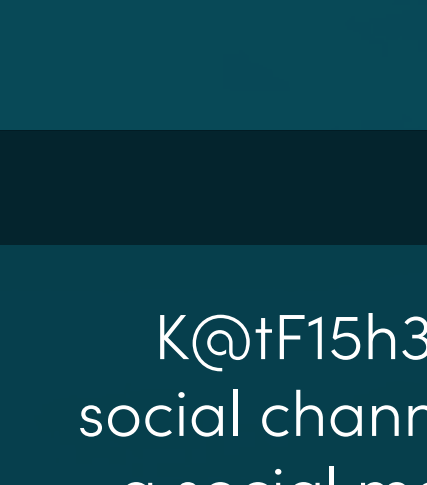


HOW WOULD YOU PROTECT YOUR CUSTOMERS AGAINST ENEMY OPERATIVES?



ENEMY OPERATIVE # 1



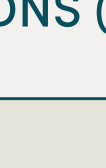
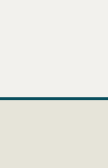
K@tF15h3D!

Social engineering racketeer. Uses ONIT (open-source intelligence) to crawl company social media feeds and websites to identify potential targets.

Attack Scenario

K@tF15h3D! sifts through the supplier websites and social channels. After spotting a senior executive without a social media profile, the threat actor quickly sets up a false online identity.

How would you protect your customers against this attack?

 Critical deployments	 Crayon solutions
DNS (Domain Name System) Filter	DNSFilter
Identity Access Management	Delinea Microsoft Netwrix
Multifactor Authentication	Microsoft
Domain Based Message Authentication Reporting and Conformance	SMX
Human Risk Management	usecure
Regular Verified Backups	Acronis Veeam Avepoint Skykick Backup365 Microsoft

ENEMY OPERATIVE # 2





H4ckP!g30n

Hacker for hire. Never sleeps. Exists on Red Bull, chocolate-coated coffee beans and the thrill of illicit financial gain.

Attack Scenario

H4ckP!g30n identifies a vulnerability which allowed them to anonymously query internal LDAP server authenticating a cloud trading platform application.

How would you protect your customers against this attack?

 Critical deployments	 Crayon solutions
Active Directory Auditing, Monitoring and Defence	Microsoft Netwrix
Identity Access Management	Delinea Microsoft Netwrix
Multifactor Authentication	Microsoft
Web Application Firewall Vulnerability testing	Invicti
Regular Verified Backups	Acronis Veeam Avepoint Skykick Backup365 Microsoft

ENEMY OPERATIVE # 3





UNC6662

Sponsored hacker group. Works in tightly coordinated sprints to rapidly exploit announced vendor vulnerabilities.

Attack Scenario

Hacking group UNC6662 is targeting boutique laboratories – and their service providers – seeking to exfiltrate and ransom high-value intellectual property.

How would you protect your customers against this attack?

 Critical deployments	 Crayon solutions
Application Allowlisting	Airlock Microsoft VMWare
Endpoint Detection and Response solutions	Trend Micro ESET VIPRE Acronis ESET
Endpoint Protection Platforms	Trend Micro ESET
Local Security Authority Subsystem Service Monitoring and Blocking	Netwrix
Regular Verified Backups	Acronis Veeam Hornet Security Probox Avepoint Skykick Microsoft

ENEMY OPERATIVE # 4





Kr@5hK@rtB@nd1Koot

Threat actor that executes attacks on e-Commerce platforms and website payment pages.

Attack Scenario

Kr@5hK@rtB@nd1Koot uses trojanised Google Tag Manager (GTM) containers to execute Magecart attacks on e-Commerce platforms and website payment pages.

How would you protect your customers against this attack?

 Critical deployments	 Crayon solutions
Dynamic Application Security Testing tools	Invicti
Privilege Access Management solution	Delinea Netwrix Microsoft
Zero Trust Network Access	Fortinet Microsoft
Cloud Access Security Broker	Microsoft
Application Allowlisting	Airlock Microsoft VMWare
Automated Patch Management	Automox Microsoft
Regular Verified Backups	Acronis Veeam Avepoint Skykick Backup365 Microsoft

Identify your customers weaknesses with a Crayon security assessment service. We offer a range of services including:



- ✔ Cloud Security Assessments
- ✔ Essential Eight Control Assessments
- ✔ Penetration testing

Did you know we offer more than 30 risk and resilience solutions and services?

Explore Crayon's Risk and Resilience Solution Stack.

[Find out more](#)