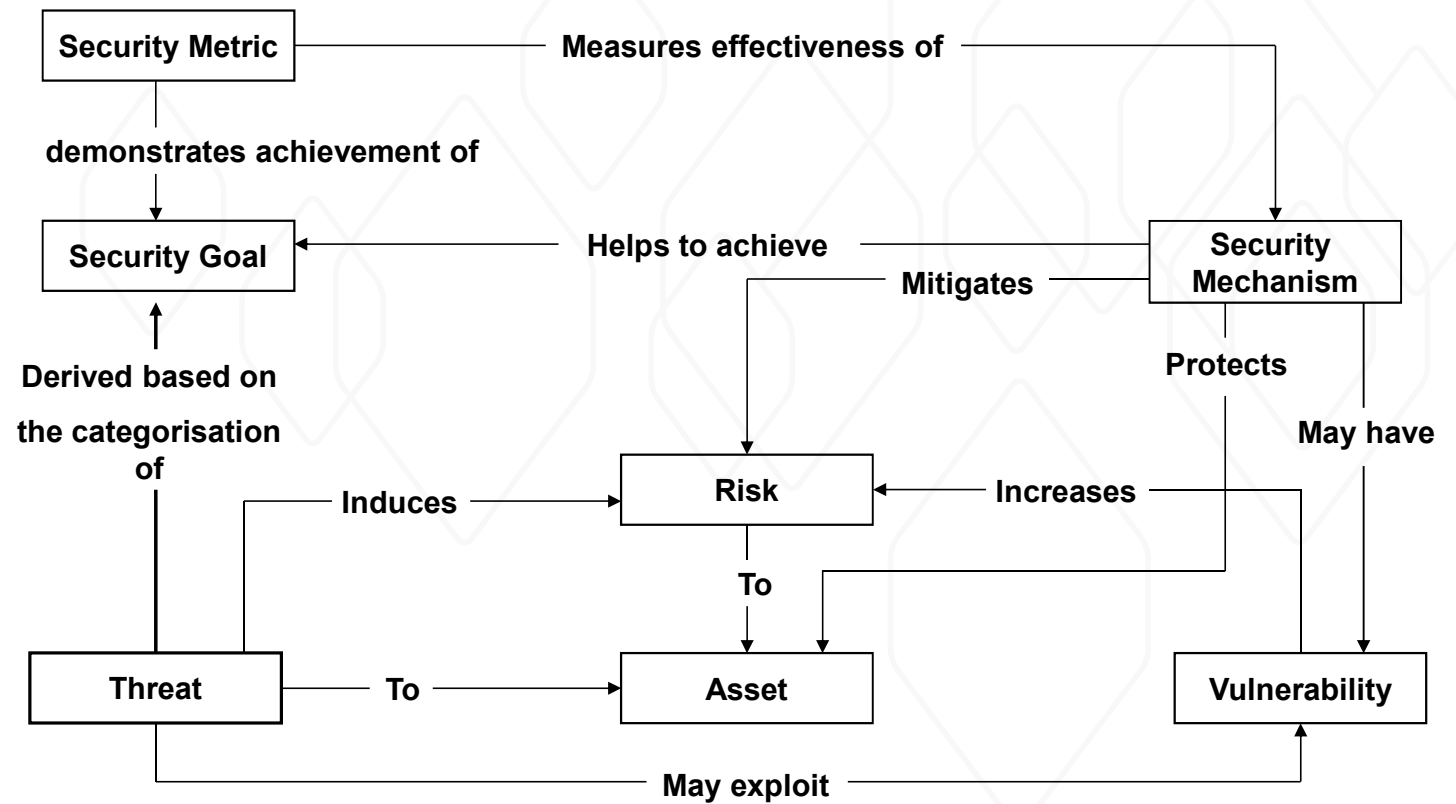
8





”If your security engineers don’t like hard problems and novel solutions you have the wrong ones”  
- Rich Smith, Etsy

# The security goal flow chart





# Credits and prior art 1/7

"discovering truth by building on previous discoveries"

## Me, Myself & I

S02-05: Saab, the corporation video (6 min) - <https://www.youtube.com/watch?v=2KsdPHsgR9Q>

S02-05: The domains of war - <https://saab.com/land/>, <https://saab.com/air/>, <https://saab.com/naval/>, <https://en.wikipedia.org/wiki/Cyberwarfare>

S02-05: LinkedIn Cyber Security Domain Map - <https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp>

S02-05: Nixu Oy at 600Minutes Information and Cyber Security 2017 (Spotlight) - This is Nixu - <https://www.youtube.com/watch?v=pwIIJnZ8pHo>

## SANS SEC530 – Defensible Security Architecture

S06-07: <https://www.sans.org/course/defensible-security-architecture-and-engineering>

## Två typer av hot

S08-09: Aktörsdrivet vs icke aktörsdrivet hot

H SÄK Grunder, 2013 - <https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/handbocker/h-sak-grunder.pdf>

IT-Säkerhetsarkitektur, 2015 - <https://www.svk.se/siteassets/aktorsportalen/sakerhetsskydd/dokument/vagledning-it-sakerhetsarkitektur-final.pdf>

## The Post-Breach Age - Quote

S10: Cybercrime Kill Chain vs. Defense Effectiveness - [https://www.researchgate.net/publication/258112939\\_Cybercrime\\_Kill\\_Chain\\_vs\\_Defense\\_Effectiveness](https://www.researchgate.net/publication/258112939_Cybercrime_Kill_Chain_vs_Defense_Effectiveness)

S10: Conference: Proceedings des 13. Deutschen Sicherheitskongress des BSI –

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/ITSiKongress/13ter/Stefan\\_Frei\\_16052013.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/ITSiKongress/13ter/Stefan_Frei_16052013.pdf)

# Credits and prior art 2/7

"discovering truth by building on previous discoveries"

## **The Post-Breach Age - Mandiant/FireEye M-Trends 2018 report**

S11: Mandiant/FireEye M-Trends report - <https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf>

## **MITRE's "assume breach" initiative**

S12: Finding Cyber Threats with ATT&CK™-Based Analytics –

<https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf>

S12: ATT&CK web page - <https://attack.mitre.org>

S12: ATT&CK conference 2018 - <https://www.mitre.org/attackcon>

## **ATT&CK – A more scientific way**

S13: A short animated video about MITRE ATT&CK™ Framework - <https://www.youtube.com/watch?v=0BEf6s1iu5g>

S13: Science – It is the answer - <https://www.deviantart.com/dormantflame/art/Because-Science-390410617>

S13: The full ATT&CK Matrix - <https://attack.mitre.org/matrices/enterprise/>

S13: 3 minutes on MITRE ATT&CK - <https://www.rapid7.com/resources/3-minutes-on-mitre-attack>

## **Threat modeling**

S14-15: Threat Modeling 101: Ten Common Traps Not to Fall Into

<https://www.tripwire.com/state-of-security/security-data-protection/threat-modeling-10-common-traps-you-dont-want-to-fall-into/>

S14-15: Threat Modeling: Designing for Security (624 pages)

<https://www.amazon.com/Threat-Modeling-Designing-Adam-Shostack/dp/1118809998?tag=viglink12354-20>

# Credits and prior art 3/7

"discovering truth by building on previous discoveries"

## **ATT&CK Matrix Use Cases**

S16: The MITRE ATT&CK Framework – A Sign of the Times - <https://www.threatq.com/mitre-attck-framework-blog/>

## **ATT&CK – A Moving target**

S17: ATT&CKing 2019 - <https://medium.com/mitre-attack/attacking-2019-c05bccefed2d>

## **APT Groups aka advance threat actors**

S18: ATT&CK Groups: <https://attack.mitre.org/groups/>

S18: The famous Mandiant/Fireeye report about APT1 (2013, Nov) - <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>

“Since 2006, Mandiant has observed APT1 compromise 141 companies spanning 20 major industries”

S18: 2013 Report to Congress of the U.S. – China Economic and Security review commission –

[https://www.uscc.gov/sites/default/files/annual\\_reports/Complete%202013%20Annual%20Report.PDF](https://www.uscc.gov/sites/default/files/annual_reports/Complete%202013%20Annual%20Report.PDF)

## **The cyber kill chain and ATT&CK**

S19-21: TripWire, Defend Your Data Now with the MITRE ATT&CK Framework - <https://www.youtube.com/watch?v=io4vCTBLa78>

Slides - <https://www.slideshare.net/Tripwire/defend-your-data-now-with-the-mitre-attck-framework>

## **The ATT&CK Matrices**

S22: <https://attack.mitre.org/techniques/enterprise/>

S22: <https://attack.mitre.org/tactics/enterprise/>

# Credits and prior art 4/7

"discovering truth by building on previous discoveries"

## **Enterprise ATT&CK focus areas (tactics)**

S23: <https://attack.mitre.org/techniques/enterprise/>

## **The post-breach / "assume breach" age and how ATT&CK can help you leverage what you already have**

S24: Image - <https://www.acsac.org/2017/workshops/icss/Otis-Alexander-ICS,%20Adversarial%20Tactics,%20Techniques.pdf>

## **The digital sleeper agents of modern systems, or the rise of LOLBins**

S25: LOLBins: Attackers Are Abusing Trusted Binaries to Target Organizations - <https://blog.barkly.com/what-are-lolbins-living-off-the-land-binaries>

## **ATT&CK and LOLBins or homesteading in the enterprise with fileless attacks**

S26: Fileless Malware Attacks on the Rise, Microsoft Says - <https://www.securityweek.com/fileless-malware-attacks-rise-microsoft-says>

S26: Carbon Black 2017 Threat Report -

<https://www.carbonblack.com/wp-content/uploads/2018/01/CB-Thread-Report-2017-122117.pdf>

S26: DerbyCon 3.0 Living Off The Land A Minimalists Guide To Windows Post Exploitation - <https://youtu.be/j-r6UonEkUw>

## **Simple examples of TTP**

S27: TTP vs Indicator: A simple usage overview - <https://stixproject.github.io/documentation/concepts/ttp-vs-indicator/>

S27: IOCs vs. TTPs - <https://azeria-labs.com/iocs-vs-ttps/>

# Credits and prior art 5/7

"discovering truth by building on previous discoveries"

## **Biancos "Pyramid of Pain"**

S28: The Pyramid of Pain - <http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>

S28: Employing the MITRE ATT&CK Matrix to Build and Validate Cybersecurity Mechanisms –  
<https://www.apriorit.com/dev-blog/582-employing-the-mitre-att-ck-matrix>

## **How to start with ATT&CK – Enterprise Tactics**

S29: Enterprise Tactics - <https://attack.mitre.org/tactics/enterprise/>

## **How to start with ATT&CK - Tactics – Techniques – Threat Groups - Tools**

S30: ATT&CK Object Model Relationships - <https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy>

## **How to start with ATT&CK - Work from tactics and break it down from there**

S31: relationships between Tactics, Techniques, Software and Adversary Groups –  
<https://www.splunk.com/blog/2019/01/15/att-ck-ing-the-adversary-episode-1-a-new-hope.html>

## **One page security architecture**

S32: [http://www.firegenanalytics.com/downloads/one\\_page\\_security\\_architecture\\_v1.svg](http://www.firegenanalytics.com/downloads/one_page_security_architecture_v1.svg)

## **Separation as a security boundary**

S33: <https://www.zdnet.com/article/microsoft-recommends-using-a-separate-device-for-administrative-tasks/>

# Credits and prior art 6/7

"discovering truth by building on previous discoveries"

## Security Design principles

S34-S46: GOTO 2016, Secure by Design – the Architect's Guide to Security Design Principles - <https://www.youtube.com/watch?v=4qN3JBGd1g8>

## The Force Multipliers - Technical Controls & Engineering

S48: Strong Authentication - [https://en.wikipedia.org/wiki/Strong\\_authentication](https://en.wikipedia.org/wiki/Strong_authentication)

S48: Pass-the-hash attacks: Tools and Mitigation (53 pages)

- <https://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283>

S48: YubiKey - <https://en.wikipedia.org/wiki/YubiKey>

S48: Smart Card - [https://en.wikipedia.org/wiki/Smart\\_card](https://en.wikipedia.org/wiki/Smart_card)

S48: Google Authenticator - [https://en.wikipedia.org/wiki/Google\\_Authenticator](https://en.wikipedia.org/wiki/Google_Authenticator)

S50: Security logging, DCShadow - <https://attack.mitre.org/techniques/T1207/>

S50: Security logging, BlueHat IL 2018 - Vincent Le Toux & Benjamin Delpy - What Can Make Your Million Dollar SIEM Go Blind - <https://youtu.be/KILnU4FhQbc>

S47: Separation, DEF CON 24 - Beyond the MCSE: Red Teaming Active Directory video (64 min)

- <https://www.youtube.com/watch?v=tEfwMReo1Hk>

S47: Separation, GOTO 2016 • Microservices at Netflix Scale: Principles, Tradeoffs & Lessons Learned • R. Meshenberg video (49 min)

- <https://www.youtube.com/watch?v=57UK46qfBLY>

S51: Top 10 Common Misconceptions About Application Whitelisting

- <http://resources.infosecinstitute.com/top-10-common-misconceptions-application-whitelisting/#gref>

S47: CIS Critical Security Controls v6.0 (2 pages) - <https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf>

S47: CIS Critical Security Controls - <https://www.sans.org/critical-security-controls>

S47: Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.

- <https://blogs.technet.microsoft.com/johnla/2015/04/26/defenders-think-in-lists-attackers-think-in-graphs-as-long-as-this-is-true-attackers-win/>

# Credits and prior art 7/7

"discovering truth by building on previous discoveries"

## The security goal flow chart

S54: The Evolution of Information Security Goals from the 1960s to today (30 slides)

<http://users.cs.cf.ac.uk/Y.V.Cherdantseva/LectureEvolutionInfoSecGOALS.pdf>

===== Other stuff =====

**A crash course in cyber, by [halvarflake](https://twitter.com/halvarflake) (<https://twitter.com/halvarflake/status/1126813939499773953>):**

[https://docs.google.com/presentation/d/1FGjvcmlWfHfIIEdr\\_khJFeSsLAYR-Up0GHXtTCsM/edit#slide=id.p](https://docs.google.com/presentation/d/1FGjvcmlWfHfIIEdr_khJFeSsLAYR-Up0GHXtTCsM/edit#slide=id.p)

## Books you should read that might have been mentioned but aren't represented by a slide:

- Site Reliability Engineering, How Google Runs Production Systems (552 pages) - <http://shop.oreilly.com/product/0636920041528.do>
- Vem kan man lita på?: den globala övervakningens framväxt (304 pages) - <http://www.adlibris.com/se/bok/vem-kan-man-lita-pa-den-globala-overvakningens-framvaxt-9789175453958>
- Konsten att gissa rätt - Underrättelsevetenskapens grunder (218 pages) - <https://www.adlibris.com/se/bok/konsten-att-gissa-ratt---underrattelsevetenskapens-grunder-9789144004389>
- The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age (384 pages) - <https://www.amazon.com/Perfect-Weapon-Sabotage-Fear-Cyber/dp/0451497899>



Mattias Almeflo

+46 702 89 83 92

[mattias.almeflo@nixu.com](mailto:mattias.almeflo@nixu.com)

[nixuoy](#)

[@nixutigerteam](#)

[company/nixu-oy](#)

[nixu.com](http://nixu.com)



**nixu**