Upskill your team with CodeRed for Enterprise.

**OUR BEST RESOURCE TO UPSKILL YOUR CYBERSECURITY TEAM’S PRODUCTIVITY**

Upskill your IT teams with custom curriculum mapping, dedicated course development that targets your organization’s needs, and deep analytics that always puts you in the driving seat of your team’s training.

**BROWSE COURSES IN YOUR FAVORITE CATEGORIES**

- Network Security
- Secure Programming
- Information Security
- Data Science
- Cloud Computing

**CUSTOMIZATION PUSHED TO THE LIMIT**

Your teams’ needs are at the heart of every enterprise offering we provide so you can see real relevant results. Fast!

- Create custom course Bundles
- Assign users
- Track learning through dashboard

Our top program architects help you assess the skill gaps in your teams, and then customize a learning path that addresses those gaps.

**Custom Curriculum Mapping**

We can even work with our industry-leading authors to create special programs just for your team.

**Custom Course Development**

You can also design and assign different learning paths to different groups within your organization to target specific knowledge gaps.

**Assign Personalized Learning Paths through bundles**

Upskill your team with CodeRed for Enterprise.
Join Expert-Led Webinar on

**IoT Based Attacks in the Healthcare Industry:**
Do You Know How to Respond?

📅 15th July 2021
🕒 7.30 pm IST / 8.00 am MST / 9.00 am CDT

Register Now!

Key Issues to be Addressed:
1. How is IoT used in the healthcare industry?
2. What are the major impacts of IoT in the healthcare industry?
3. Types of IoT-based attacks on healthcare devices
4. How to respond to such attacks.

Moderator:
**Amol Kodag**
Engineering Director – R&D, Medtronic,
Heading Cardiovascular Portfolio
at Medtronic Engineering and Innovation Center (MEIC)

Panelists:
**Scott E. Augenbaum**
Retired FBI Supervisory Special Agent / Cyber Division

**Ricoh Danielson**
Executive Cyber Security Advisor of Incident Response and Digital Forensics at 1st Responder LLC – A Cyber Security Firm

Worried About Rising IoT Attacks in the Healthcare Sector?
The Colonial Pipeline attack on May 7 was a watershed moment in the universal fight against ransomware attacks. It was the first incident in which the ransom paid to attackers was recovered. The attack on Colonial impacted the fuel supply chain, leading to a temporary fuel shortage along the Northeast coast of the U.S. The pressure was building for Colonial Pipeline and their CEO, Joseph Blount, to make a difficult decision – paying up. In an interview with the Wall Street Journal, Blount acknowledged he authorized the ransom payment of 75 Bitcoin, which is approximately $4.4 million. A few weeks later, the Department of Justice and the FBI announced that they recovered most of the ransom amount.

In his blog post dated June 16, Brian Krebs, Editor of KrebsOnSecurity, reported that the Ukraine Cyber Police arrested six people from the CLOP ransomware group. The gang reportedly extorted ransom of $6 million. Cyber Police arrested six people from the CLOP ransomware group. The gang reportedly extorted more than half a billion dollars from victims.

Ransomware attacks are now an everyday occurrence. A report from Cybersecurity Ventures estimated a ransomware attack on businesses every 11 seconds in 2021. While there are numerous debates about whether impacted companies should be paying the ransom, we could soon have legislation for this. Last year, the Department of the Treasury's Office of Foreign Assets Control (OFAC) published an advisory informing the public that the payment of ransom demanded by cybercriminals may be a violation of U.S. law.

For sure, there will be more ransomware attacks in the coming months. The adversaries see this as a lucrative opportunity, more so now, when the pandemic has office workers at home, with weak security on their home networks. Ransomware gangs are getting more organized with affiliate programs. They now offer Ransomware-as-a-Service – case in point, the DarkSide ransomware group that brought Colonial Pipeline to its knees. Read more about this in "The Vulnerabilities that Open the Door to Ransomware" on page 68.

So, are we just going to sit around and watch? And become the next victim?

Isn’t it time we did something about it?

The fight against ransomware attacks goes beyond private organizations, as even governments and critical infrastructure are being attacked. Immediately after the Colonial Pipeline attack, the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI issued a security advisory with mitigation steps to reduce the risk of compromise by ransomware attacks.

The increased involvement of APT groups who engage in cyber warfare would make it extremely difficult to contain ransomware attacks. This was on the agenda for discussion during the recent meeting between President Biden and Russian leader Vladimir Putin. There were similar discussions at the G7 meet in the U.K. in June.

Ransomware needs to be tackled on a global stage, with the involvement of governments, and organizations like Interpol, Europol, NIST, CERT, ACSC (Australia), National Cybersecurity Center (U.K.), and others.

Isn’t it time they banded together and fight back!
Contents

RANSOMWARE GETS MEATY WITH JBS ATTACK

INTERVIEW SPECIAL

"I expect security options to evolve over time with the rollout of 5G"

"We want to bring together incident response and security teams from every country to ensure a safe internet for all"

"I believe in building products and teams that are obsessed with customer success"

"The most hacker-resistant environment is the one that is administered from end-to-end"

"IoT technology will always improve but it will never be 100% secure"

"Let’s bring together incident response and security teams from every country to ensure a safe internet for all"

The Vulnerabilities that Open the Door to Ransomware

How Communication Service Providers are Keeping the World Connected During COVID-19

The Vulnerabilities that Open the Door to Ransomware

How Communication Service Providers are Keeping the World Connected During COVID-19

TOP CYBERSECURITY NEWS OF THE MONTH
Ransomware has by far been the buzzword of 2021. Until now, ransomware attacks only appeared under the Tech section of news dailies. However, this has changed. Stories of ransomware attacks are now front page news and make it to cover stories. The modus operandi of ransomware operators has evolved over the years. They are not just looting businesses but targeting critical sectors and larger supply chains, raising the stakes for national security. Remember the Colonial Pipeline hack, which virtually exhausted the entire gas supply on the East Coast? And the Babuk ransomware gang's attack on D.C. Metropolitan Police Department that acted as a roadblock for the law enforcement in the city? These attacks have grown manifold, and are found everywhere.

The dust of the Colonial Pipeline ransomware attack had just begun to settle as the U.S. Department of Justice's (DoJ) newly formed digital extortion task force reported recovering majority of the ransom paid (approximately $2.3 million of $4.4 million in Bitcoins) by the company to the cybercriminals. And while one company was heaving a sigh of relief, another sophisticated ransomware attack took center stage. This time, adversaries struck a meaty blow at the world's largest meat producer – JBS.
The Aftermath?

The ransomware attack on JBS' systems did not just affect its IT infrastructure; it had a ripple effect. The attack paralyzed its worldwide supply chain. It halted slaughter operations not just in the U.S. but across its units in Canada and Australia. Transactions and supplies with both – customers and suppliers – were suspended temporarily. The company issued a press release in which it deemed the incident as "organized cybersecurity attack."

Upon discovery, JBS suspended all systems and networks that were known to have been intruded on and informed the respective law enforcement authorities – CISA and FBI. The only silver-lining in the entire incident was the fact that JBS had a data backup in place. The company issued a statement confirming that its backup servers were not affected, and thus (they were) actively working with an incident response firm to restore its systems as soon as possible.

JBS did not mention how the ransomware intruded on its systems or the perpetrators involved. But certain news reports suggested that it was the evil hand of the Russian-speaking REvil ransomware gang. REvil, the notoriously infamous gang, did not post any details related to the hacking incident on their underground forum, which they call the "Happy Blog." REvil is known to post a part of the stolen data on this forum as proof for pressuring victims into meeting its ransom demands.