The Immune System Approach

Cyber AI for Industrial Control Systems

Contents

Introduction

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. As IT security teams become accountable for securing Operational Technology (OT) and OT-specialist teams similarly inherit responsibility for traditional IT security, this technical convergence requires the synergy of both specialist skills and working practices.

Compromised OT devices within ICS and SCADA environments can lead to enormous physical damage and danger to human life. Since the widely reported discovery of the Stuxnet attack in 2010, threats to industrial systems have increased in both number and capability.

Today's malware campaigns can actively acquire critical data about control systems, quietly maintain persistent access and then reprogram them, completing the kill chain. Legacy defenses such as firewalls have become antiquated and inadequate, especially in detecting threatening insiders with privileged access. Increasingly sophisticated machine-speed attacks, alongside ever-rising control system vulnerabilities has heralded a new era of OT cyber-threat.

The Industrial Immune System

The Industrial Immune System is a Cyber AI Platform for OT environments which detects and autonomously responds to threats, regardless of whether they appear on legacy tool blacklists or are completely novel zero-day attack techniques. Its intelligent understanding of the entire digital estate allows it to recognize even subtle signals of emerging threats in real time.

The technology provides complete visibility across OT, IT, and industrial IoT in a unified view, giving security teams complete oversight of its decision-making.

It works by passively analyzing the 'pattern of life' for every user, device and controller, enabling the technology to recognize dangerous anomalies in behavior. Technology and protocol agnostic, it can be deployed across both OT and IT environments, providing full coverage of an organization without disrupting daily operations.

The Challenge of Securing OT

Convergence with Traditional IT

Even when operating in the same organization, corporate IT systems and Industrial Control Systems will have different objectives. Control engineers have historically been unimpeded by cyber-threats emerging through corporate IT systems and IT security staff have had little contact with control systems or the physical equipment that those systems manage.

However, intensified competition resulting from globalization has propelled the convergence and synergy of the cyber-physical realm and more general and disparate information networks. Increasingly accountable for both OT and IT security, CISOs have also assumed responsibility for the security of ICS environments without necessarily possessing the specialized OT skills.

The most likely attack vector for ICS compromise is the IT network – this has been true of all major publicly known OT-targeted malware campaigns, as well as known cases of indiscriminate IT malware affecting OT systems.

Discovering threats while still within the corporate network will vastly increase the defense-in-depth of the control system. Pre-emptive threat detection will protect confidential data about the control system which would potentially include detailed operational diagrams, device details and efficiency and safety reports.

The organizational changes that come with the convergence of OT and IT systems present new and significant technological risks, but also provide an opportunity for improving OT security and resilience. Sharing a common network architecture will enable monitoring and detection strategies across both domains.

> “Enterprises that require a cyber security solution for IT, OT and physical environments will find Darktrace an effective tool for real-time advanced threat detection.”
>
> **- Earl Perkins of Gartner, Cool Vendors in Energy & Utilities**

Industrial Internet of Things

In addition to developments resulting from converging OT and IT systems, the scope of Operational Technology is broadening with the rise of Industrial Internet of Things (IIoT) devices integrated into traditional ICS environments. The IoT paradigm presents two challenges – more complex and dynamic networks, and the deployment of new, unique technology.

There has been a dramatic increase in the number of connected devices in industrial environments, bearing significant implications for security teams. As the attack surface has expanded, complete visibility of the digital environment has become increasingly complex and unattainable.

As the shift towards IIoT introduces myriad device classes, there is wide-spread change across all forms of networked communications. The increasing availability of smart, small form-factor devices is reorienting computing away from monolithic platforms towards highly distributed nodes. IoT devices are typically connected in wireless topologies, with processing and analytics distributed close to the last mile in “edge” and “fog” computing designs. Particularly in Smart Grids providing electricity to customers across entire districts, this means a broadened attack surface endangering millions of homes.

Difficulties in ICS Security

Whilst effectively designed to be interoperable and resilient, industrial control systems are not necessarily easy to secure, 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. It has become clear that any possible connection to the internet can be exploited, even if it is not direct.

Meanwhile, patching is extremely difficult, as the in-built methods for delivering updates in an operational environment are unsuited to the requirement for 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.

Threats Facing Industrial Control Systems

ICS environments face numerous cyber security threat vectors with varying degrees of potential loss, ranging from non-compliance to disruption of operations which could result in the destruction of property and potential loss of human life. Examples of potential ICS-related threats include:

- Advanced Persistent Threats (APTs), including OT-targeted campaigns that bring together leading IT malware and OT control system attack skills
- Insider sabotage
- Supply chain disruption and compromised vendors or contractors
- Human misconfigurations
- Distributed Denial of Service (DDoS) attacks, resulting from increased use of the internet as an OT data transport mechanism

In June 2010, the Stuxnet virus targeted PLCs in Iranian nuclear centrifuges, marking the first revealed instance of targeted malware to cause physical damage, and propelling the vulnerability of ICS into public consciousness. Since then, several high-profile attacks have hit manufacturers and utilities, including an attack targeting the Ukrainian power grid, as well as the closure of a French power plant in the Middle East after malware had compromised its control systems.

Spillover from Corporate Network Compromises

Industrial control systems are often damaged as unintended side effects 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 major US power stations have been publicly attributed to this method of attack.

Additionally, the 2017 WannaCry ransomware attack that affected the IT systems of organizations across multiple verticals and geographies caused severe disruptions to manufacturing facilities across the world. Such incidents demonstrate that indirect compromise poses as significant a threat to operational environments as successful targeted attacks against ICS.

Insider Threat

Over the lifecycles involved with the building and utilization of infrastructure and manufacturing equipment, many individuals will have interacted with control systems and supporting physical equipment. Many of them will have had access privileges, allowing them to modify configurations or the underlying software and hardware.

Such increased ICS exposure allows malicious insiders' actions to be well-targeted and effective at disrupting operations. Insiders will not encounter border defenses and have a greater ability to masquerade as others, making their activities harder to identify and attribute. Where supply chains or contractors are involved, it becomes increasingly impossible to distinguish between the 'inside' and 'outside'.

Whilst vetting and training staff can reduce the risk of insider threat, there is still the possibility of a misconfiguration, or a deliberate act of sabotage by a disaffected or ideologically motivated individual.

Monitoring complex networks needs to start from a complete understanding of what is normal for the unique environment. Only then can it have the insight to identify the emerging patterns and correlated actions that indicate threat.

Ukrainian Power Grid

In 2015 and 2016 the Ukraine experienced the first known instance of an extensive and focused cyber-attack targeting the power grid at scale. These highly sophisticated attacks utilized advanced malware designed to compromise SCADA environments, and left thousands of citizens without power for several hours. Since these incidents, the US Department of Homeland Security has issued warnings that long-term attack campaigns against the energy sector are ongoing.

Triton Attacks

In 2017, a multinational corporation was forced to shut down operations of a power plant in the Middle East after malware compromised its industrial control systems. The attackers used sophisticated malware, dubbed "Triton", to take remote control of safety systems and attempted to reprogram them, causing related processes to shut down. Security researchers reported in 2019 that the same hacking group are targeting the industrial control systems' of utility companies in the US, Europe, East Asia, and the Middle East.

The Industrial Immune System

Organizations providing critical infrastructure must now look to a cyber security technology that delivers continuous insight and provides early warning of both indiscriminate and targeted compromises.

Darktrace's AI technology is a cutting-edge innovation that implements a real-time 'immune system' for operational technologies and enables a fundamental shift from the traditional approach to cyber defense. Built on a foundation of Bayesian mathematics and unsupervised machine learning, the system analyzes complex network environments to learn a 'pattern of life' for every network, device, and user.

Rather than relying on knowledge of past attacks, the technology learns what is normal for its environment, discovering previously unknown threats by detecting subtle shifts in expected behavior. Through identifying these unexpected anomalies, security teams are able to investigate malware compromises and insider risks as they emerge and throughout all stages of the attack lifecycle.

> "Darktrace's machine learning approach is unmatched. We are now finding anomalies, in real time, that would have taken us weeks, or even months, to find on our own."
>
> **- Terrell Johnson, Manager of Systems and Networks, Sunsweet**

Sunsweet is the world's largest manufacturer of dried fruit. Darktrace protects Sunsweets' physical machinery and sensitive data.

Real-Time Detection of Emerging Threats

The traditional approach of blacklisting historical attack types cannot keep up with the pace of emerging vulnerabilities. Darktrace does not require a priori assumptions about environments or threats, and can therefore detect the 'unknown unknowns'; threats that are as yet unidentified, either because they are novel or have been tailored to a particular defender.

Darktrace continues to adapt and self-learn throughout its entire deployment. It does not require operators to manually maintain or instruct its understanding, allowing them to spend their limited time benefitting from the output.

Whenever an abnormal change to behavior takes place within the environment, the Industrial Immune System identifies deviations from the learned 'pattern of life' and alerts the organization to the possible threat. Because Darktrace's AI builds an evolving understanding of its network, it is vendor and protocol agnostic and can adapt and evolve to any operational environment.

The advanced mathematics that Darktrace leverages make it uniquely capable of highlighting significant potential threats without burying them beneath many insignificant or repeating alerts. Far more than a set of simple rules applied to network traffic, it can correlate many subtle indicators separated by type or time into strong evidence of a real emerging threat, meaning that security analysts are not flooded with false positives.

Passive Observation

While connecting new devices into a corporate network is generally risk-free, straightforward and routine, the same is not true of industrial networks, where for many applications even the slightest interruption in service could be damaging.

The Industrial Immune System typically runs on a server that is connected passively to an ICS network, receiving copies of as much communication traffic as possible. It receives copies of raw network data using the built-in port mirroring or "spanning" capabilities of network switches, or using fail-safe taps, sometimes via an aggregator to bring together numerous connections in one location.

For cloud, edge, and physical deployments, Darktrace's lightweight, host-based OS-Sensors are installed on each cloud endpoint and configured to send intelligent copies of network traffic to a local vSensor deployed in the same cloud environment.

Deep Coverage at Scale

Modern OT networks are deliberately segregated following the principles laid out and refined over time in the Purdue model architecture. Through monitoring network traffic, the Industrial Immune System has direct visibility and provides cyber security for everything from Level 1 (Basic Process) through supervisory functions (2, 3), DMZs, business logistics and enterprise networks (4, 5) and beyond into Cloud networks and SaaS services. It also has indirect visibility into Level 0 (Process) as information about it transits the higher Levels.

From single appliances monitoring small localized networks, the Industrial Immune System can be scaled all the way to multi-national businesses with millions of devices. Cyber AI is the only technology capable of handling threat detection in complex environments. Unlike simpler methods, that inherently scale linearly with the number of devices, connections or bandwidth in the network, Cyber AI takes advantage of the increased context available when judging the likelihood of a cyber-threat to scale its alerts far more effectively.

Cyber AI Analyst: Augmenting Security Teams

Cyber AI Analyst is a feature within the Industrial Immune System that uses AI to automatically triage threats and generates at-a-click investigation reports, drastically augmenting the capability of security analysts.

Powered by supervised machine learning, AI Analyst replicates expert human decision-making, forming hypothesis and reasoning to reach informed and insightful conclusions. The Industrial Immune System then presents a coherent security narrative of the overall incident in a matter of seconds.

Security teams that oversee both OT and IT as a result of digital transformation projects experience a huge increase in productivity as a result of using the Industrial Immune System. Both new and unknown threats are automatically investigated, and time to triage is reduced by 92%.

> "Darktrace Industrial is fundamentally changing the game of ICS cyber defense."
>
> **- Michael Sherwood, Director of IT, City of Las Vegas**

The City of Las Vegas adopted Darktrace's Industrial Immune System to protect the thousands of Industrial IoT devices in operation throughout the city's wastewater facilities.

Unified Visibility across OT, IT and IoT

Architectures of ICS and their operational networks are complicated and will typically have undergone many changes by multiple individuals over their lifetime. 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 allows 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.

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. 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 AI continuously compares this activity against expected and intended patterns.

Whilst the Threat Visualizer interface 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) system, to integrate with established processes and procedures.

Darktrace Proof of Value

Darktrace's Proof of Value (POV) allows organizations to experience first-hand the Industrial Immune System's ability to detect previously unseen threats and anomalous behaviors within a customer's industrial environment. During the POV, Darktrace provides access to the Threat Visualizer for use as well as weekly, custom-made Threat Intelligence Reports.

> "Artificial intelligence is now vital to our security posture, as it is flexible enough to defend our entire SCADA environment, including diverse legacy systems."
>
> **- Kevin McCauley, Director of Networking, Utilities Kingston**

Utilities Kingston

Utilities Kingston provides utility services to tens of thousands of customers in Ontario, Canada, including water, wastewater, electricity, natural gas, and fiberoptic broadband. Darktrace's Industrial Immune System protects the entire infrastructure.

Fig.1: The Threat Visualizer displays a graphical, real-time overview of the industrial environment and allows for in-depth investigations

Darktrace Discoveries

Suspicious Downloads and Serpent Ransomware Infection

At an integrated oil refiner and supplier, Darktrace's Industrial Immune System identified the first signs of a ransomware infection in the company's network. As well as writing its own ransom note files, a desktop device was found to be making a series of connections to rare external destinations, via an internal proxy server, and then downloading potentially malicious files.

The device proceeded to make a number of SMB directory queries, amplifying the anomalous series of actions that the Industrial Immune System converted into multiple high-priority alerts relating to the device. Darktrace's Industrial Immune System recognized that this activity closely matched the typical pattern of behavior for the ransomware, alerting the customer's security team before the infection was able to spread into the OT environment.

Internal Reconnaissance Detected within OT Network

At a US manufacturing company, the Industrial Immune System highlighted a known but rarely active device within an OT network suddenly broadcasting multiple dedicated OT protocol commands for devices using that protocol to respond with their identities. While the control system as a whole often used this command in various ways as part of its normal operations, this particular use was found to be unusual for several reasons.

The activity in this case proved to be benign, but most modern OT campaigns that used a specialized protocol payload performed a very similar step as part of their reconnaissance stages.

Reconnaissance Detected from Blacklisted External Device

Internal reconnaissance was detected at the heart of a US oil and gas production company. A rare internet endpoint that had never interacted with the customer's network before was discovered connecting to several key elements of the network infrastructure, using a VPN.

After briefly connecting to the domain controller, it then connected to an employee's computer and the mail server, attempting to gain access via three different entry points. The Industrial Immune System detected this malicious exploration attempt in its earliest stages, giving the security team the ability to reinforce its defenses and ensure no compromises occurred.

> "There's no denying the benefit that Darktrace delivers."
>
> **- Martin Sloan, Group Head of Security, Drax**

Drax Group is Britain's fifth largest non-domestic energy supplier and the biggest supplier of renewable power to UK businesses.

Conclusion

Security teams in the OT space increasingly find themselves having to defend against attacks entering through the IT network. This convergence, alongside complex and evolving OT environments are creating conditions in which cyber-attacks against operational systems are becoming increasingly frequent and effective.

With Darktrace's self-learning Industrial Immune System, organizations are able to detect and respond to emerging threats in real time, irrespective of device protocols, operating systems or other characteristics that make OT networks unique from one another. Its AI algorithms automatically form an understanding of these diverse environments, and also protect the IT network, enabling full visibility and protection.

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, the Industrial Immune System has become the leading AI technology for industrial cyber defense that works across all your existing OT technologies – and is ready for your future ones too.

> "Signature-based malware detection is dead. Cyber security needs a quantum leap forward. It needs to rely on machine learning-based artificial intelligence."
>
> **Senior Fellow, Institute for Critical Infrastructure Technology**

Learn more

darktrace.com | @darktrace | LinkedIn