

Security Strategy and Program Antipatterns

Common mistakes that increase organizational risk and friction



Security blamestorming

Focusing blame for security incidents instead of partnering to continuously improve



Security Silo(s)

Security teams not integrated with business, technology, or acquisition teams



Department of No / Resist Trends

Ignore Cloud, DevOps, AI, Software Bill of Materials (SBOM), etc. until absolutely required



Delay Security until the end

Makes security fixes difficult, expensive, and unlikely



Context and Guidance Vacuum

People lack context on how to effectively apply security as a leaders or individual contributor



Outdated Policy

Outdated policy – static policy not keeping up with cloud/etc and difficult to change

Best Practice – Normalize Security

Make security a routine part of business and IT processes using pragmatic understanding of people, process, and technology

This workshop helps you define and rapidly improve on best practices including:

- *Align security to business priorities and risks*
- *Assign security accountability to decision makers (not subject matter experts without decision authority)*
- *Integrate security standards into acquisition and development of technology*
- *Position security as an enabler build partnership up to trusted advisor role*
- *Ensure stakeholders throughout the organization understand security context relevant to them*
- *Security is a team sport across security, technology, and business teams*

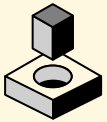
Common Security Antipatterns - Technical Architecture

Common mistakes that impede security effectiveness and increase organizational risk



Skipping basic maintenance

Skipping backups, disaster recovery exercises, and software updates/patching on assets



Securing cloud like on premises

Attempting to force on-prem controls and practices directly onto cloud resources



Wasting resources on legacy

Legacy system maintenance and costs draining ability to effectively secure business assets



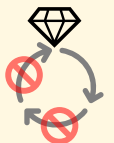
Artisan Security

Focused on custom manual solutions instead of automation and off the shelf tooling



Disconnected security approach

Independent security teams, strategies, tech, and processes for network, identity, devices, etc.



Lack of commitment to lifecycle

Treating security controls and processes as points in time instead of an ongoing lifecycle

Best Practices

Develop and implement an **end to end technical security strategy** focused on durable capabilities and Zero Trust Principles

This workshop helps you define and rapidly improve on best practices across security including:

- ***Asset-centric security*** aligned to business priorities & technical estate (beyond network perimeter)
- ***Consistent principle-driven approach*** throughout security lifecycle
- ***Pragmatic prioritization*** based on attacker motivations, behavior, and return on investment
- ***Balance investments*** between innovation and rigorous application of security maintenance/hygiene
- ***'Configure before customize'*** approach that embraces automation, innovation, and continuous improvement
- ***Security is a team sport*** across security, technology, and business teams

"We don't patch" common antipattern caused by:



'If it ain't broke, don't touch it'
*because of a fear that systems are fragile
& could easily break*

Best practice – adopt a **'patch by default'** model that assumes manufacturers invest in patches for good reason and apply them automatically (unless issues arise through phased deployment).



'I accept the risk'
*because incentives favor availability,
but don't consider organizational risk*

**Choice of downtime to apply patches on your schedule
or downtime to restore systems on the attacker's schedule**

Best practices

- **Accountability and Incentives** - Ensure business owners for systems own security maintenance and risk of neglect
- **Team approach** - Build a team approach with app and infra owners accountable to apply patches, security compliance doing independent audits, and posture management providing technical help



'We want zero downtime'
*because business/system owners carry no
accountability for security risk downtime*

Best practice – Build resiliency and patching into normal IT Operations processes (maintenance windows, image deployment, etc.) to increase reliability and digital transformation agility.



'I'm waiting for perfect patches'
*because of misperception that vendors can
provide/test perfect patches for all scenarios*

Best practice – Recognize active use by attackers and use explicit industry guidance to urgently build awareness + sponsorship with executive leaders to prioritize system maintenance



'Attacks won't happen to us'
*because it hasn't happened before
or hasn't been detected*

Common patching antipatterns to avoid



'Wait, what is that?'

Surprise vulnerabilities and incidents on unknown or unmaintained systems

Best practice – Process to continuously improve asset discovery, risk assessment, and ownership designation



IT Operating System (OS) Myopia

Focusing on only applying OS patches to servers and workstations without also addressing security configurations and other assets (containers, applications, firmware, IoT/OT devices, etc.)

Best practice – Build an end to end program that progressively address all software updates on all systems and platforms



Exposing vulnerable systems

Allowing connectivity between unpatched / unsecurable systems (IT/IoT/OT) and internet connected workstations, servers, user devices, etc.

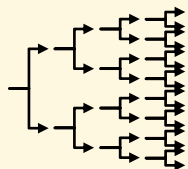
Best practice – Build an exception management policy that isolates them from internet-based risk, retires or replaces them, or updates them to be maintainable.



'We don't know what to do first'

because all systems are managed the same, results in the least secure policy everywhere

Best practices – (1) Prioritize business critical and high internet exposure systems. (2) Build exception policy and focus on both mainstream excellence + solving exceptions



Custom Builds from Random Patches

Unique criteria for choosing patches effectively creates custom builds that don't reflect current versions tested by vendors

Best practices – (1) Prioritize when to apply patches (not whether) by active exploitation and other risk factors
(2) Fully catch up on all patches regularly to stay on tested/supported build configuration

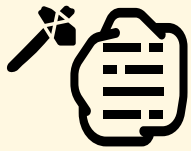
Common Access Management antipatterns

Common mistakes increase organizational risk and friction



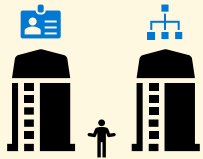
Network-Centric Castles

Focusing on protecting 'the network' instead of the business assets (asset centricity)



Outdated Best Practices

Focusing on former best practices (strong passwords, rotating passwords, etc.)



Silo'd Access Controls

Independent teams, strategies, processes, and technologies for network, identity, and others



Nest of Complexity

Access policies and firewall rules are beyond the capacity of any human to understand



Skipping Security Best Practices

Giving attackers opportunities via vulnerabilities in software, configuration, & operational practices



Hairpin Cloud Traffic

Damage user experience and drive Shadow IT by re-routing all cloud traffic through network

Best Practice – Integrated Strategy

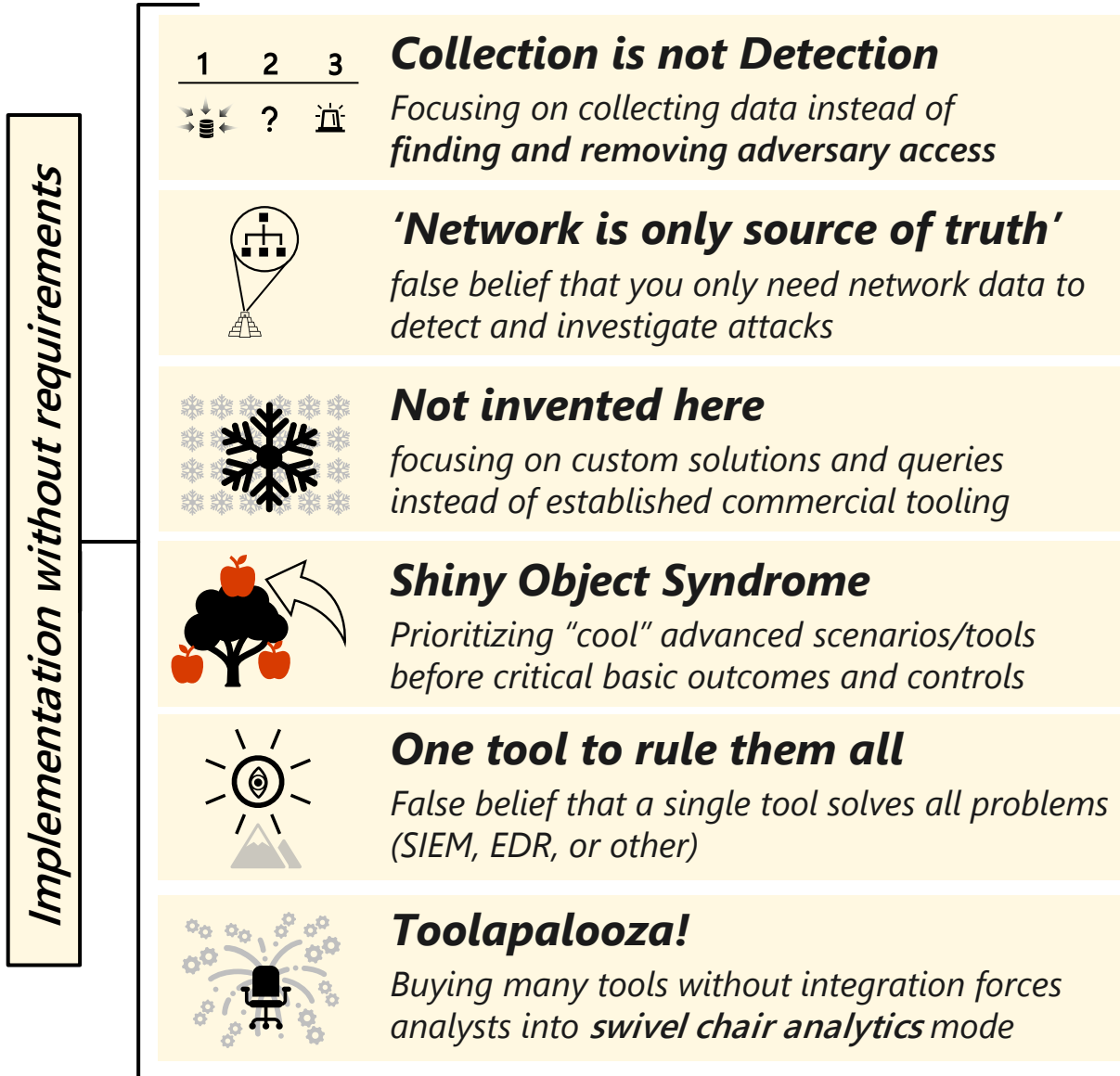
Build and implement a unified access management strategy

This workshop helps you define and rapidly improve on best practices including:

- **Access Management is a team sport** across identity and networking (+ technology, security, and business teams)
- **Stay Current** - Keep up with continuously evolving threats, identity standards, and business requirements
- **Simplicity and Consistency** – Integrated all access controls (identity, networking, applications, etc.) to provide good user experience and consistent policy enforcement across all access paths and technologies
- **'Configure before customize'** Embrace cloud and off the shelf solutions (using custom solutions as last resort)
- **Zero Trust** - Asset-centric adaptive access approach to enable and secure resources on any network using real-time threat data, rich context, and multiple policy enforcement points (network, identity, apps, data, devices, & more)

Common Security Operations (SecOps/SOC) antipatterns

Common mistakes impede SecOps effectiveness and increase burnout



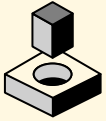
Best practice – Develop and implement a Security Operations (SecOps/SOC) strategy focused on clear outcomes across people, process, and technology

This workshop includes references to help you define and rapidly improve:

- *Mission and Metrics*
- *Organizational Functions and Teams (including use cases and scenarios)*
- *Business and Technical processes*
- *SOC Architecture, Tooling, and Integration*
- *Skill education and enablement*
- *Automation Strategy*
- *Data strategy*

Infrastructure/Development Security Antipatterns

Common mistakes increase friction and organizational risk



Securing cloud like on premises

Attempting to force on-prem controls and practices directly onto cloud resources



Bizarro Risk Exceptions

Granting permanent security exceptions for business-critical workloads (for political reasons)



Manual management

Individually managing servers, resource, & security controls instead of using automation



Department of No / Resist Trends

Ignore Cloud, DevOps, AI, Software Bill of Materials (SBOM) until absolutely required



Delay Security until the end



Makes security fixes difficult, expensive, and unlikely



Lack of commitment to lifecycle

Treating security controls and processes as points in time instead of an ongoing lifecycle

Best Practice – Integrated Strategy

Normalize security as part of IT, development, & business practices

This workshop helps you define and rapidly improve on best practices including:

- ***Security is a team sport*** – integrate culture and accountabilities across development, technology, and security teams.
- ***Clear Expectations*** - Set up clear security standards and risk accountability (aligned with organizational risk) that set up security teams as enablers, partners, and trusted advisors.
- ***Native Process Integration*** - Integrate security natively with development workflows (including blameless postmortems), IT Admin processes, and automation (CI/CD, Infrastructure as Code (IaC), and others).
- ***Establish support mechanisms*** – Establish security education and local champions programs to enable everyone to make informed and effective security judgements.
- ***Stay Current*** - Keep up with continuously evolving threats, trends, technologies, and business requirements