DARKTRACE
INDUSTRIAL

Cyber Security for Industrial Control Systems: A New Approach

WHITE PAPER

Introduction

Industrial Control Systems (ICS) underpin individual businesses and National Critical Infrastructure around the world. They maintain control of power stations and nuclear plants, water distribution systems and manufacturing sites – and today, they are routinely targeted by cyber attackers looking to spy on, compromise and damage those organizations.

Historically, industrial networks were kept separate from corporate networks, but significant efficiency gains and a broad trend for digital interconnectivity have driven a convergence between Operational Technology (OT) and Information Technology (IT) systems. Adoption of new control technologies, and the introduction of the Industrial Internet of Things (IIoT) are also increasing the complexity and interconnectedness of traditional OT environments.

The business of cyber security has changed dramatically in the past few years, presenting a significant challenge to management teams across all industries and business domains. A report conducted by the Cybersecurity Research Group found that 67% of companies with critical infrastructure experienced at least one cyber-attack in the last year and 78% expected their ICS and SCADA systems to be exploited in the next two years.

We see an increasing trend toward IT security teams taking on more accountability and responsibility for securing the OT systems, which require different specialist skills and working practices. This cultural and technical convergence will bring a steep learning curve that must be overcome.

Increasingly exposed to the same attack vectors used in the majority of cyber-attacks, OT devices within ICS and SCADA environments are inherently harder to secure, but their compromise can lead to enormous physical damage and danger to human life. The critical nature of ICS environments also makes securing these devices more challenging than in IT environments. Ever since the Stuxnet malware was widely reported in 2010, threats to industrial systems have grown rapidly in both number and capability. This was made clear in, among others, the 2014 compromise of a German steel mill that caused massive damage to a blast furnace and the 2015 and 2016 attacks against the Ukrainian power grid.

Ongoing malware campaigns are actively acquiring critical data about control systems, while quietly maintaining persistent access. Existing defenses such as firewalls have repeatedly proven inadequate on their own, especially against insiders who already have privileged access. The security community is increasingly coming to the consensus that we are entering a new era of serious OT cyber-threat, with ever rising numbers of vulnerabilities being found in control system devices.

> **Darktrace's Industrial Immune System is a fundamental innovation that views data from an ICS network in real time, and establishes an evolving 'pattern of life' for operators, workstations and automated systems.**

Darktrace uses machine learning and AI algorithms to detect and respond to cyber-threats that get through perimeter controls and evade rule-based approaches that can only identify previously-seen threats. Darktrace's Industrial Immune System technology is deployed across both OT and IT environments to provide full coverage of an organization.

"The threat landscape is evolving so fast, and threats are becoming so sophisticated. It's becoming near impossible to keep up. Darktrace's machine learning is clearly the way forward."

Ken Soh, Chief Information Officer
BH Global

ICS and SCADA

ICS is an umbrella term covering many historically different types of control system such as SCADA (Supervisory Control and Data Acquisition) and DCS (Distributed Control Systems). Also known as IACS (Industrial Automation and Control Systems), they are a form of Operational Technology involving the supervision and coordination of control devices – sensors and actuators deployed to monitor and influence physical processes. In practice, media publications often use "SCADA" interchangeably with "ICS".

Corporate Information Technology (IT) systems and Industrial Control Systems have different objectives, even when operating within the same organization. While OT and IT often speak different languages, cyber-attacks across both environments have continued to evolve to become more targeted and destructive. When it comes to ICS, safety and reliability are the primary concerns as attackers aim to disrupt the critical services customers rely upon.

OT and IT systems are converging, driven primarily by economic pressures resulting from globalization and intensifying competition, along with the benefits and eventual competitive advantages that stem from the integration of these disciplines. Such benefits include: cost reduction, increased control, enhanced performance and business optimization.

> **The cost is significantly higher to remediate a system than to detect a cyber threat early, not only in time and money, but also in safety and reputation.**

Having been traditionally separate domains, the convergence of OT and IT poses an operational and strategic challenge for organizations as well as a technical one. An integrated security strategy requires CISOs to reshape current enterprise security practices as well as develop new OT security capabilities and functions.

Increasingly accountable for both OT and IT security, CISOs have had to assume responsibility for the security of ICS environments without necessarily possessing specialized OT skills. This organizational change threatens to present a new range of change-management and technological risks. In this environment, development of an effective unified approach to security strategy will become an urgent operational priority.

However, the architectural changes that come with convergence can provide an opportunity for improving OT security. Sharing of a common network architecture can open the door for unified monitoring and detection strategies across both OT and IT domains, as well as the extension of modern IT traffic monitoring approaches to ICS networks.

"Signature-based malware detection is dead. Cyber security needs a quantum leap forward. It needs to rely on machine learning-based artificial intelligence."

James Scott, Senior Fellow,
Institute for Critical Infrastructure Technology

Industrial Internet of Things

In addition to the changes brought about through convergence, the scope of Operational Technology is broadening with the adoption of Internet of Things devices into traditional ICS environments. The Internet of Things is causing wide spread change across all forms of networked communications through the introduction of new device classes. The availability of smart, small form-factor devices is increasingly driving a shift in computing away from monolithic platforms towards highly distributed nodes.

In the industrial space, the Industrial Internet of Things (IIoT) refers to the adoption of IoT architectures and device types into control environments, augmenting PLC based systems with distributed sensor grids. This new paradigm had significant implications for the design, and security of control environments. Sensor grids dramatically increase network complexity and the number of connected devices. These devices are typically connected in wireless topologies, with processing and analytics distributed close to the last mile in “edge” and “fog” computing designs. In Smart Grid deployments, this is expanding the potential attack surface of the ICS out into millions of customer’s homes.

ICS Cyber Security Issues

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 destruction of property and potential loss of human life.

Examples of potential ICS-related threats include:

- Advanced Persistent Threats (APTs)
- Unintended spillover of corporate network compromises
- Disruption of voice & data network services
- Coordinated physical & cyber-attack
- Insider sabotage
- Hacktivist attacks
- Supply chain disruption or compromise
- Catastrophic human error
- Distributed Denial of Service (DDOS)

Historically, industrial control environments were relatively isolated from corporate networks and the internet. However, computer viruses and other forms of cyber-attacks have been known to bridge the gap by exploiting security holes related to the handling of removable media, or simple human error.

While security is an upside of having a seemingly closed or isolated system, the downsides include limited access or inability to access enterprise decision making data or to allow control engineers to monitor systems from other networks. Additionally, ICS often ties together decentralized facilities such as power, oil and gas pipelines, water distribution and wastewater collection systems, among many others, where the network is hard to physically secure.

ICS systems, whilst effectively designed to be interoperable and resilient, are not necessarily easy to secure. With the increasing number of connections between ICS systems, corporate networks and the internet, combined with the move from proprietary technologies to more standardized and open solutions, they are becoming more susceptible to the kind of network attacks that are found more commonly in IT environments.

Cyber-security researchers are particularly concerned about the systemic lack of authentication in the design, deployment and operation of some existing ICS networks and the belief that they are completely secure simply because they are physically secure. It has become clear that any possible connection to the internet can be exploited, even if it is not direct. ICS-specific protocols and proprietary interfaces are now well documented and easily exploited. The use of a VPN (Virtual Private Network) is also not sufficient protection for ICS users as this can be trivially bypassed with physical access to network switches and never provides end-to-end coverage. Supply chain risks and remote access requirements from vendors and service supplies present an often unknown level of risk for otherwise segregated environments.

"Darktrace adds another level of sophistication to our defense systems, and had already identified threats with the potential to disrupt our networks."

Martin Sloan, Global Head of Security, Drax

Vulnerability

While it is likely that many attacks are never revealed to the public, the list of known compromises is growing. The most notorious incident that arguably propelled the vulnerability of ICS into the mainstream consciousness was the discovery of the Stuxnet attack in June 2010, a "weaponized" form of malware. Since then several high-profile attacks have been seen against manufacturers and utilities, while others go under the radar, including long-term cyber espionage campaigns.

There are an increasing number of threat actors with both the motivation and capability to compromise industrial control networks and devices. The consequences of compromise range from damaging to catastrophic, from immediate physical harm to long-term industrial espionage.

Control engineers historically have not had to worry about cyber threats coming through corporate IT systems, while IT security staff have had little to do with the fundamental differences in control systems or the physical equipment that those systems manage. ICS devices are inherently insecure, and extremely difficult to update with even the rudimentary protections that are possible.

A 2016 industry report found that attacks targeting ICSs increased over 110% compared to the previous year, and a 2017 SANS study found that 69% of ICS security practitioners believe threats to the ICS systems are high or severe and critical.

Sabotage and Shutdowns

ICS networks have also been damaged as unintended side effects of problems starting in corporate networks that took advantage of increasing connectivity, proving clearly that the standard PCs that now form part of a typical ICS are open to the same compromises as their enterprise counterparts. At least three problems at major power stations have been publicly attributed to this; the Davis-Besse nuclear power station (Ohio, USA) when safety systems were crippled by the Slammer worm, the Browns Ferry nuclear power station (Alabama, USA) being manually scrammed as a result of a drastic increase in network traffic, and the Hatch nuclear power station (Georgia, USA) due to a faulty software update on a business network machine that communicated with the control network.

Additionally, the 2017 WannaCry ransomware attack that

affected the IT systems of organizations across multiple verticals and geographies caused severe disruptions to Honda's manufacturing facilities. Such incidents demonstrate that indirect compromise poses as significant a threat to operational environments as successful targeted attacks against ICSs.

German Steel Mill

At the end of 2014 hackers struck an unnamed steel mill in Germany. This was a targeted Advanced Persistent Threat (APT) compromise, beginning with a spear-phishing attack that enabled the hackers to gain initial access to the office network of the steelworks. From there, they were able to successfully explore the company's networks and eventually manipulate and disrupt the production networks. Failures of individual control components accelerated, resulting in a blast furnace being unable to shut down which caused "massive" damage to the installation.

Havex

Havex was targeted against ICS customers by using a highly effective 'watering-hole' attack, where the attackers compromised three legitimate ICS vendor websites and replaced real software updates with versions already containing the malware. There was no possible way for traditional network defenses such as border firewalls to protect against this, and standard procedures employed in many corporations would have trusted the 'trojanized' updates and added them to internal whitelists of software for authorized use. If an environment is infected in this manner, only its unique behavior, once installed on the ICS network, could be used to detect Havex's presence.

Ukrainian Power Grid

In 2015 and 2016 the Ukraine experienced the first known instances of deliberate cyber-attack targeting the power grid. These attacks utilized advanced malware designed to compromise SCADA environments, known as BlackEnergy, and Industroyer. These highly sophisticated attacks demonstrated the existence of specialized tools capable of compromising an ICS, as well as the feasibility and achievable consequences of such attacks. Since these attacks the Department of Homeland Security has issued warnings that long term attack campaigns against the energy sector are on-going.

Insider Threat

Threat from 'trusted' insiders is an important consideration for OT environments. Over the long lifecycles involved with the building and utilization of infrastructure and manufacturing equipment, a large number of different individuals, including both permanent staff and short-term contracted specialists, will usually have interacted with control systems. Many of them will have had privileges that allow them to modify configurations or the underlying software and hardware.

Vetting and training staff can reduce but not eliminate the risk of insider incidents from occurring. These incidents can be unintentional due to a mistake or intended short cut that puts something important at risk, or a deliberate act by a disaffected or ideologically motivated individual. The increased access and organizational familiarity that insiders have means their malicious actions can be very well targeted and effective at disrupting operations. They also have a greater ability to interfere with monitoring or masquerade as others, making their activities harder to identify and attribute.

Insider risk is a serious challenge often underestimated in breadth. When supply chains or contractors are involved, it becomes impossible to draw a neat line between 'inside' and 'outside'. We need to trust people in our extended organizations with the access and privilege that they require in doing their jobs, but we also need mechanisms to identify when something is going wrong and needs to be corrected.

Traditional network border defenses such as firewalls perform an important function in a complete cyber-security solution, but insiders are a key example of their limitations. Insiders do not have to pass through border defenses to accomplish most of their potential goals, meaning that those defenses have no chance at all to prevent or identify their actions.

> **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.**

A New Approach: Darktrace and the Immune System

Utilities, OT-centric industries and other national infrastructure organizations, are challenged with rethinking cyber security across all technologies to deliver continuous insight that provides early warning of both indiscriminate and targeted compromises, supported by mechanisms that can manage incidents before they become a business crisis. Total prevention of compromise at any cost is untenable, however, detection and response to prevent a crisis from developing is an achievable cyber security goal in an OT/IT environment.

Darktrace's Industrial Immune System is a cutting-edge innovation that implements a real-time 'immune system' for operational technologies and enables a fundamental shift in 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.

The technology does not rely on knowledge of past attacks. Instead it operates like the human immune system, and can discover previously unknown threats by detecting subtle shifts in expected behavior.

By identifying unexpected anomalies in behavior, defenders are able to investigate malware compromises and insider risks as they emerge and throughout all stages of the attack lifecycle.

"Enterprises that require a cybersecurity 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 and Utilities, March 2015

Darktrace Technology

New vulnerabilities are emerging at a pace that is difficult to keep up with, and looking only for published historical attack types is an unsuitable approach for operationally important environments. Darktrace does not require *a priori* assumptions about environments or threats, and can therefore detect the 'unknown unknown' threats that are as yet unidentified, either because they are novel or have been tailored to a particular defender.

> **The Darktrace architecture continues to adapt and self-learn throughout its entire deployment. This ability to adapt means that no new or customized threat has the ability to hide from Darktrace.**

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. Changes that are not real threats are incorporated into Darktrace's evolving understanding of normality.

The advanced mathematics inside Darktrace 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.

Darktrace's Threat Visualizer interface can be used to triage and investigate these detections, but 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.

Passive Observation

Connecting new devices into a corporate network is straightforward and routine, with little attached risk. The same is not true of industrial networks, where for many applications even the slightest interruption in service could be damaging. This is why larger and more critical networks are left as untouched as possible between planned outages.

The Darktrace appliance runs on a server that is connected passively to an ICS network, receiving copies of as much communication traffic as possible. It does not interfere with the operation of the control network in any way, flagging anomalies for investigation but not attempting to influence the situation. The appliance 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.

ICS networks are deliberately segregated into Trust Levels as defined by the ISA95/Purdue reference model, depending on how much each device on the network is trusted to behave as expected. Darktrace can be connected at Level 2 (supervisory control), Level 3 (data servers) and Level 4 (IT networks) to provide defense in depth. It also extends cyber-security coverage down into Level 1 (field devices).

A highly flexible, distributed architecture allows Darktrace to securely cover multiple Trust Levels and the wide variety of network topologies within and between them. Examples include wholly separate appliances for each Trust Level, or multiple appliances within a widely distributed single Trust Level with a master appliance providing a single interface. If required, a network diode device could guarantee that a channel for moving data from one Trust Level to a higher Trust Level to reach a single appliance covering both cannot be used to communicate in the other direction.

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 in a situation in which Darktrace is monitoring both.

Visibility Into ICS

Architectures of ICS and their operational networks are often documented to a standard that exceeds corporate equivalents, but these long-lived environments are complicated and will typically have undergone many changes by multiple individuals over their lifetime. Knowing and understanding what is genuinely happening inside the environment can be a real challenge. Darktrace addresses this challenge by observing, analyzing and capturing communications along with their associated metadata.

In addition to its core identification of anomalous activity and possible compromise, Darktrace's Threat Visualizer interface uniquely displays all this rich information in an intuitive 3D dashboard that allows the operator to get a true and real-time overview of what is happening. This can be used to investigate whether the control system's real behavior matches its intended design.

In ICS environments segregation and zoning of the network is a critical security control, especially given the often inherent lack of security within endpoint devices themselves. In such environments, understanding the correct flow of data on the network and how it compares to expected conduits and patterns of communication is essential. The Threat Visualizer allows OT security teams to view real time information about data flows within the Industrial network, and compare this against expected and intended patterns.

Darktrace's Industrial Immune System retains all of the capabilities of Darktrace in the corporate environment, and will ideally be deployed observing both the ICS and corporate networks. The most likely attack vector for ICS compromise is the IT network. Discovering threats while still within the corporate network vastly increases the defense-in-depth of the control system. This also protects confidential data about the control system stored on corporate servers, which might include detailed operational diagrams, device details or efficiency and safety reports.

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 own environment. Along with the POV, Darktrace provides access to our Threat Visualizer for use during the POV as well as weekly Threat Intelligence Reports produced by its team of cyber security specialists. Some organizations prefer to trial Darktrace on their corporate IT systems to confirm the passive and secure operation before engaging installation into ICS networks.

"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

Conclusion

Businesses face many challenges as we move into an era of ever increasing connectivity. Those trying to secure industrial control systems as well as corporate networks face additional and substantially different problems, as the devices involved are far less secure than their corporate counterparts.

There is public evidence of growing motivation and capability of threat actors towards control systems, a trend likely to continue and brought into sharp focus by the attacks over the past few years. Most of these attacks used state-of-the-art methods to reach the control systems of targets with little political or ideological significance, a combination not previously observed.

De-risking the OT environment is a perpetual challenge requiring new technologies that will deliver continuous insight and provide early warning of both indiscriminate and targeted compromise. Total prevention of compromise seems effectively impossible for the foreseeable future, but prevention of crises is an achievable goal across both corporate IT and operational technology environments.

A new approach that can manage incidents across corporate IT and OT before they become an operational crisis is required. With Darktrace's self-learning immune system, organizations are able to detect and respond to emerging threats in real-time. Machine learning and AI algorithms can detect even previously unseen, novel or tailored attacks, regardless of whether they originate in the corporate IT or OT domains or traverse them.

With ICS deployments in 5 countries across oil and gas, manufacturing and transportation sectors, critical infrastructure providers now 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 machine learning and AI technology for industrial cyber defense.

"Darktrace is the clear leader in anomaly detection."

Eric Orgen, 451 Research

About Darktrace

Darktrace is the world's leading machine learning company for cyber security. Created by mathematicians from the University of Cambridge, the Enterprise Immune System uses AI algorithms to automatically detect and take action against cyber-threats within all types of networks, including physical, cloud and virtualized networks, as well as IoT and industrial control systems. A self-configuring platform, Darktrace requires no prior set-up, identifying advanced threats in real time, including zero-days, insiders and stealthy, silent attackers. Headquartered in San Francisco and Cambridge, UK, Darktrace has 30 offices worldwide.

Contact Us

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