VULNERABILITY MANAGEMENT AND REMEDIATION

REAL WORLD THREATS

Lessons from the Aurora Vulnerability

In 2007, the Department of Homeland Security, working with the Idaho National Laboratory, undertook to demonstrate that a cyberattack could, in fact, cause real-world physical damage. It had already been known that cyberattacks could destroy computer equipment by creating anomalous behavior in hard drives and by overclocking microprocessors; the goal of this test was to determine if the manipulation of various control components could damage or destroy large infrastructure. The test was a success as it proved it could be done. However, it also determined the vulnerability it revealed could be difficult to mitigate. The test was code named "Aurora" and is known as the "Aurora vulnerability".

The root cause of the Aurora vulnerability is poor physical security and poor cybersecurity. The aurora vulnerability, if not mitigated, can extensively damage much of the equipment connected to the grid, and could cause extended power outages. The attack does not have to happen at the generator or the substation; it can be initiated from anywhere.

Click to Read More

Rising Cyber Threat: Oldsmar Water Treatment Facility Attack

A computer controlling the water treatment system in Oldsmar, Florida, was remotely accessed on Friday. Oldsmar is a suburb 15 miles northwest of Tampa Bay with a population of about 15,000 residents.

In the Oldsmar water treatment facility attack, the hacker accessed the software system and increased the sodium hydroxide content from 100 parts per million (ppm) to 11,100 ppm. The operator that detected this was able to bring the water content back to normal. There is no immediate danger to the people who rely on the plant for drinking water.

As a result, there is a growing need for manufacturers and operation managers to secure vulnerable computers, nodes and other access points (APs) from hackers. These APs, which used to be isolated and cut off from the internet, are now part of the Industrial Internet of Things (IIoT), which brings different devices together to help them communicate and interact with one another.

Click to Read More

How a Cyberattack Caused Physical Damage at German Steel Mill

In 2015, details emerged from a cyberattack that caused "massive damage" to a blast furnace at a German steel mill. This was the second-ever digital attack that caused physical harm to equipment and served as a potential harbinger of future, destructive attacks on critical infrastructure.

According to The 2015 annual report from the German Federal Office for Information Security (BSI) report, hackers infiltrated the German steel mill's business network via a spear-phishing attack, a targeted, social engineering hack in which a bad actor, disguised as a trusted source, tricks a target into clicking a link that implants malware into the system.

Once the attackers gained access, they crossed over into the mill's other networks, including those that controlled plant equipment. This caused several areas to fail, and operators were unable to shut down a blast furnace properly, which resulted in the damage. This kind of cross breach is a common problem in the age of digital transformation, where almost everything is on a network.

Click to Read More

VULNERABILITY MANAGEMENT AND REMEDIATION

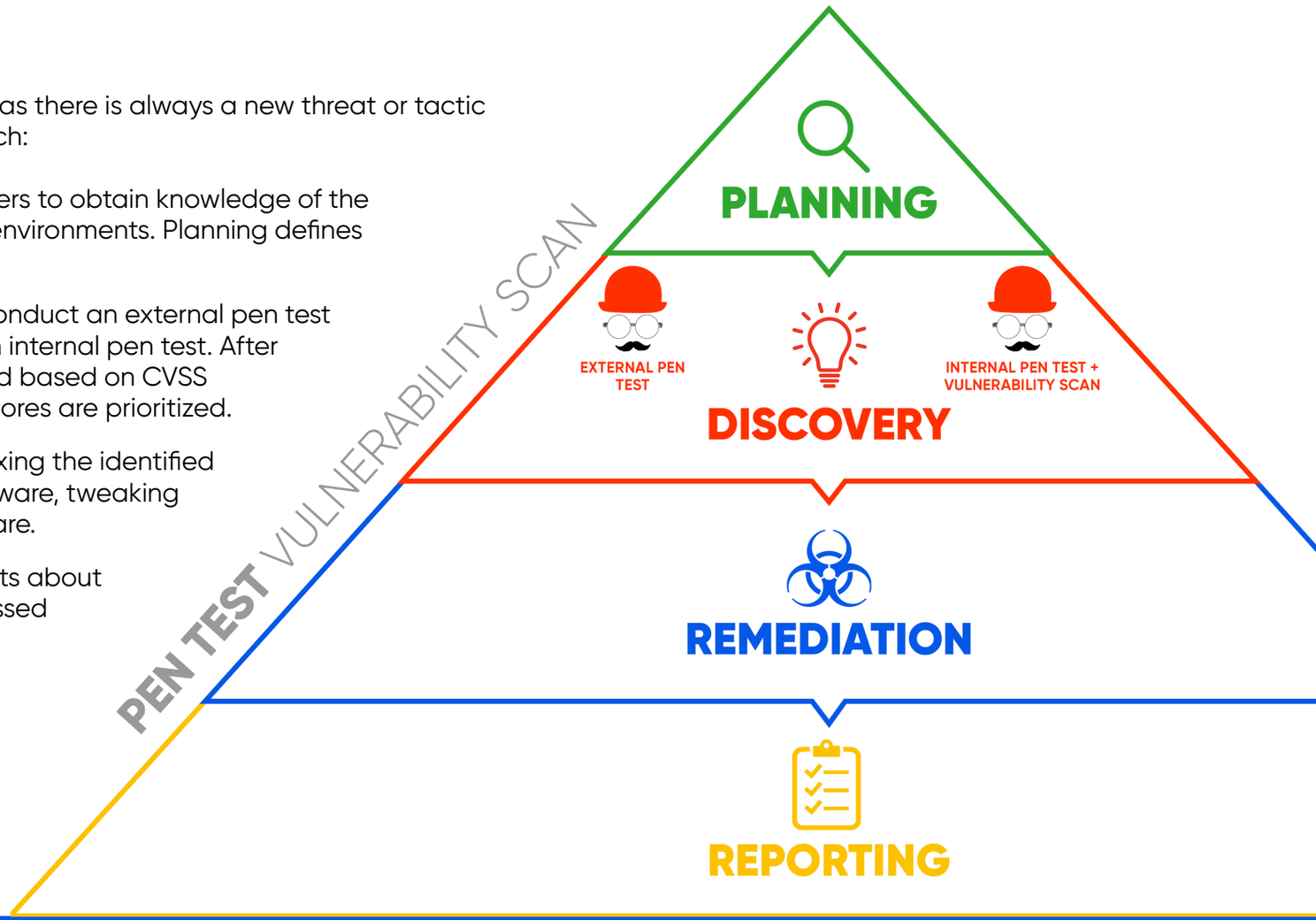
OUR FOUR-STEP APPROACH

BCS365

How Does it Work?

Vulnerability management is an ongoing process, as there is always a new threat or tactic to remediate. These four steps outline our approach:

1. **PLANNING:** The Planning phase allows the testers to obtain knowledge of the architecture and system configurations in the environments. Planning defines what is in the scope.
2. **DISCOVERY:** During the Discovery phase, we conduct an external pen test to scan for vulnerabilities. This is followed by an internal pen test. After identifying vulnerabilities they are assessed and based on CVSS (Common Vulnerability Scoring System), and scores are prioritized.
3. **REMEDIATION:** Remediation is the process of fixing the identified vulnerabilities. This might involve patching software, tweaking configurations or, sometimes, replacing hardware.
4. **REPORTING:** The final step is to generate reports about the vulnerabilities found, how they were addressed and what actions are needed in the future. This ensures that the management team is well-informed about the security state of the business and can make strategic decisions accordingly.



VULNERABILITY MANAGEMENT AND REMEDIATION

FOR BUSINESS INFRASTRUCTURE

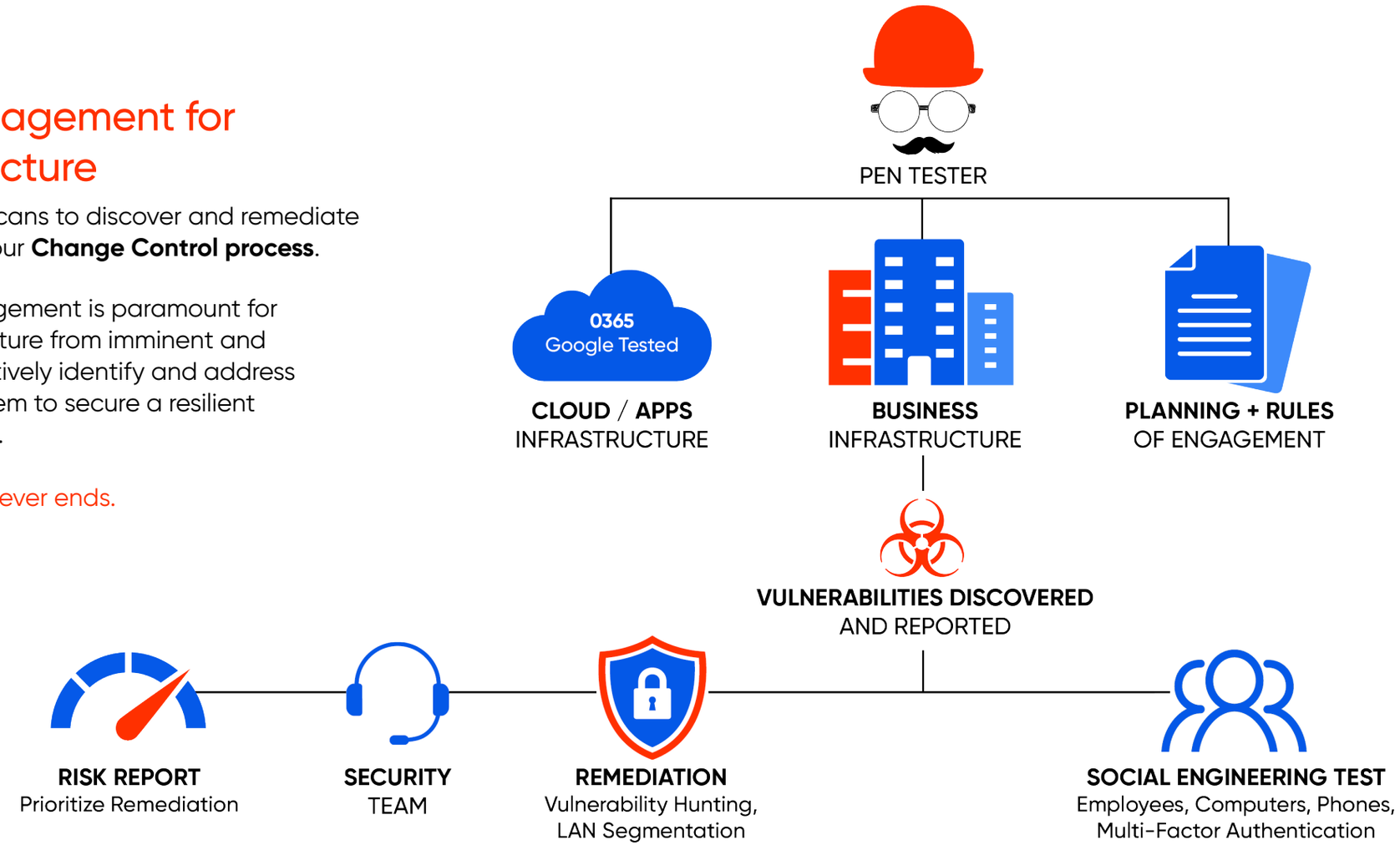
BCS365

Vulnerability Management for Business Infrastructure

BCS365 conducts monthly scans to discover and remediate critical vulnerabilities using our **Change Control process**.

Effective vulnerability management is paramount for safeguarding your infrastructure from imminent and potential threats. We proactively identify and address weaknesses within your system to secure a resilient foundation for your business.

Vulnerability Management never ends.



888-886-5767 sales@BCS365.com BCS365.com

PROTECT YOUR BUSINESS

WITH OUR VULNERABILITY MANAGEMENT AND REMEDIATION SERVICES

BCS365

What's Included?

- **Integrated Suite of Security Products:** Our program offers an integrated suite of advanced security products to safeguard your email communications. From robust firewalls to sophisticated encryption tools, we provide a comprehensive solution to protect your sensitive information.
- **Prioritization of Security:** We prioritize the security of your endpoints above all else. Our program ensures that potential threats are swiftly identified and addressed, minimizing the risk of data breaches and ensuring business continuity.
- **Utilization of Threat Intelligence:** By leveraging advanced threat intelligence, we stay one step ahead of cyber threats. Our program utilizes real-time data and analysis to proactively detect and respond to potential security incidents.
- **Rapid Response and Actions:** In the event of a security incident, our expert team is ready to take immediate action. We swiftly analyze the situation, assess the impact, and implement the necessary measures to neutralize the threat, ensuring minimal disruption to your business operations.
- **Threat Remediation:** Our program goes beyond incident response. We work closely with your organization to eliminate vulnerabilities and strengthen your overall security posture. By addressing the root causes, we help prevent future incidents and enhance your security resilience.
- **Review of Post-Incident Reports:** Learning from past incidents is crucial for continuous improvement. Our program includes a thorough review of post-incident reports, allowing us to identify areas for enhancement and strengthen your security infrastructure.

How We Do It

UEBA

UEBA, which stands for User Entity Behavior Analytics, utilizes machine learning to scrutinize raw data, produce behavior profiles, and identify irregular behavior. This helps in recognizing advanced attacks, thus improving the overall security system.

MITRE ATTACK

Mitre Attack is a framework that provides advanced detection policies, which can detect incidents in real-time. It offers a comprehensive and structured approach to detecting, responding to, and recovering from cyber-attacks.

CUSTOM DETECTION POLICIES

Custom detection policies designed by BCS365 can be used to alert on specific events that matter the most to the user. For instance, alerts can be generated when users are added to sensitive groups, sign-ins are made from unapproved countries, or users access specific SharePoint sites.

ALERT AGGREATION

Alert aggregation is an essential process that collects alerts from all areas of the Microsoft tenant. This ensures that all alerts are reviewed with the necessary urgency, thus preventing any potential security breaches.

Invest in our Vulnerability Management and Remediation Program today and gain peace of mind knowing that your network is protected by a comprehensive and proactive security solution. Safeguard your business from cyber threats and ensure the confidentiality of your valuable data.

888-886-5767 sales@BCS365.com BCS365.com