DARKTRACE

WHITE PAPER

A Comprehensive Guide to OT Security

CONTENTS

Abstract

The emergence of OT cyber security solutions in recent years demonstrates that critical infrastructure and industrialized organizations are trying to find a way to address the risks posed by modernizing networked industrial operations and the threats who aim to disrupt them.

However, many OT cyber security solutions are limited in scope. By assuming IT and OT are separated, they use legacy security techniques such as malware signature detection and vulnerability management as a means to reduce the cyber risk to OT. This white paper will explore the new challenges posed to OT security professionals and explore the best solutions for fighting the eminent cyber threats associated with OT and ICS security.

A New Era of OT Security

The practice of cyber security has changed dramatically in the past few years, presenting a significant challenge to management teams across all industries and business domains.

Compromised OT devices within ICS and SCADA environments can lead to enormous physical damage and danger to human life. All the while, industrial and energy industries have remained heavy targets for threat actors, accounting for a combined 18% of data breaches in IBM's 2023 Data Breach Report.

For the industrial and critical infrastructure sectors, the consequences associated with attacks on OT and the growing threat to OT has recently increased OT cybersecurity pressure on these industries from regulatory authorities and cyber insurance providers. Recent government initiatives — such as the US Department of Energy's 100-day 'cyber sprint' to protect electricity operations and President Biden's Executive Order on Improving the Nation's Cybersecurity, TSA cybersecurity directives for Pipeline, Airports and Rail Systems — and regulatory frameworks and directives such as the EU's NIS directive have either encouraged or mandated that critical infrastructure industries start addressing the new risks directly associated with OT environments.

With increased pressure to secure these environments, IT security teams have become more accountable for defending Operational Technology (OT) and OT-specialist teams have similarly inherited responsibility for traditional IT security with an OT focus. Additionally, the convergence of IT and OT technologies and responsibilities requires the synergy of both specialist skills and working practices to protect these mission critical environments.

> More than 40% of the total number of global industrial control systems (ICS) computers saw some kind of malicious attack during the course of 2022.
>
> **Kaspersky**

What are the Challenges of Securing OT Environments?

IT & OT convergence

Even when operating in the same organization, corporate IT systems and Industrial Control Systems (ICS) will have different objectives. However, intensified competition resulting from globalization has propelled the convergence and synergy of the cyber-physical realm and more general and disparate information networks.

Organizations with OT have traditionally tried to reconcile the conflict between IT and OT by attempting to separate them completely into distinct networks. While historically this was accomplished with an air gap, or a combination of uni-directional firewalls, jumpshot servers, and micro-segmentation so that any cyber threats that slip into IT systems do not then spread laterally into highly sensitive, mission-critical OT systems.

Regardless of how well an organization separates their IT and OT environments, there are often multiple ways an attacker can move from one environment to the other. Adversaries take advantage of organizations lacking visibility especially of OT network traffic and commonly exploit vulnerabilities including unpatched systems and unnecessary open ports on devices to laterally move while other TTPs may include directly targeting OT via removable media and rogue devices.

Full visibility across IT and OT ecosystems in a single pane of glass is thus essential for organizations seeking to secure their OT. This is not only to illuminate any points of IT/OT convergence and validate the fact that an air gap exists in the first place, but also to see when an attack persists from IT to OT.

Spillover from corporate network compromises

Industrial control systems and industrial operations are increasingly affected as an unintended side effect of attacks targeting corporate networks. Standard PCs that now form part of a typical ICS are open to the same compromises as their enterprise counterparts. Several cyber security breaches on US power stations have been publicly attributed to this method of attack.

Colonial Pipeline, one of the largest oil pipelines in the US, experienced a ransomware attack in 2021 that targeted their IT systems.

While the attack did not directly compromise any operational technology, it cost them approximately $5 million in ransom and forced the organization to shut down operations for nearly a week to not risk compromise of their physical pipelines. The shutdown prompted gas shortages across the east coast of the United States. Such incidents demonstrate that indirect compromises pose as significant a threat to operational environments as successful, targeted attacks against ICS.

Introduction of IIoT to ICS

The scope of Operational Technology is broadening with the rise of Industrial Internet of Things (IIoT) devices being integrated into traditional ICS environments. The IoT and IIoT paradigm presents the challenge of managing more complex dynamic and potentially exposed industrial networks.

As the shift towards IIoT introduces myriad device classes and an expanded attack surface, complete visibility of the digital ecosystem has become increasingly unattainable. While effectively designed to be interoperable and resilient, industrial control systems are not necessarily easy to protect and are typically extremely difficult to update. Cyber security researchers are particularly concerned about the systemic lack of authentication in the design, deployment, and operation of some existing ICS networks. For this reason, the addition of IoT and IIoT in traditional industrial networks has made it increasingly clear that any connection to the internet can be exploited to access inherently unsecure by design ICS networks.

IoT/IIoT increasing points of initial access to industrial networks poses significant risk as there are usually a myriad of unpatched vulnerabilities. Patching is extremely difficult within ICS network, as the inbuilt methods for delivering updates in operational environments are unsuited to the requirement of uninterrupted availability. Security support for operating systems at the point of installation has also proven not to last as long as the control systems themselves. Security teams suffer from the inability to retrofit security features into devices with decades of service life remaining.

Transitioning OT to managed cloud services

Though moving Industrial Control Systems (ICS) to the cloud has been theoretically possible for at least 10 years, the associated risks have meant that uptake has been slow. Operational technology is often bespoke and has traditionally been isolated from the Internet, and so moving OT systems to the cloud can impact reliability, performance, and security. Industrial Control Systems are high-stake environments: the slightest period of downtime can have significant ramifications for the safety of workers and the business as a whole.

These considerations have traditionally led most organizations to conclude that the benefits of moving ICS to the cloud — namely, making it cheaper and easier to manage, and improving its availability — are outweighed by the risks. Even though workers may be able to remotely control equipment on the factory floor, for example, the threat of those with malicious intent gaining access to the same protocols is a strong deterrent for organizations to hold back on transitioning to the cloud.

However, the conditions brought about by the COVID-19 pandemic have since brought unique challenges to the management of SCADA systems on site, causing organizations to consider secure ways to slowly transition these environments to the cloud.

As OT converges with IT in the cloud, so too do their respective risks. Only complete and unified visibility across both IT and OT will allow companies to accelerate their digital transformation whilst at the same time managing the associated risks of digitization and of their increasingly dynamic workforces.

Keeping up with changing cyber regulations

Cyber regulations, agencies, and standards are expanding and evolving. These regulations will always be changing to catch up with the changing threat landscape. Similarly, they can often be hard to interpret and apply to unique contexts and situations. Additional challenges to complying with cyber regulations may include complex environments that require different compliance standards, resource constraints, maintaining appropriate documentation, and more.

To address these challenges, OT facilities need to be aware of the cyber regulations that apply to their industry and establish ongoing training on policies and procedures that can help them comply with relevant regulations.

Threats Facing OT Systems

Advanced Persistent Threats (APTs)

APTs are sophisticated and perform highly targeted forms of cyber-attacks. These attacks are typically launched by organizations like nation-states, state-sponsored criminal organizations, and highly capable and developed cybercrime organizations that have the resources to carry out specialized and persistent malicious activity that takes place over extended periods of time and is considerably more effective and disruptive than common cyber-attacks.

In some cases, APTs are part of a larger strategic agenda to disrupt a nation's critical infrastructure or retrieve sensitive data with malicious intent. These attacks use advanced tactics, such as unique novel malware, in an attempt to move laterally through systems while remaining undetected, leveraging previously unknown vulnerabilities and gaining unauthorized access to information and controls.

Insider threats

Insider threats can come in the form of employees, vendors, contractors, or anyone with access to sensitive systems, data, or information. The cyber risk posed by insiders can be grouped into malicious insiders, such as rogue or disgruntled employees, or accidental, such as a well-meaning employee inadvertently leaking data or introducing a security flaw.

There are generally two types of insider threats: malicious and non-malicious, or accidental. For organizations managing OT, both types originate from personnel who have legitimate privileged access to OT networks and have insider knowledge of assets, configurations, locations, security controls, or vulnerabilities. Of increasing concern to security teams, these personnel can also include external contractors, such as vendors or consultants, who require high levels of access to perform their role.

Compliance breaches, poor cyber hygiene, and disgruntled or rogue employees all pose a greater everyday threat to these systems than APTs or the latest zero day.

Insider threats rarely use attack tools or malware to achieve their goal, rendering signature-based threat detection useless. Instead, they leverage their legitimate access to make changes to native functionality. Rules-based threat detection can be used to prevent certain actions, but playbooks are limited to the imagination of the person implementing them and the time they have to create and maintain them.

Real world insider attacks:

The 2001 sewage spill in Maroochy Shire, Australia, was the first high-profile example of a malicious insider manipulating control systems to impact OT. More recently, the 2021 incident at the Oldsmar Water Facility in Florida was the result of poor cyber security practices. While there is much speculation as to the exact cause of the incident, the root cause appears to have been human error which resulted in changes to intended chemical content levels in drinking water.

Exposed OT initial access point

For some organizations with OT/IoT, the adversary's intention may not be to target OT and disrupt operations or physical process controlled by the OT. Instead, for these organizations, internet facing unsecured OT many times in the form of building or warehouse management systems, IIoT, and IoT devices that exist as part of the organizations expanded network attack surface may be left exposed and unprotected. These devices if internet facing can act as an initial point of access for attackers who can exploit the device and pivot from these devices and move laterally to action upon more critical systems or data.

Ransomware

Ransomware has become an increasingly prevalent threat for organizations operating ICS, with several high-profile attacks hitting organizations in recent years affecting operations. Many of these organizations provide critical infrastructure, meaning any disruption they suffer as a result of ransomware can have broad societal or safety consequences, and place more pressure on the organizations themselves to deliver ransom payments.

Ransomware can target ICS mechanisms directly, as with EKANS ransomware attacks, or can indirectly impact Operational Technology by disrupting the IT systems which provide essential visibility into them. IT/OT convergence has considerably widened the attack surface for OT ransomware and made it harder to predict where attackers will come from next.

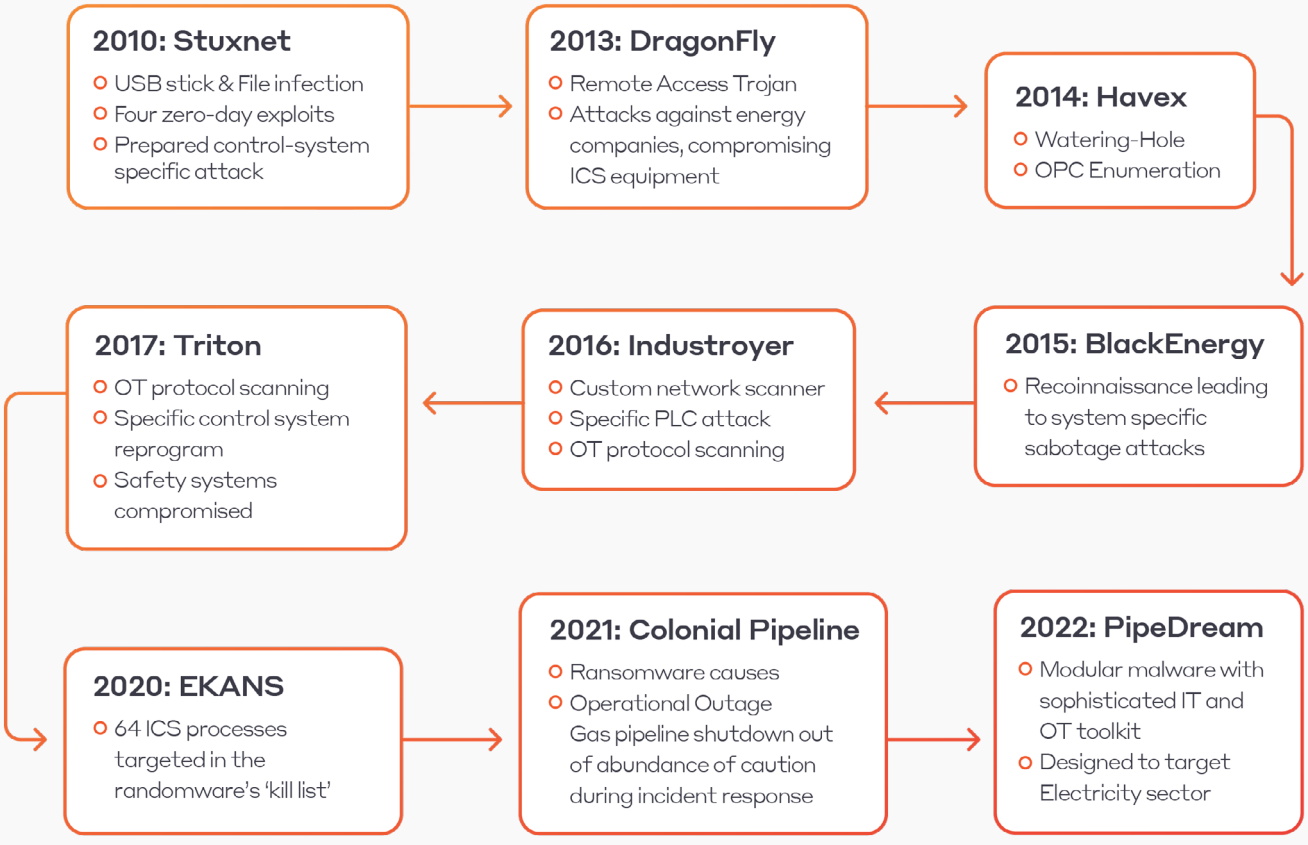
Gaining visibility remains challenging in industrial environments, where decades-old legacy devices, designed without security in mind, are often deployed alongside newer technologies, such as the industrial internet of things (IIoT).

This heterogenous composition makes asset identification and accurate visualization of connections and activity difficult.

Vulnerability management is also a process of diminishing returns. Many advisories for ICS devices have no practical mitigation advice, with the 2021 SANS ICS Security Summit confirming that over a fifth of reported common vulnerabilities and exposures (CVEs) do not include a patch.

Remote access is an emerging attack vector. Many industrial organizations have adopted remote access tools such as TeamViewer to allow employees to control ICS and OT without taking the health risk associated with entering physical premises, creating additional attack paths for threat actors.

A Timeline of High-Profile Industrial Ransomware Attacks



Each of these threats are not mutually exclusive. An APT may leverage a disgruntled employee to exfiltrate sensitive data. Equally, a ransomware gang may well be backed or aided by a nation state. Thus, attribution in OT security can be tricky and demonstrates the limitations of relying on threat intelligence for detection.

What to Consider When Choosing an OT Solution

Does it help meet required compliance regulations?

A large number of OT operators work in critical infrastructure industries (i.e. government/defense, water providers, electric cooperatives, and transportation). This means that there are government mandated security standards that need to be complied with.

Consider finding an OT security solution that maps out how its solutions and features can help your organization comply with relevant compliance mandates such as NIST, ISA, FERC, TSA, HIPAA, CIS Controls, and more.

Can it integrate with existing technology and systems?

OT and ICS devices make up complex digital environments that can sometimes be further complicated with non-integrated security solutions. Implementation of several point solutions that complete individual tasks runs the risk of increasing workloads for operators and creates additional challenges with compliance, budgeting, and technical support.

Does it have the availability to scale?

As new devices are added and OT environments expand or evolve, static security solutions require constant tuning, updating, and sometimes even an entire overhaul of the security structure.

To keep up with the demands of digitization and the expansion of business, OT security buyers should seek a solution that can grow with their business.

Does it provide visibility and tracking of assets?

In today's threat landscape, where many attacks target OT infrastructure after first pivoting through IT environments, having a unified view of IT and OT systems has become an invaluable tool for detecting and neutralizing threats before the damage is done.

Similarly, OT security professionals should consider a security solution that provides both active and passive options for keeping track of their digital and physical assets.

Key Benefits:

- Active Identification:
  Accurate enumeration, real time updates, vulnerability assessment, asset validation
- Passive Identification:
  Eliminates risk of operational disruption, minimizes risk, does not generate additional network traffic

Does it use anomaly-based detection?

Anomaly based detection enhances an organization's cyber security posture by staying ahead of evolving threats, proactively defending against potential attacks, and maintaining a comprehensive view of their attack surface.

Static baselines cannot keep pace with changes in the diverse technologies used in ICS ecosystems, where legacy devices are often retrofitted and used alongside IIoT. Siloed security solutions also fail to detect attacks that span the entire organization like malware that enters through a phishing email and moves laterally, disrupting visibility into OT.

OT Security Challenges	IT Security Solution	OT Security Solution	Separate IT & OT Security Solutions	Solution Natively covering IT & OT
Detects initial IT intrustion	X		X	X
Detects attack on IT devices in industrial network	X			X
Detects malicious change to OT devices		X	X	X
Detects pure OT attack e.g. Insider threat		X	X	X
OT Asset inventory and vulnerability management		X	X	X
Threat hunting across IT and OT			X	X
Detect lateral movement from IT into OT				X

Figure 1: The advantages of a combined IT/OT security solution

Can it secure both IT and OT in unison?

Given that most OT cyber-attacks actually start in IT networks before pivoting into OT, investing in an IT security solution rather than an OT-specific solution may at first seem like a better business decision. However, IT solutions fall short if an attacker successfully pivots into the OT network, or if the attacker is a rogue insider who already has direct access to the OT network. A siloed approach to securing either IT or OT in isolation will thus fall short of the full scope needed to safeguard industrial systems.

A mature security posture for critical infrastructure would include security solutions for both IT and OT. Even then, using separate solutions to protect the IT and OT networks is limited, as it presents challenges when defending network boundaries and detecting incidents when an attacker pivots from IT to OT. Under time pressure, a security team does not want changes in visibility, detection, language or interface while trying to determine whether a threat crossed the 'boundary' between IT and OT.

Separate solutions can also make detecting an attacker abusing traditional IT attack TTPs within an OT network much harder if the security team is relying on a pure OT solution to defend the OT environment. Examples of this include the abuse of IT remote management tools to affect industrial environments, such as in the suspected cyber-attack at the Florida water facility.

> We needed a solution that would converge IT and OT together to have a single pane of glass where we can look at all the incidents and alerts related to IT and OT.

/ Information Security Manager, Media and Entertainment

Darktrace/OT: A Unified Platform Solution

Organizations providing critical infrastructure must now look to cyber security technology that delivers continuous insights and provides early warning of both indiscriminate and targeted compromises. If an OT network is not monitored in real time, there is no way of knowing if assets have vulnerabilities or not.

Darktrace's Self-Learning AI technology is a cutting-edge innovation that implements real time prevention, detection, response, and recovery for operational technologies and enables a fundamental shift from the traditional approach to cyber defense by learning a 'pattern of life' for every network, device, and user.

Rather than relying on knowledge of past attacks, AI technology learns what is 'normal' for its environment, discovering previously unknown threats by detecting subtle shifts in behavior. Through identifying these unexpected anomalies, security teams can investigate novel attacks, discover blind spots, have live time visibility across all their physical and digital assets, and reduce time to detect, respond to, and triage security events.

> Organizations that used these [AI and automation security] capabilities extensively within their approach experienced, on average, a 108-day shorter time to identify and contain the breach.

IBM
/ Cost of a Data Breach Report, 2023

Identify vulnerable assets and harden systems

Preventative security measures like attack surface management, penetration testing, and vulnerability assessment provide security teams with a proactive approach to securing their most critical assets. Being able to identify the most at-risk systems and running emulated attacks allows organizations to harden defenses where attacks are most likely to occur, reducing risk and preventing attacks before they happen.

Darktrace assesses the strategic risks facing an organization by identifying and prioritizing high-value targets and pathways to secure vital internal systems and assets.

Attack surface management

The solution continuously monitors the external attack surface, assessing all your Internet-exposed assets for risks and identifying possible initial access vectors into the core OT network.

Attack path modelling

Maps the most relevant and impactful attack paths through your organization in real time based on MITRE ATT&CK for Enterprise and for ICS frameworks.

Pentest augmentation

Assesses all potential attack pathways around the clock.

Breach & attack emulation

Deploys de-fanged "attacks" that emulate malware, phishing, spoofing, and other common threats.

Security and awareness training

Identifies users who are exposed or vulnerable to phishing, allowing security teams to tailor training based on real-world data.

Cyber risk prioritization and reporting

Identifies CVEs on OT assets and contextualizes wider possibilities and weaknesses to intelligently prioritize patching recommendations, or the use of other mitigation controls.

Unified visibility across OT, IT, & IoT

Architectures of ICS and their operational networks are complicated and typically undergo many changes by multiple individuals over their lifetime. In ICS environments, segregation and zoning of the network is a critical security control, especially given the lack of security within endpoint devices themselves. In such environments, understanding the correct flow of data on the network and patterns of communication is essential. Darktrace addresses this challenge by observing, analyzing, and capturing communications along with their associated metadata.

Darktrace's unified view technology can be safely implemented as a separate appliance designed to provide a consolidated view into both OT and IT environments. Its user interface, the Threat Visualizer, uniquely displays all this rich information in an intuitive 3D dashboard that gives the operator a comprehensive, real-time overview of their network. This can be used to investigate whether the control system's actual behavior matches its intended design.

The Threat Visualizer allows security teams to view real-time information about data flows across OT, IT, and the Industrial Internet of Things, all while Darktrace's Self- Learning AI continuously compares this activity against expected behavior patterns.

While Cyber AI Analyst can be used to triage and investigate these detections, it is also possible to route the output to an organization's existing Security Information and Event Management (SIEM) systems to integrate with established processes and procedures.

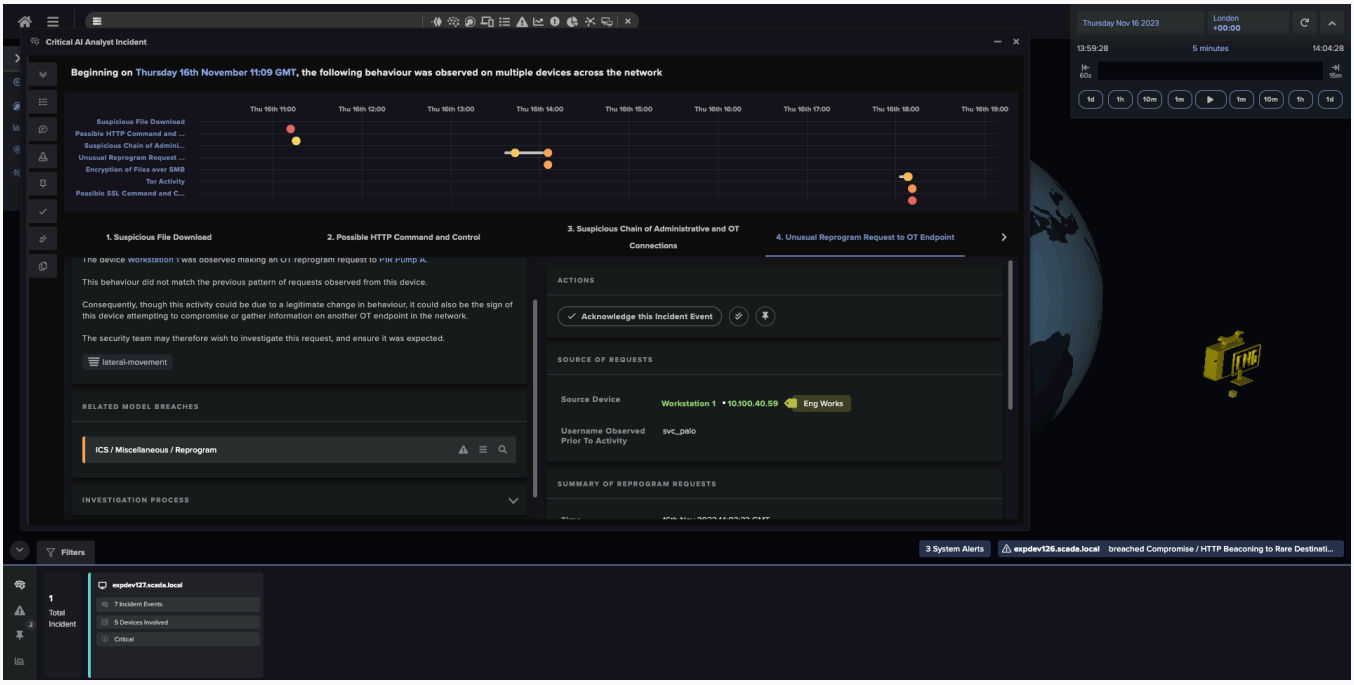


Figure 2: Darktrace AI generates an incident summary of a suspicious activity at the IT layer followed by an unusual reprogram request on an OT endpoint

OT anomaly detection and real time response

Critical infrastructure organizations control the operations of essential systems such as power grids, water treatment plants, transportation systems, and manufacturing facilities, making operational downtime detrimental to society and risks people's safety. Real time detection and response helps spot early warning signs of a cyber-attack and can significantly reduce operational downtime in the face of an event, allowing organizations to respond quickly and effectively mitigate attacks.

By analyzing all traffic and activity on a granular level in a protocol and technology agnostic capacity, Darktrace provides continuous detection, full visibility, actionable insights, and, where appropriate, autonomous response for diverse and complex ICS ecosystems. Darktrace harnesses Self-Learning AI to continuously learn 'normal' for all forms of machine and human behavior, identifying deviations indicative of an emerging attack.

Darktrace/OT can be configured to defend all the way down to Level 1 devices in the Purdue model and indirectly into Level 0. It also covers all higher Purdue levels, from supervisory functions, business logistics, and enterprise networks (Level 4&5), and beyond into cloud and SaaS. The technology also provides visibility into and around the DMZ.

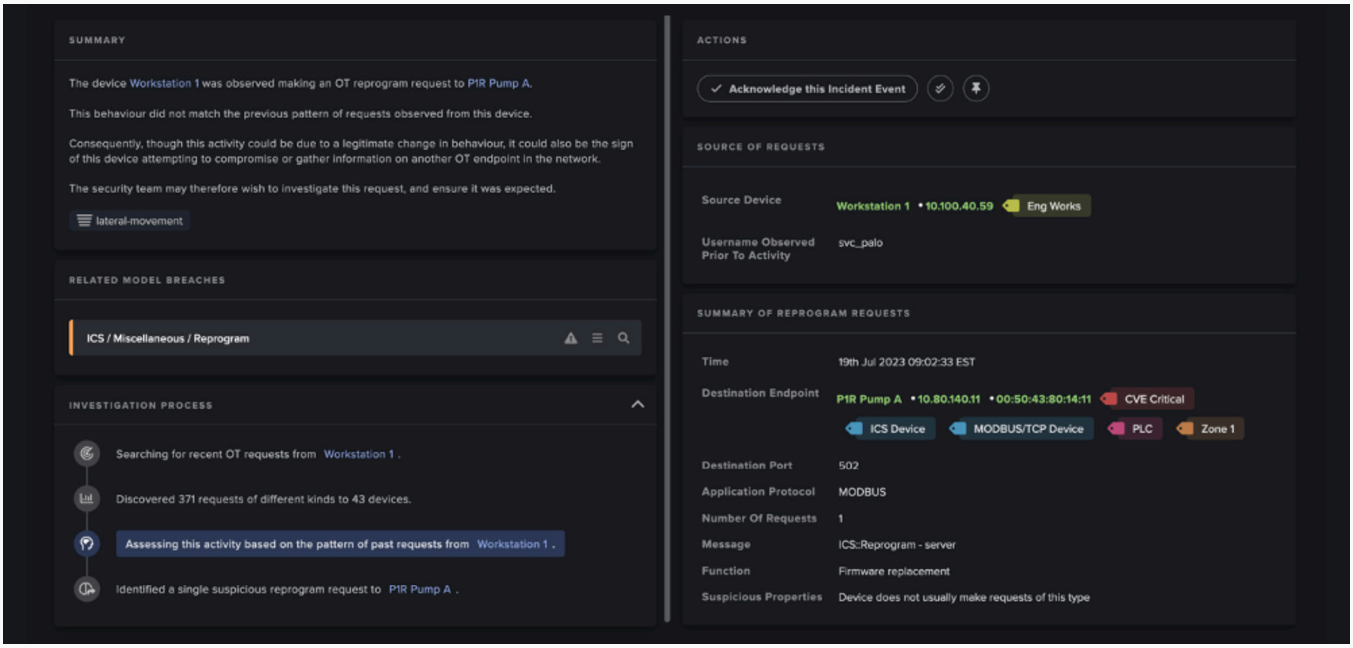


Figure 3: AI Analyst Incident reporting an unusual reprogram command using the MODBUS protocol.
The incident includes a plain English summary, relevant technical information, and the investigation process used by the AI.

CASE STUDY

Enforcing policy and IR

Darktrace/OT monitors connections in and out of the OT environment at a large geographically distributed organization. This organization uses a Secure Remote Access Solution (SRAS) to grant remote personnel access to OT systems.

Because Darktrace ingests logs from the SRAS, it was able to alert the security team to a suspicious remote access attempt. Darktrace determined the user's remote access account has become compromised, and a malicious actor is attempting to access critical control systems.

Darktrace autonomously blocked the remote connection by updating Firewall rules via an integration. Even without the integration, Darktrace can respond by taking a native response against the jump host, such as blocking matching internal connections to prevent the attacker from reaching further OT devices.

Additionally, the victim organization leverages Darktrace to enforce incident management policies. While Darktrace autonomously responds to the compromised remote access, the security team is prompted with additional human confirmable respond actions:

- Block all incoming connections to the industrial control system via Darktrace pushing preset rules to the firewall at the security perimeter.
- Isolate the endpoint device of the user with compromised endpoint device via Darktrace/Endpoint.
- Force logout or lock the remote access account of the end user via integration with the remote access solution.

Streamlined workflows for OT/ICS specialists

OT engineer

Provides an operations-focused dashboard for control engineers. This includes a subset of alerts with high operational relevance that are suitable for those with typical controls engineer domain knowledge. This feature grants access to immediate information on emerging threats for fast triage, with the aim of minimal interface time. Further, drawing on Darktrace's native ability to evolve alongside changes in the ecosystem, no tuning is necessary.

OT explore

Enables a top-down visualization of the OT environment. This provides a time-bounded snapshot of connectivity and also allows users to drill down into the subnet and device level. This can surface unexpected relationships through tags, such as clusters of similar devices not associated prior to exploration.

Vulnerability and asset tracking

Darktrace's ability to passively identify assets eliminates the risk of operational disruption. Based on the behavior of devices, Darktrace autonomously catalogues IP-connected and non-IP ICS devices. This allows Darktrace/OT to create a profile and full history of all devices seen on network. This device data is fully searchable with Advanced Search, Elastic Search, API, and OT threat detection models.

Additionally, Darktrace provides an active identification module to be used where desired. The active identification module makes requests to known OT devices to identify them using their observed and current protocol and service port combination.

Gaining visibility into assets in industrial environments is a challenge due to the diversity of devices used in OT and ICS ecosystems, from decades old legacy devices that are retrofitted, to cutting edge IIoT.

Reduce time to triage and report security events

OT security teams are simultaneously suffering from a skills shortage and tight budgets, remaining perpetually understaffed.

Darktrace's Cyber AI Analyst augments security and operation teams, providing actionable insights, closing knowledge gaps between IT and OT specialists. By conducting autonomous investigations across IT and OT that automatically triage all unusual behavior and connects the dots among disparate events, AI Analyst generates incident reports which are 'human readable' spelled out in attack phase terminology.

Darktrace's analysis has shown that this reduces time to triage by an average of 92%, putting security teams in a position to immediately take action, allowing them to better maintain availability and integrity as an attack emerges.

Organizations operating critical infrastructure must often comply with legislation like the US Cyber Incident Reporting for Critical Infrastructure Act, requiring prompt cyber incident reporting. Cyber AI Analyst's high-level summaries of incidents also helps organizations that need to generate incident reports for these compliance regulations, using AI-generated natural language summaries to accelerate this process, making it considerably easier for organizations to hit government deadlines.

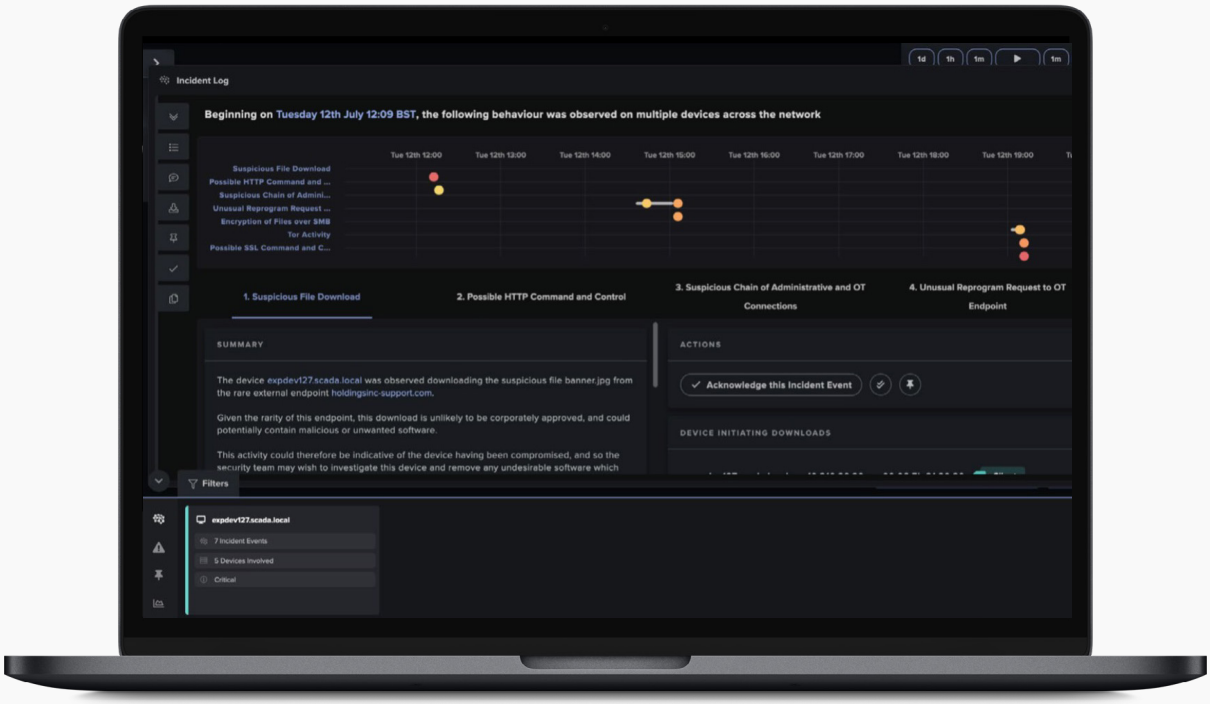


Figure 4: Darktrace's Cyber AI Analyst detecting anomalous encryption of a suspicious chain of ICS administrative credentials

Attack Case Studies

Hundreds of critical infrastructure providers across oil and gas, energy and utilities, manufacturing, transportation, and smart cities rely on Darktrace to protect their control environments against all forms of cyber-threat. With years of experience defending highly complex and diverse control systems, Darktrace/OT has become the leading AI technology for industrial cyber defense that works across all existing OT technologies – and is ready for future ones too.

> With its ability to self-learn what's normal for our organization and take action autonomously, Darktrace's Cyber AI has fast proven to be our team's most valuable assistant.
>
> / CIO, Manufacturing and Supply

CASE STUDY

Protecting industrial IoT

The mass adoption of IIoT devices has made industrial environments more complex and more vulnerable than ever. Darktrace recently detected a series of pre-existing infections in Industrial IoT (IIoT) devices at a manufacturing firm in the EMEA region.

Self-Learning AI recognized a device exploiting the SMBv1 protocol in order to attempt lateral movement. Darktrace also detected the device abusing default vendor credentials for device enumeration. The device made a large number of unusual connections, including connections to internal endpoints of which the company had previously been unaware. As these occurred, Darktrace illuminated the unusual activity's spread from the infected device across the infrastructure.

In total, Darktrace identified 13 infected production devices. This 'unknown known' threat was detected without any prior knowledge of the devices, their supplier, or patch history, and without using malware signatures or IoCs.

By casting light on this previously unknown threat, Darktrace enabled the customer to perform full incident response and threat investigation before the attack caused any serious damage to the company.

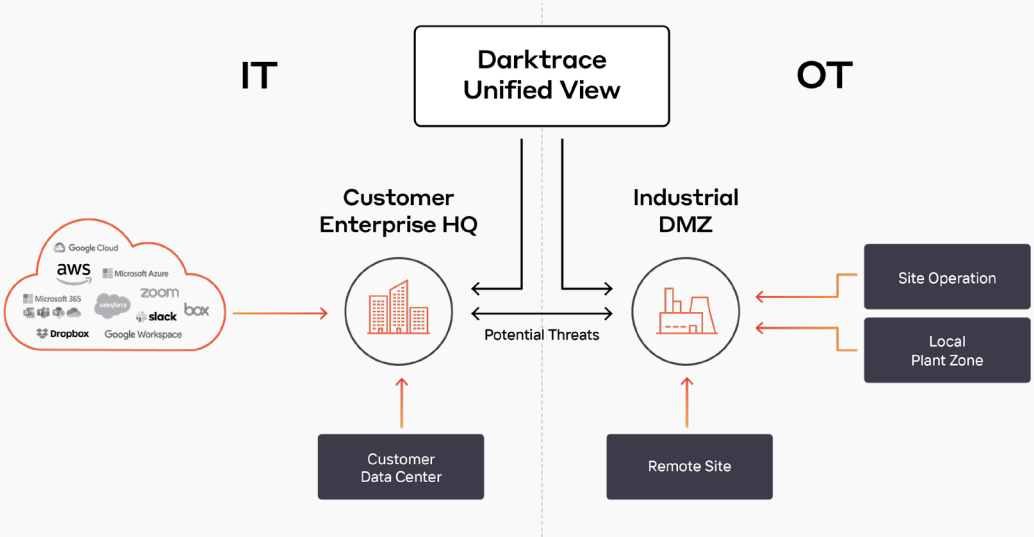


Figure 5: Darktrace's unified view provides complete visibility across IT and OT

CASE STUDY

Conti ransomware

In late 2021, Darktrace identified a Conti ransomware attack targeting an OT R&D investment firm in Europe.

A compromised domain controller led to the infection of several devices, which performed network reconnaissance as the attacker began to escalate their privileges within the organization.

The ransomware payload was delivered when infected OT devices used SMB to connect to a folder on the domain controller and read a malicious executable file. This payload stayed dormant for some weeks while cryptomining software was installed elsewhere on the network. The device made successful C2 connections to around 40 unique external endpoints, and Darktrace detected beaconing-type behavior over suspicious TCP/ SSL ports including 465, 995, 2078, and 2222.

Darktrace detected every stage of the intrusion, and Cyber AI Analyst stitched together many forms of unusual activity across the compromised devices to give a clear security narrative containing details of the attack. Had the target organization deployed Autonomous Response, or reacted to Darktrace's threat notifications, this ransomware attack would have been stopped in its earliest stages. The incident report for the Historian server is shown below. This provides a clear illustration of how Cyber AI Analyst can close any skills or communication gap between IT and OT specialists.

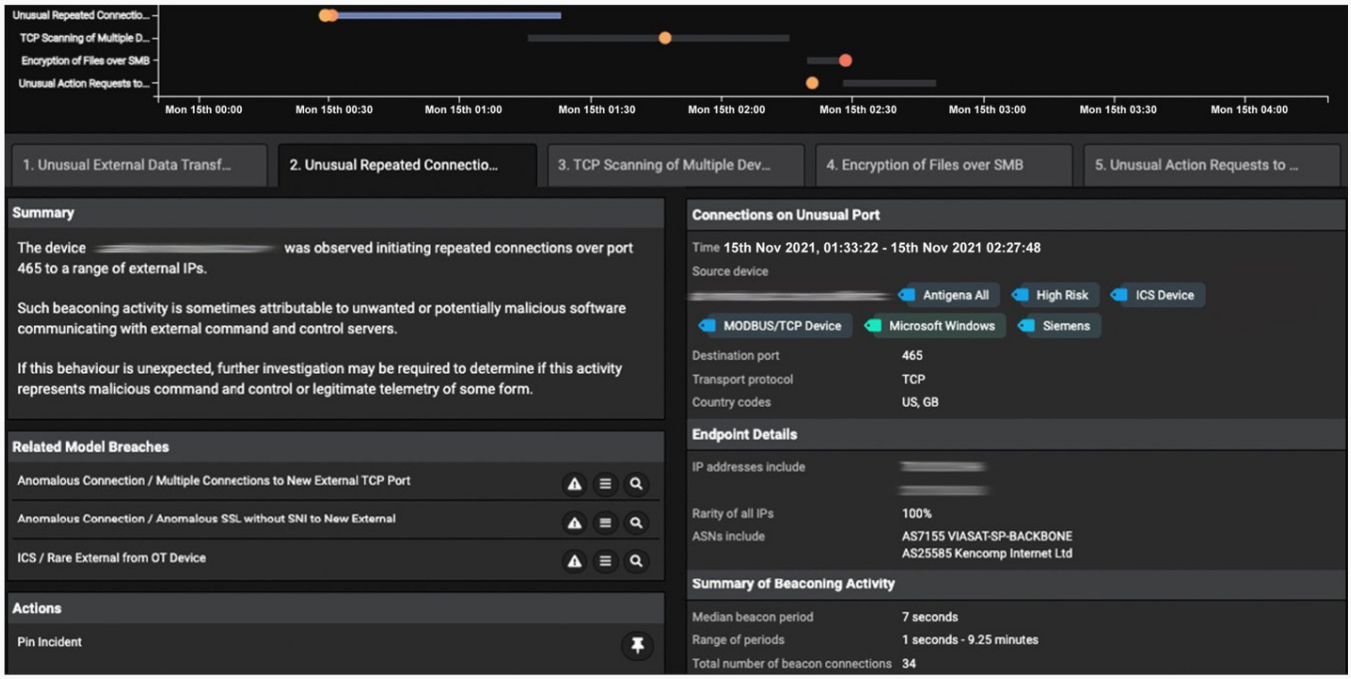


Figure 6: Cyber AI Analyst of the Historian server (abc-histdev). It investigated and reported the C2 communication (step 2) that started just before network reconnaissance using TCP scanning (step 3) and the subsequent file encryption over SMB (step 4).

CASE STUDY

Spotting insider threats

Darktrace/OT detected a subtle deviation from normal behavior when a reprogram command was sent by an engineering workstation to a PLC controlling a pump, an action an insider threat with legitimized access to OT systems would take to alter the physical process without any malware involved.

In this instance, AI Analyst, Darktrace's investigation tool that triages events to reveal the full security incident, detected the event as unusual based on multiple metrics including the source of the command, the destination device, the time of the activity, and the command itself.

As a result, AI Analyst created a complete security incident, with a natural language summary, the technical details of the activity, and an investigation process explaining how it came to its conclusion. By leveraging Explainable AI, a security team can quickly triage and escalate Darktrace incidents in real time before it becomes disruptive, and even when performed by a trusted insider.

> Cyber AI can detect cyber-threats before damage is done – whether they arise from an employee or from the industrial systems on our production floor. You need AI in place to quickly identify and respond to threats – you truly can't put a dollar value on Darktrace.

/ Director of Infrastructure and Technical Services, Produce Manufacturing

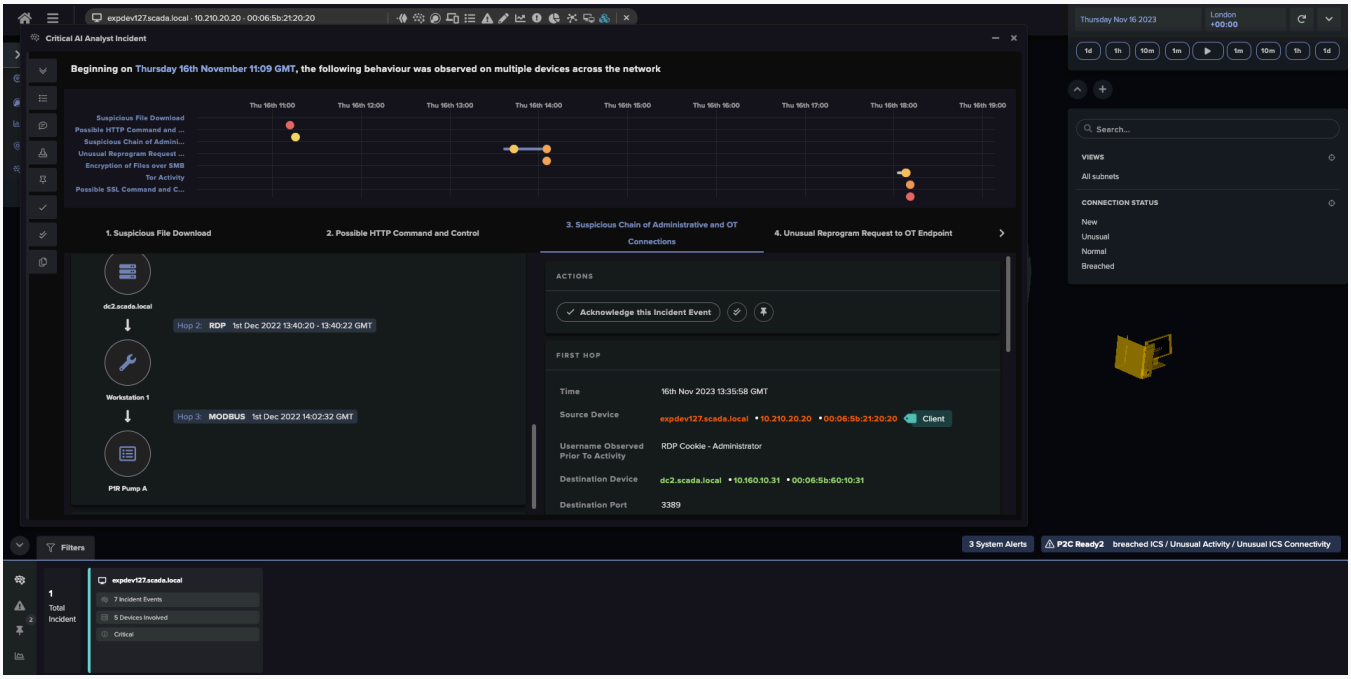


Figure 7: AI Analyst revealing a suspicious chain of OT and administrative connections

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. Breakthrough innovations from its R&D Centers have resulted in over 145 patent applications filed. Darktrace employs over 2,200 people around the world and protects c.8,800 organizations globally from advanced cyber-threats.

Scan to
LEARN MORE

DARKTRACE
Evolving threats call for evolved thinking™

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
Latin America: +55 11 97242 2011
info@darktrace.com

darktrace.com