ON2IT AND AMS-IX PRESENT: THREAT TALKS

Threat Talks
Zero Trust

Never trust, always verify.

Zero Trust is a strategic initiative that helps prevent successful data breaches by eliminating digital trust from your organization. Contrary to popular believe, Zero Trust does not mean we don't trust people. It means we don't blindly trust the digital traffic moving through our networks.

Instead of engaging in an endless arms race with hackers across your entire, ever-growing attack surface, Zero Trust shifts the focus to what matters most. A strategy based on prevention, the Zero Trust strategy protects your most valuable data, applications, assets, and services.

In this Threat Talks infographic we will discuss the five steps of Zero Trust:

- **Step 1:** Define the protect surface
- **Step 2:** Map the transaction flows
- **Step 3:** Build a Zero Trust architecture
- **Step 4:** Create a Zero Trust policy
- **Step 5:** Monitor and maintain

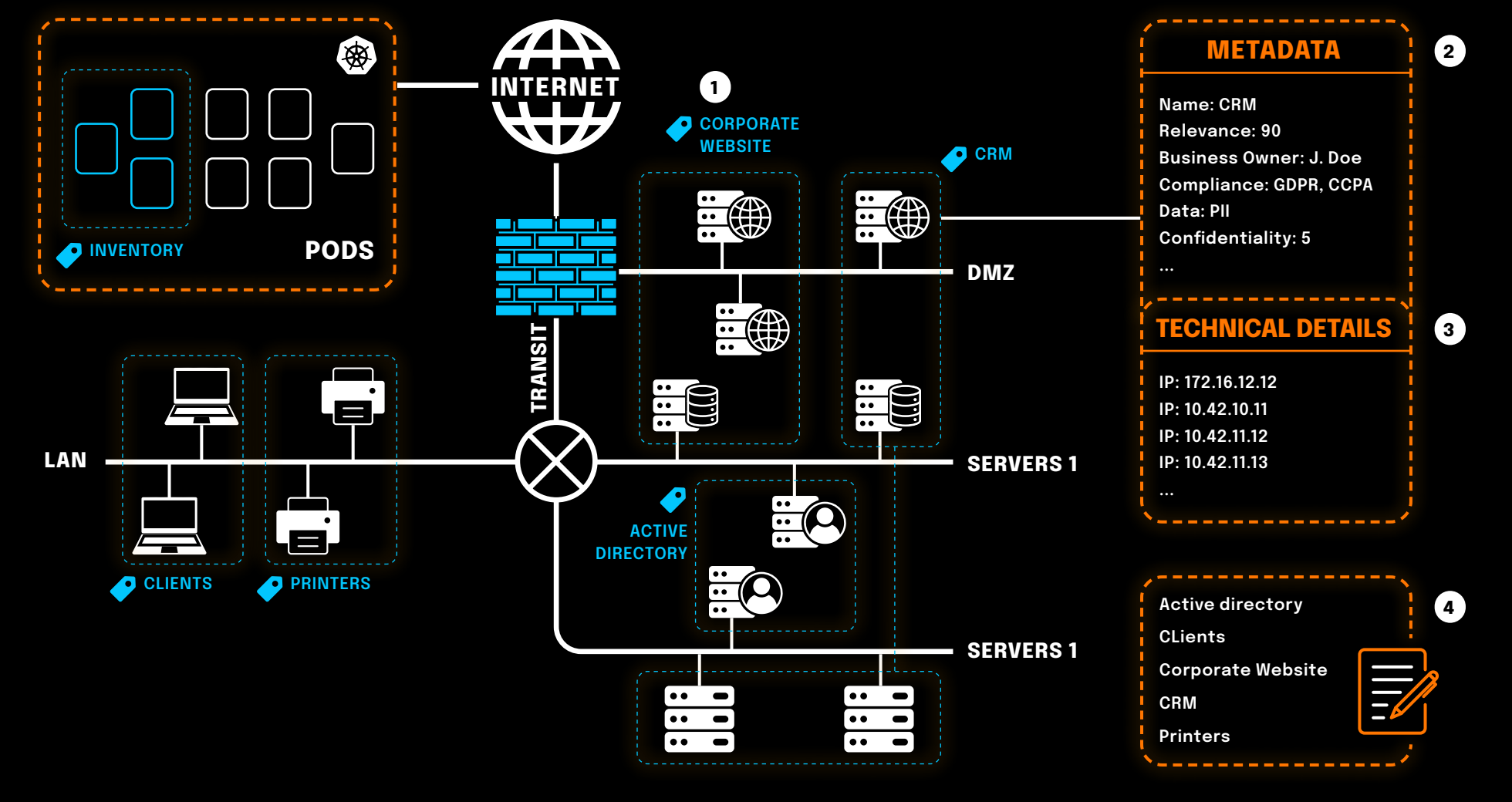
Step 1
Define the protect surface

It really is that simple. In step one, we define what we need to protect.

It is important to understand that security is not the goal itself: it exists to help the business run smoothly. That means we must look at what needs protection from a business perspective. For example: it is not about protecting web servers, but about protecting the corporate website. It is not just a database, it is the Customer Relationship Management (CRM) system that is essential to our daily operations.

We call these domains that need protection protect surfaces. Once we have identified our protect surfaces, we add metadata to them. This helps us understand who owns the protect surface, how critical it is for the business, and whether there are any compliance requirements tied to it.

As a general rule, the easier it is to define metadata, the better defined the protect surface is. And one last tip: don't try to identify all protect surfaces at once. As your Zero Trust journey evolves, more will naturally become visible.



Definition
1. Define and write down what you want/need to protect, DAAS could help here. Don't make it an endless list; 10 or 15 to start is okay, the rest will follow naturally. Next, pick the top five protect surfaces to start with.

Metadata
2. Fill in the metadata, i.e. name, relevance, description, business owner, CIA-rating, compliance- and datatags per protect surface.

Technical data
3. Find the technical details i.e. IP-addresses, cloud-resource-IDs. The graphic shows a fictional network, but assets can also be in the cloud, wheter it is IaaS, PaaS or SaaS.

   As a tip: smaller SaaS applications can be handled as a single protect surface.

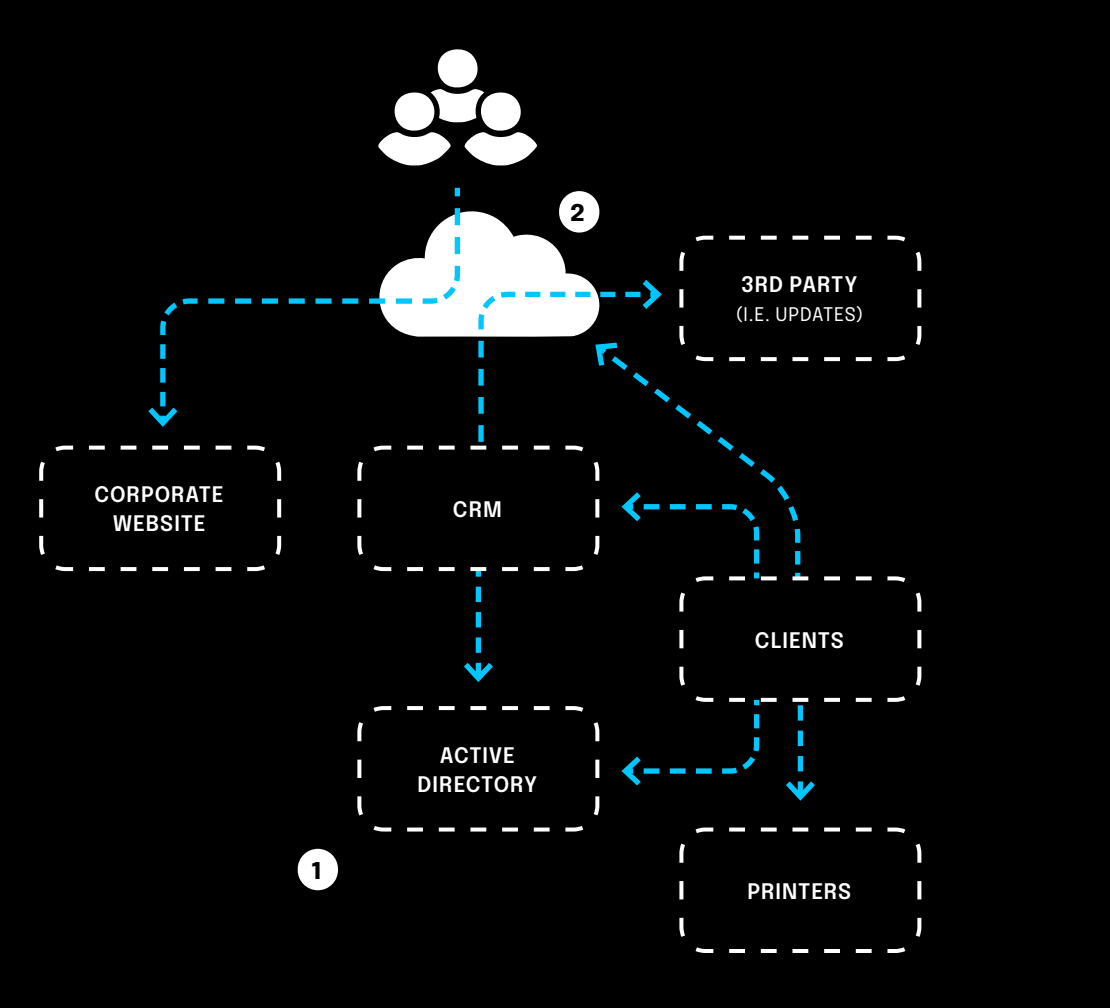
Scoping list
4. Store all this information, cause this will be your working list, also referred to as scoping list.

Step 2
Map the transaction flows

Once you have identified a few protect surfaces, the next step is to start mapping the transaction flows: how these protect surfaces communicate with one another.

This step provides valuable insight into where data is moving across your environment, and just as importantly, helps you understand the potential blast radius in case of an attack. Knowing these communication paths allows you to assess which systems could be affected if something goes wrong.

Later in your Zero Trust journey, the transaction flow matrix can also serve as a powerful validation tool. By comparing actual traffic flows with the expected ones, you can verify whether your security controls and policies are correctly implemented and aligned with your design.



3

FROM \ TO	Active Directory	Clients	Corporate Website	CRM	Printers	Outside
Active Directory	✓	✓				
Clients	✓	✓		✓	✓	
Corporate Website			✓			
CRM	✓			✓		✓
Printers					✓	
Outside			✓			

4

Transaction flows
1. Map out the transaction flows between protect surfaces. Be aware: the direction of the communication is important.

Outside access
2. Pay extra attention if protect surfaces need access to or from the internet (or anywhere outside your infrastructure), make this very specific where possible. As a rule of thumb, except maybe for the clients, no protect surface should be allowed to have unspecified internet access. This is also a great way to map your suppliers.

Access density
3. Once you have the transaction flows, you can map them out to a matrix, which shows you the access density.

Blast radius
4. This matrix will also show you the potential blast radius from a single protect surface, making it really clear why the protect surface 'clients' is a favourite target for attackers.

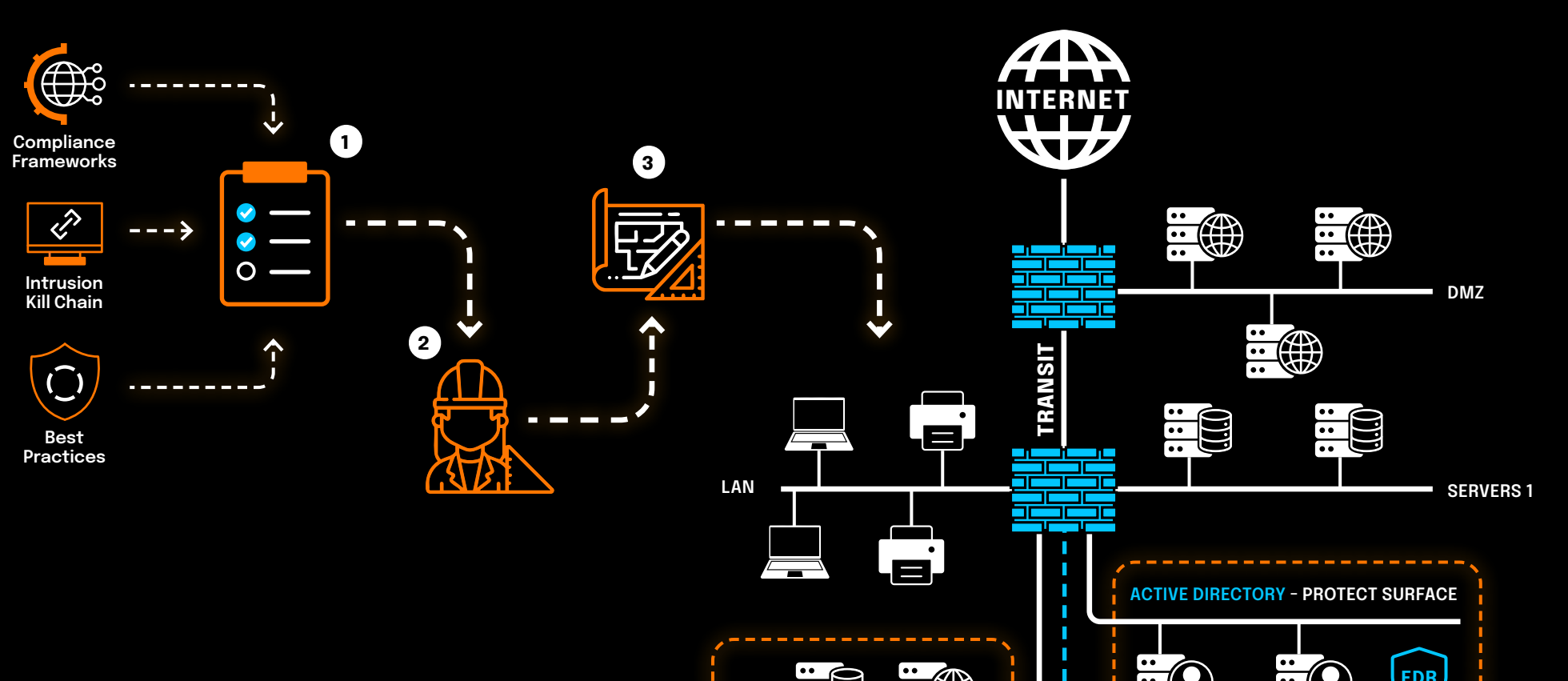
Step 3
Build a Zero Trust architecture

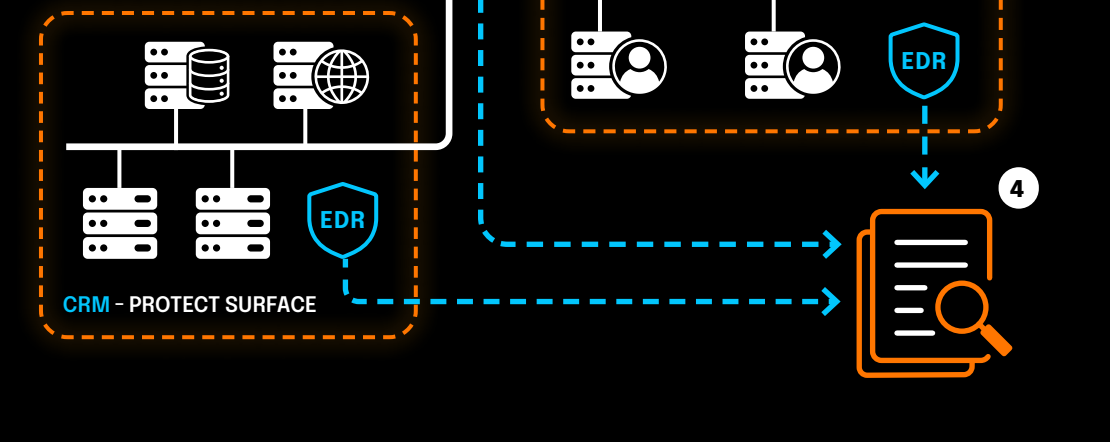
Step 3 is where plans meet reality. In this phase, we determine which security measures are necessary to properly protect each protect surface and meet the requirements of relevant compliance frameworks.

To give a simple example: a guest network requires far fewer safeguards than a mission-critical system like your CRM. Once the security requirements are clear, architects can begin translating them into a Zero Trust architecture. This is the point where strategic goals are turned into a concrete blueprint for implementation. After the architecture is complete, operational teams can begin the rollout.

While the process itself is not overly complex, success depends heavily on business alignment. A strong Zero Trust implementation requires cooperation from all levels of the organization. Zero Trust is not just a technical project, it is a business initiative!

One final tip: segmentation is a fundamental control that will apply to nearly every protect surface. Even for cloudbased or SaaS services, it is worth considering how segmentation can help reduce risk and improve control.





Measures
1. Identify and assign the appropriate measures for the protect surface based on:
   - Compliance requirements
   - Organizational standards
   - Industry best practices
   - Intrusion kill chain analysis

Practical architecture
2. Translate the assigned measures into a practical architecture. If a measure is infeasible due to tooling, complexity, or cost, treat it as a risk, document the rationale and make a conscious decision on how to proceed.

Controls into action
3. Put the defined controls into action. While the example shows segmentation (called micro-perimeters in Zero Trust) and EDR, these are just illustrative: controls can vary, such as including MFA. The exact architecture and controls will differ based on your environment.

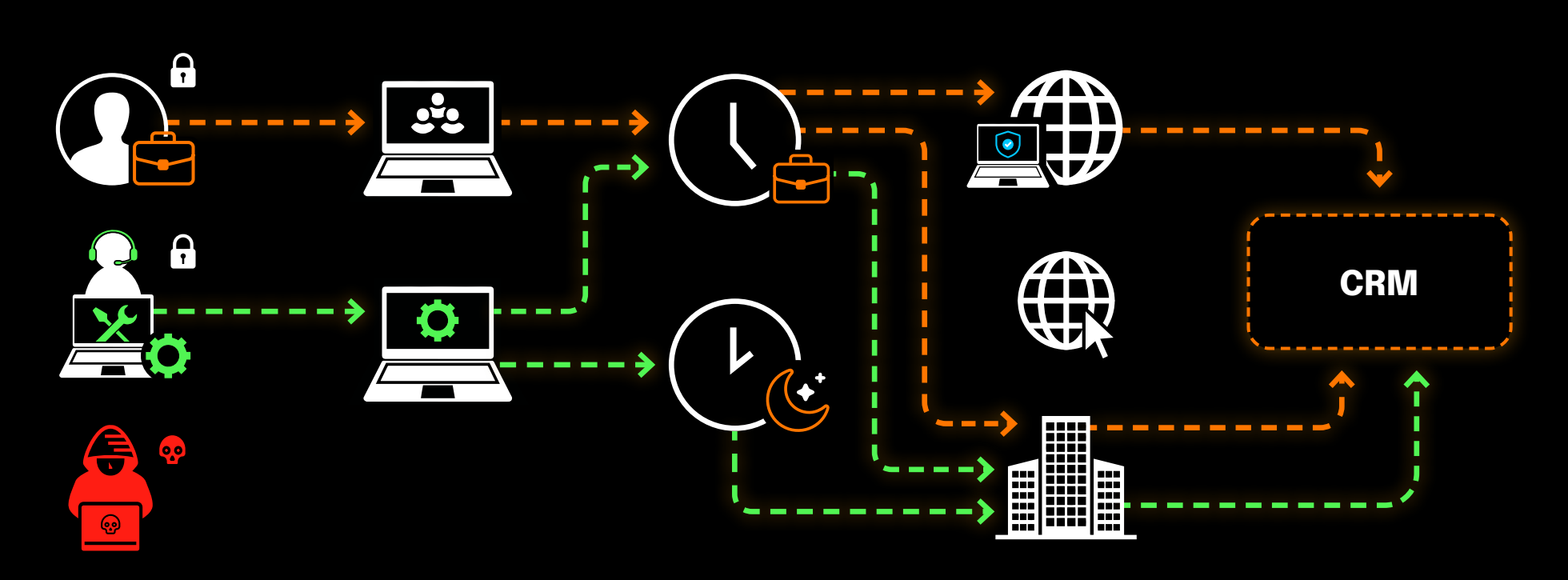
Assess effectiveness
4. Regularly assess control effectiveness and collect evidence. This is vital not only for validation, but also for meeting compliance and audit requirements.

Step 4
Create Zero Trust policy

In this step, we define the Zero Trust policy for each protect surface. The foundation of Zero Trust is simple: by default, there is no access, nothing is trusted unless explicitly allowed.

From this starting point, we build a granular policy using the Kipling Method: who should have access, what they are accessing, where they are accessing it from, when they are allowed to access it, why they need access, and how the connection is made.

This structured approach ensures that policies are clear, specific, and enforceable. Importantly, policies should always be defined from a business perspective. It is then the responsibility of engineers and security teams to translate these into operational controls that reflect the intent of the business.



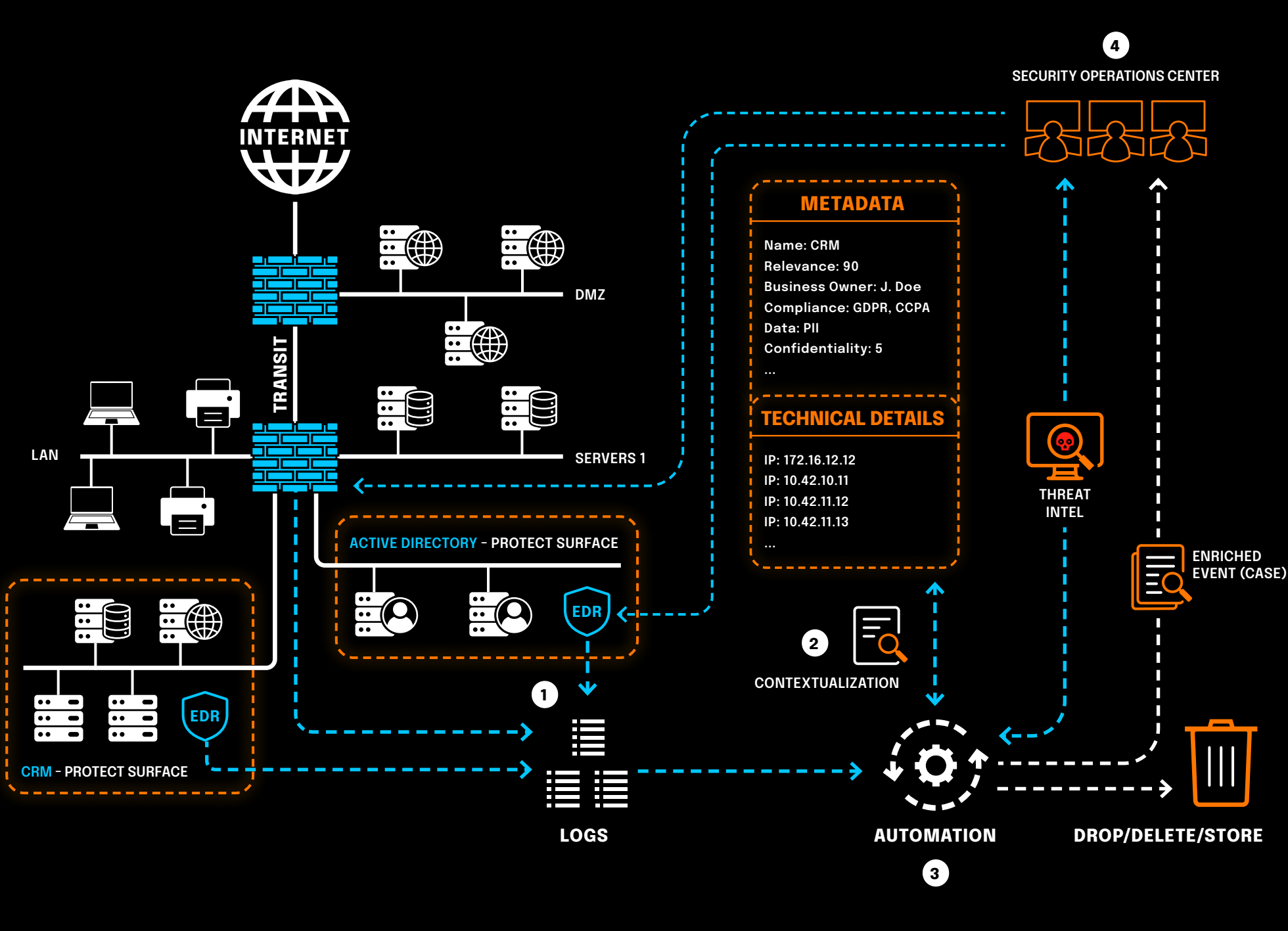
WHO	WHAT	WHEN	WHERE	WHY	HOW
SALES	Customer Records	Business Hours	Office / SASE	Drive sales	Encrypted (TLS), All actions are logged
ADMIN	CRM Settings	24/7	Office	Maintain CRM	Encrypted (TLS), All actions are logged MFA on critical changes

Step 5
Monitor and maintain

The more mature your Zero Trust implementation becomes, the more logs you'll generate. If you are not cautious, these logs can quickly become overwhelming. Logs provide precise insights into what's happening in your environment and where attention is needed, although raw logs generated by your security controls lack business context.

That's why it's important to enrich raw logs with Zero Trust context (especially the metadata defined in step 1). This transforms basic logs into rich, meaningful information.

With rich logging, you can immediately understand the potential business impact of an event. It also opens the door to smart automation, allowing your SOC to focus on what truly matters.



Collect logging
1. As your Zero Trust implementation matures, your security controls will generate an increasing volume of logs. These logs provide vital visibility into what's happening across your environment. More than just data, they offer early indicators of potential attacks, misconfigurations, and opportunities for optimization.

Enrich logging
2. Raw logs lack business relevance. They may tell you what happened, but not where or why it matters from a business perspective. By enriching logs with metadata (see step 1), such as the associated protected surface, compliance requirements, or affected user data: you transform vague alerts like "brute force attack on 172.16.12.12" into meaningful insights like "CRM system under attack." This context allows for smarter, faster decisions and proper automation.

Automation
3. With the sheer volume of logs, manual review becomes impossible. Automation is essential to filter out noise and focus on what matters. But tread carefully: not all "blocked" or "killed" events should be dismissed. For example:
   - Ignore: It is safe to ignore Brute force attempts on a public login page that are automatically blocked.
   - Investigate: But don't ignore similar attacks on internal systems, even if blocked. This could signal a breach or a misconfiguration like an expired service account.

   When in doubt, create a case and escalate to the SOC for further analysis.

Security Operations Center
4. The Security Operations Center (SOC) reviews these cases. If it's a false positive, automation rules can be adjusted to avoid future noise. If it's a valid threat or a sign of weak controls the SOC can recommend or implement improvements. Thanks to enriched context, they can also quickly involve business owners when needed, ensuring security actions are aligned with business impact.

threat-talks.com

ON2IT ZERO TRUST INNOVATORS

amsix

CONTACT US