DEADLY SINS OF AI

BlastWave

A MODERN TALE OF SIN

For years, Operational Technology (OT) systems relied on the isolation of "air gaps" and obscure protocols, trusting in obscurity as a kind of false virtue. But like many illusions of righteousness, this protection has fallen to temptation. With the rise of AI, especially generative AI, attackers desire greater power with less effort. Tasks that once took weeks are now completed in moments, as if time has been bent by forbidden knowledge.

AI now walks a more ambiguous path. It has become an instrument of both defense and transgression. Hackers use machine learning and large language models to probe networks, uncover weaknesses, and conjure attack code almost effortlessly. What was once painstaking labor is now automated sin. Efficient, scalable, and dangerously precise. Our critical infrastructure stands increasingly exposed; Power grids, factories, the very lifeblood of modern society.

Meanwhile, many OT systems remain relics of an earlier age, never designed to face the open world. Unchanged, unadapted, and vulnerable. Against them stand AI-driven threats that evolve with relentless hunger. This mismatch creates a perilous imbalance, where old defenses falter against new forms of cunning.

The result is a digital fall from grace. Organizations can no longer rely on passive defenses or the comfort of tradition. Instead, they must pursue resilience with vigilance, embracing proactive strategies that match the speed and adaptability of AI. In this new landscape, security is now moral challenge: a constant struggle against ever-evolving forms of digital sin.

TEMPTATION FROM WITHOUT. TEMPTATION FROM WITHIN

AI threats in OT environments manifest in two forms: external and internal – echoing the dual nature of sin itself.

Direct threats are an outward expressions of corruption. Here, AI amplifies familiar attacks, making them more deceptive and potent. Phishing emails become utterly convincing, crafted with human subtlety. Network scans occur at superhuman speed, a relentless pursuit of access, data, and control. They are deliberate, calculated intrusions, refined by AI into tools of precision.

Indirect threats are more insidious, the internal use of AI tools meant to assist but vulnerable to misuse. When organizations deploy AI for monitoring or maintenance without proper oversight, they risk inviting sin from within. Overreliance on powerful tools, unchecked consumption of data, and blind trust in automated systems. Attackers may poison AI models or exploit unauthorized "shadow AI," subtly twisting trusted systems into instruments of harm.

Both forms of sin must be reckoned with: One, the external tempter; the other, the internal failing. To remain secure, organizations must guard against both – defending their boundaries while also disciplining their own use of AI.

In the end, cybersecurity in the age of AI is about vigilance, diligence, and the humility to recognize that even the most powerful tools can lead to downfall if left unchecked.

PRIDE: AI-DRIVEN SOCIAL ENGINEERING

Our pride tells us we would “never fall for that”. We’re too smart, too savvy.

Attackers can now create phishing messages that perfectly mimic known colleagues or vendors,generating deepfake voices or videos to impersonate trusted figures, like senior engineers.We trust what looks familiar and AI exploits that over-confidence.

In our arrogance we believe in protections like passwords and simple MFA. But these are no longer enough. A single mistake can give attackers full access.

It’s time for organizations to remember that pride comes before a fall, to eliminate reliance onhuman judgment, and to adopt stronger authentication methods that cannot be faked.


Pride is a wound, and
vanity is the scab on it.
SOPHOCLES

GREED: AI-POWERED RECONNAISSANCE

Information is good; more information is better. Information greed drives attackers to gather as much, and as quickly, as possible. AI now satiates that greed at a scale and a speed that's unimaginable.

AI tools can scan entire networks in minute, mapping systems, identifying devices, and spotting weaknesses. They even use public data, like manuals or online records,predicting how systems are built, eliminating "security through obscurity." Hidden or niche systems are no longer safe from the avarice of attackers.

Traditional defenses like firewalls and VPNs often expose entry points that AI can detect. Once inside, attackers can quickly mapeverything, especially in flat OT networks.

To defend against this data greed, organizations must make systems invisible, limit exposure, and require strong authentication before any connection is allowed.


MOST OF ALL,
I HATE YOU
BECAUSE I THINK OF YOU.
OFTEN.
The Cruel Prince
HOLLY BLACK

LUST: AI BROWSER EXPLOITATION

AI attackers will get what they want, especially if your AI-powered tools can be lead into temptation.

Attackers hide malicious instructions in documents or websites. When an AI assistant reads or summarizes the content, it may unwittingly execute those hidden instructions.

This can lead to stolen data, and exposed credentials. In OT environments, where browsers are used to access critical systems it can leadto unsafe recommendations or catastrophic decisions.

We all yearn for a life of ease, but organizations should limit browser-based access for sensitive operations and ensure strong authentication and isolation between systems.

Envy

ENVY: ADAPTIVE MALWARE AND C2

Envy drives attackers to imitate normal behavior – and blend in.

AI-powered malware can change its structure constantly to avoid detection. It can also mimic normal network traffic, making malicious activity look legitimate.

Attackers use large numbers of fake domains to maintain communication channels, making them hard to block. This allows long-term, hidden attacks that slowly damage systems without being noticed.

To counter this, organizations must focus less on detecting patterns and more on verifying identity – ensuring that only trusted devices and users can communicate at all.

Envy

It is not greed
that drives the world
but envy

WARREN BUFFET

GLUTTONY: AI-DRIVEN LATERAL MOVEMENT

AI-powered attackers can, and will, take as much as possible. It will never be enough.

Once inside a network, AI attacks move vorasciously, identifying targets and exploiting connections between systems. See, grab, take; more, More, MORE. And you may never notice; AI can test stolen credentials everywhere, all at once, mimicking normal network traffic to avoid detection.

In an OT environment, this can turn a small breach into a major incident affecting critical operations.

Organizations can opt to **NOT** ring the dinner bell, but instead enforce strict identity controls, limit communication between systems, and ensure that each user or device only has access to what it truly needs.

Stop attackers' overconsumption.

I want it, I want it, I want it, I want it

I need it, I need it, I need it, I need it

BUCKCHERRY — GLUTTONY


#DMV


WRATH
In the souls of the people
the grapes of wrath are filling
and growing heavy
JOHN STEINBECK
::init_sequence>> alpha-noc
if (signal_entropy > ∞)
// scrambled tokens

WRATH: AI MODEL POISONING

The wrath of AI attackers can target AI systems meant to defend.

Attackers can poison defensive AI models by feeding them misleading data. Over time, can cause the defensive AI to misinterpret threats or ignore them entirely.

Systems may report everything is normal while an attack is happening, or they may trigger unnecessary shutdowns, rendering automated defenses useless at best and complicit at worst.

Protecting your data integrity, controling data sources, and avoiding over-reliance onAI “defense” decisions with a Zero Trust approach means deterministic, rule-based controls remain effective.

SLOTH: AI-DRIVEN EXPLOITATION

It can be hard to move when every fiber of your being is telling you to sit still and do nothing. Sadly, AI will absolutely take advantage of you maintaining your cybersecurity status quo.

Attackers use AI to quickly find and exploit vulnerabilities, often faster than organizations can patch them. This is especially dangerous in OT systems, where updates are either slow or, because of projected downtime, impossible.

The gap between attackers moving fast, and defenders struggling to keep up is growing. And still we do nothing.

Yet, overcoming this procrastination is easy and actually requires very little effort: adopt a Zero Trust stance on access to vulnerable systems, isolate critical assets, and control where, and what actions are allowed on the network.


I'm busy doing nothing
Working the whole live whole day through
Trying to find lots of things not to do.
Bing Crosby, William Bendix, Cedric Hardwicke

BlastWave's OT Protection Solution

BlastWave delivers a comprehensive Zero Trust Network Protection solution to provide the best possible outcome for OT environments. With a unique combination of network cloaking, secure remote access, and software-defined microsegmentation, we minimize the attack surface, eliminate passwords, and enable segmentation without network downtime.

To learn more, come to www.blastwave.com

v20260520

Prevent industrial cyberattacks, and ensure the world's critical infrastructure stays protected, productive, and profitable. Together we can build a resilient future for OT networks. Join the movement at **www.blastwave.com**

©2026 BlastWave Inc. | 1045 Hutchinson Ave., Palo Alto, CA 94301 USA | T: +1 650 206 8499

BlastWave
PREVENT
INDUSTRIAL
CYBERATTACKS