GURUCUL

Critical Infrastructure

Get Proactive Against Cyber Threats with Gurucul's Next-Gen SIEM

As threats against the nation's critical infrastructure continue to grow, public sector and private organizations alike need to get more proactive about protecting their digital assets.

Critical Infrastructure is a Massive Target for Cyberattacks

Many cybersecurity attacks are targeted toward critical national infrastructure like pipelines, communications, transportation, and utilities. Even large financial institutions can be considered part of the nation's infrastructure, given that prolonged disruptions in their operations could have devastating effects on the U.S. economy. It's more important than ever that these types of organizations deploy a proactive approach to defense against cyber threats.

Cyberattacks against critical infrastructure have increased in recent years, according to U.S. cybersecurity officials at Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the government body that helps companies investigate attacks against ICS and corporate networks. Many such cyberattacks come from nation-states such as Russia, China, North Korea, and Iran. Russia alone accounts for 58 percent of all cyberattacks against the U.S., according to data from Microsoft, followed by attacks coming from North Korea.

Why Attack Infrastructure?

Malicious actors have various motivations for attacking critical infrastructure (CI). Some use ransomware to extort money from owners and operators. Others want to obtain intellectual property that can be used to create competitive products or services. And some attackers are looking to do economic damage or cause physical harm—especially since the world has entered a new sort of Cold War where cyberwarfare is now a routine component of military arsenals.

Consider the following:

- In 2021, ransomware was the number one attack vector on critical infrastructure, according to a report by the industrial cybersecurity company Dragos. Water plants in Nevada, Maine, and California were all hit with ransomware in 2021. Companies like Colonial Pipeline are willing to pay millions of dollars in ransom in order to restore order to their business. Unfortunately, paying the ransom doesn't guarantee the ability to fully restore the organization's data. The average company only restores 65% of its data following a ransom payment.

Gurucul really stood out because the analytics engine was the most powerful. The machine learning algorithms are the strongest. We saw results very, very quickly.

- William Scandrett
CISO, Allina Health

- The Commission on the Theft of American Intellectual Property estimates that annual costs from IP losses range from $225 billion to $600 billion. American Semiconductor Company reported a $1 billion loss in market value when a Chinese company stole source code for small industrial computers used in wind turbines. What's more, China's "copycat" Air Force advanced quickly after the country stole engineering plans from U.S. firms.
- Research conducted at the University of Surrey highlights there has been a 100% rise in significant nation-state incidents between 2017-2020. Over 40% of incidents analyzed involved a cyberattack upon assets that also had a physical component. For example, a hacker tried to poison a California water supply by deleting programs that the water plant used to chemically treat drinking water.

The fact is, cyberattacks on our nation's critical infrastructure can support the national interest, business advantage, and military goals of a hostile country, at a lower cost and risk than a direct physical attack.

For Cyber Defense, There's Strength in Numbers

One of the challenges is that much of the critical infrastructure in the U.S., including pipelines, communication facilities, and energy systems, is owned by private companies rather than government entities. This puts the onus on the corporate owner to pay for and implement cybersecurity defenses and execute an effective response if an attack occurs. Even in the face of regulatory requirements that mandate cybersecurity protections – such as those imposed by NERC-CIP – the private owner is alone in choosing precisely what measures to deploy, and how to deploy them. This results in spotty and disjointed coverage of cyber defenses among the nation's CI facilities.

In addition, many CI companies operate in an ecosystem that makes multiple companies dependent on each other. For example, an energy grid is comprised of numerous electricity generators, bulk power transmission companies, energy storage companies, local operators, and more. If one aspect of the grid fails due to cyberattack, others may fail too. Thus, infrastructure enterprises must band together to help protect the whole ecosystem from cyberattacks.

The Federal government is already encouraging, and in many ways coordinating, such cooperation. The National Council of ISACs is a collection of member-driven organizations, delivering all-hazards threat and mitigation information to asset owners and operators. There are numerous ISACs that are aimed at critical infrastructure industries and organizations. One purpose of the ISACs is to share with members threat intelligence that can be fed into SIEMs and other security solutions.

The Cybersecurity & Infrastructure Security Agency (CISA) is the national coordinator for critical infrastructure security and resilience. The agency works across public and private sectors to engage with government, industry, academic, and international partners to come up with effective ways to counter cyber and physical threats to critical infrastructure. The goal is to build a collective defense against the threats organizations face.

Gurucul uses external threat intelligence from CISA, the ISACs, and various other sources to keep current with cyber threats.

Gurucul's Next-Gen SIEM Platform Helps CI Organizations Stay Ahead of Threats

Cybersecurity solutions have traditionally focused on information technology environments. However, today's tools are evolving to go beyond IT to include IoT and OT devices as well. This is critically important, given the trend of IT/OT convergence. OT is no longer secure by virtual of obscurity;

Tools are evolving in other ways as well. Cloud-native solutions take away the burdens of on-premise tools, including installation, operation, and maintenance. More importantly, machine learning and artificial intelligence are now integral components that allow modern solutions to quickly decern improper behaviors that may indicate a threat to the environment.

Gurucul's cloud-native Next-Gen SIEM leverages machine learning behavior profiling with predictive risk-scoring algorithms to predict, detect and prevent attacks leading to deployment of malware, corruption or exfiltration of data, fraudulent activity, and other risks. It also reduces the attack surface and eliminates unnecessary access rights and privileges to increase protection.

A key differentiator of our Next-Gen SIEM is that it includes User and Entity Behavior Analytics (UEBA) and Identity Analytics.

UEBA Is Essential to Monitor OT and IoT Devices

UEBA is especially important in the realm of critical infrastructure, where the behavior of non-human entities such as OT devices (e.g., PLCs, SCADA, DCS, CNC, etc.) and IoT devices (e.g., sensors, actuators, machines, etc.) must be monitored for unusual behavior that may be indicative of intrusion.

Gurucul UEBA focuses on the detection of risks and threats beyond the capabilities of signatures, rules, and patterns. Instead, UEBA uses machine learning models to detect unknown threats early in the kill chain. It quickly identifies anomalous activity, thereby maximizing timely incident or automated risk response. This is the most realistically effective approach to comprehensively manage and monitor user and entity centric risks.

Using big data, Gurucul provides risk-based behavior analytics delivering actionable intelligence for security teams with low false positives. Gurucul is able to consume the most data sources out-of-the-box and leverages the largest machine learning library. Additionally,

we deliver a single unified prioritized risk score per user and entity. This enables organizations to find threats – unknown unknowns – quickly with no manual threat hunting and no configuration, and get immediate results without writing queries, rules, or signatures. And because Gurucul's platform operates from the cloud, it can scale to monitor millions of users and devices in near real time.

Gurucul's Identity Analytics Reduces the Access Plane for Cyber Threats

Stolen or abused user identities, especially privileged identities, are often used to make an initial illicit foray into a network, or to move around laterally to search for assets and systems to compromise. Gurucul Identity Analytics (IdA) comprehensively manages and monitors identity-based risks and threats across an organization's siloed environments. Using big data, Gurucul provides a holistic 360-degree view of identity, access, privileged access, and usage in the cloud, on mobile, and on-premises. IdA reduces the access plane by detecting and removing access risks, access outliers, and orphan or dormant accounts. This improves an organization's security posture by significantly decreasing the number of accounts that can be compromised or abused.

Identity Analytics delivers the data science that improves IAM and PAM, enriching existing identity management investments and accelerating deployments. IdA surpasses human capabilities by leveraging machine learning models to define, review, and confirm accounts and entitlements for access. It uses dynamic risk scores and advanced analytics data as key indicators for provisioning, de-provisioning, authentication, and privileged access management. The objective is to clean up the access plane to enable access only where it should be provided.

Gurucul Provides One Unified Platform for Cyber Risks

In short, Gurucul's Next-Gen SIEM technology delivers one platform for cyber risks spanning security, identity, and fraud. Gurucul enables you to:

- ✔ Centralize and streamline access to cybersecurity data to drive analytics for identifying and managing risks
- ✔ Predict, detect, and prevent data breaches, insider threats, and other risky activity
- ✔ Protect essential information and data on premise and in the cloud
- ✔ Eliminate unnecessary access rights and excessive privileges to increase protection
- ✔ Meet and surpass regulatory compliance mandates including NERC CIP
- ✔ Adhere to threat framework models for cybersecurity protection such as MITRE ATT&CK and the NIST Cybersecurity Framework.

About Gurucul

Gurucul is a global cyber security company that is changing the way organizations protect their most valuable assets, data and information from insider and external threats both on-premises and in the cloud. Gurucul's real-time Cloud-Native Security Analytics and Operations Platform provides customers with Next Generation SIEM, XDR, UEBA, and Identity Analytics in a single unified platform. It combines machine learning behavior profiling with predictive risk-scoring algorithms to predict, prevent, and detect breaches. Gurucul technology is used by Global 1000 companies and government agencies to fight cybercrimes, IP theft, insider threat and account compromise as well as for log aggregation, compliance and risk-based security orchestration and automation for real-time extended detection and response. The company is based in Los Angeles. To learn more, visit gurucul.com and follow us on LinkedIn and Twitter.

Gurucul | 222 North Pacific Coast Highway, Suite 1322 | El Segundo, CA 90245 | 213-259-8472 | sales@gurucul.com | www.gurucul.com