

SXQgaXMgcG9zc2libGUgdG8g
 aW52ZW50IGEgc2luZ2xlIG1h
 Y2hpbmUgd2hpY2ggY2FuIGJl
 IHVzZWQgdG8gY29tcHV0ZSBh
 bnkgY29tcHV0YWJsZSBzZXFl
 ZW5jZS4gSWYgdGhpcyBtYWNo
 aW5lIHRaZS4gY29tc2luZ2xlIG1h
 d210aSBhIHRaZS4gY29tc2luZ2xlIG1h
 IGJlZS4gY29tc2luZ2xlIG1h
 aCBpcyB3cm10dGVuIHRobSBt
 LkQgb2Ygc29tc2luZ2xlIG1h
 bmcgbWFjaGlucyB3cm10dGVuIHRobSBt
 VuIFUgd21sbCBjb21wdXQ
 RlIHRobSBzYW1lIH
 NlcXVlbnNlIG
 FzIEOuCg
 ==

CENTER FOR CYBER DEFENCE AND INFORMATION SECURITY



SWEDISH ARMED FORCES



Swedish
Defence
University



Swedish
Defence
Research
Agency

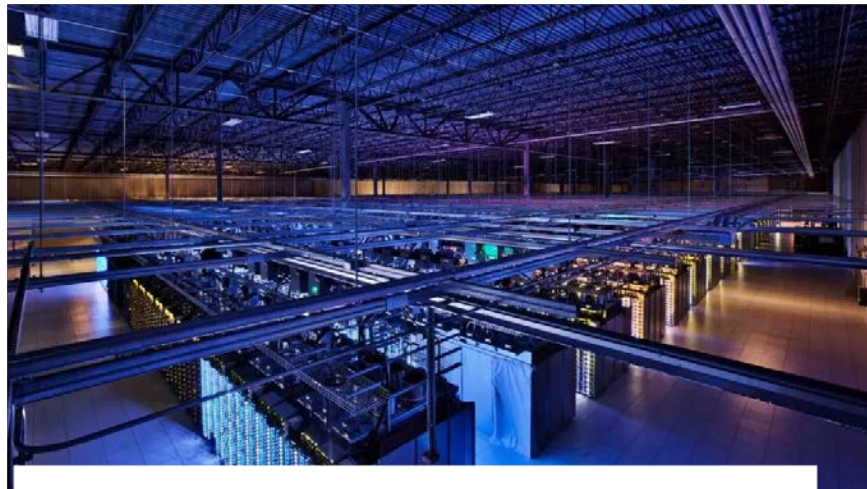


*National
Defence Radio
Establishment*

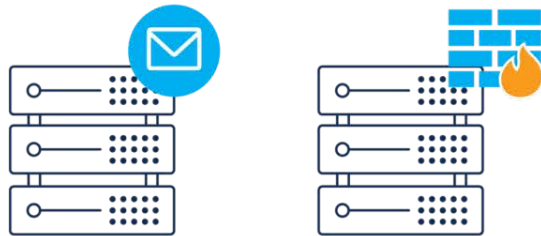


Swedish Civil
Contingencies
Agency

Over seven out of ten production workloads now execute inside a VM



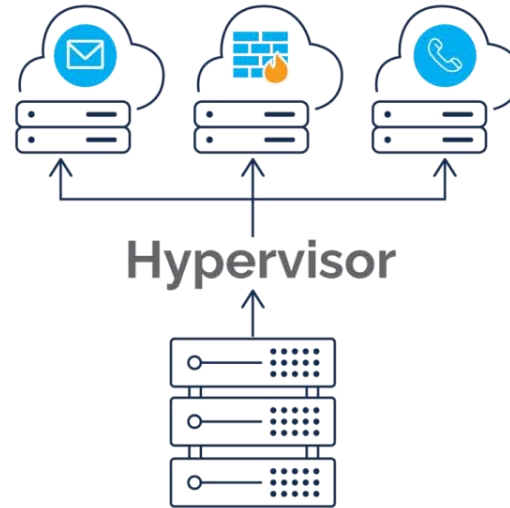
Traditional



X Cores
XX GB Ram
XXX GB HDD
30% Utilization

X Cores
XX GB Ram
XXX GB HDD
6% Utilization

Virtualization



Hypervisor

X Cores
XX GB Ram
XXX GB HDD
60% Utilization

5X2gaXNgcPec1l1b0q608g
w02Jm0f0g0c1w2Jm101a
Y2h0m0g2h0f0gY2P10G1
2w02g0g0f0c1w2Jm101a
h0gY2P10G1w2Jm101a
2w02g0g0f0c1w2Jm101a
w02Jm0f0g0c1w2Jm101a
a02g0g0f0c1w2Jm101a
Lk0g02g0f0c1w2Jm101a
h0gY2P10G1w2Jm101a
VulP0g2Jm101a
w2Jm101a
h0gY2P10G1w2Jm101a
F0c1w2Jm101a
w02Jm0f0g0c1w2Jm101a

CDIS

CVE-2025-22224, CVE-2025-22225, CVE-2025-22226: Zero-Day Vulnerabilities in VMware ESXi, Workstation and Fusion Exploited



[Satnam Narang](#)

March 4, 2025 | 3 Min Read



Broadcom published an advisory for three flaws in several VMware products that were exploited in the wild as zero-days. Organizations are advised to apply the available patches.



ТОСТОУ



```
ssize_t vmci_queuepair_put(void *buf, size_t len) {  
    if (len > Q_LIMIT)  
        return -EINVAL;  
    copy_from_guest(q_tail, buf, len);  
}
```



```
ssize_t vmci_queuepair_put(void *buf, size_t len) {  
    if (len > Q_LIMIT)  
        return -EINVAL;  
    copy_from_guest(q_tail, buf, len);  
}
```



Q_LIMIT

0x600

```
ssize_t vmci_queuepair_put(void *buf, size_t len) {  
    if (len > Q_LIMIT)  
        return -EINVAL;  
    copy_from_guest(q_tail, buf, len);  
}
```

0x400



Q_LIMIT

0x600

```
ssize_t vmci_queuepair_put(void *buf, size_t len) {  
    if (len > Q_LIMIT)  
        return -EINVAL;  
    copy_from_guest(q_tail, buf, len);  
}
```

0x400



Q_LIMIT

0x600

```
ssize_t vmci_queuepair_put(void *buf, size_t len) {  
    if (len > Q_LIMIT)  
        return EINVAL;  
    copy_from_guest(q_tail, buf, len);  
}
```

0x1800



Q_LIMIT

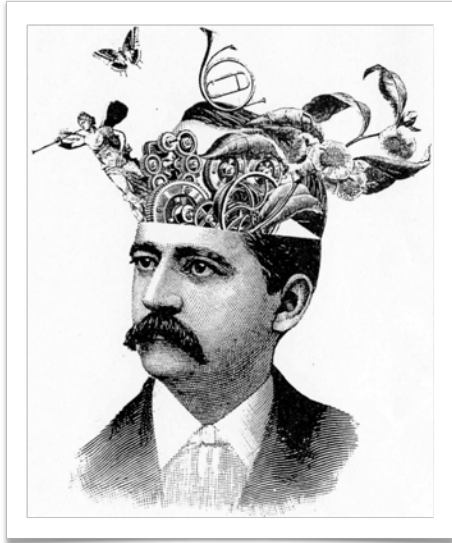
```
ssize_t vmci_queuepair_put(void *buf, size_t len) {  
    if (len > Q_LIMIT)  
        return -EINVAL;  
    copy_from_guest(q_tail, buf, len);  
}
```

0x1800

💣 *HEAP OVERFLOW* 💣

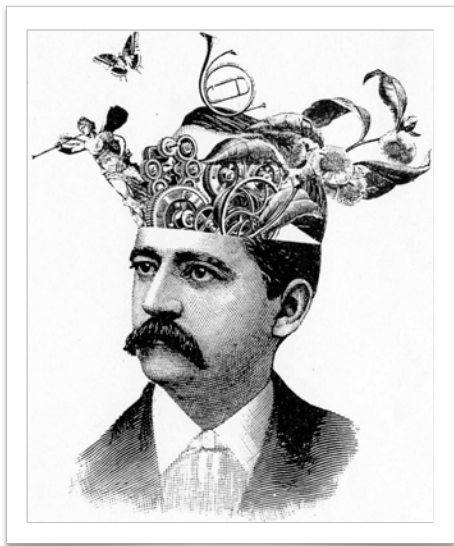
Q_LIMIT

Root cause: Cognitive complexity

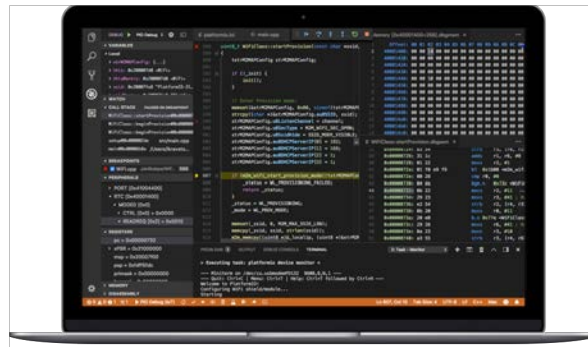


Cognitive complexity

Developers need cognitive assistance



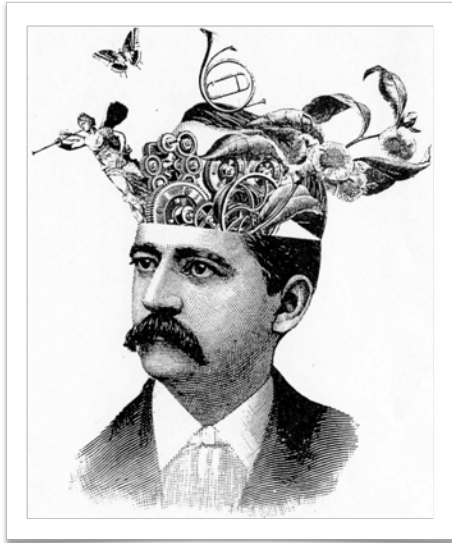
Cognitive complexity



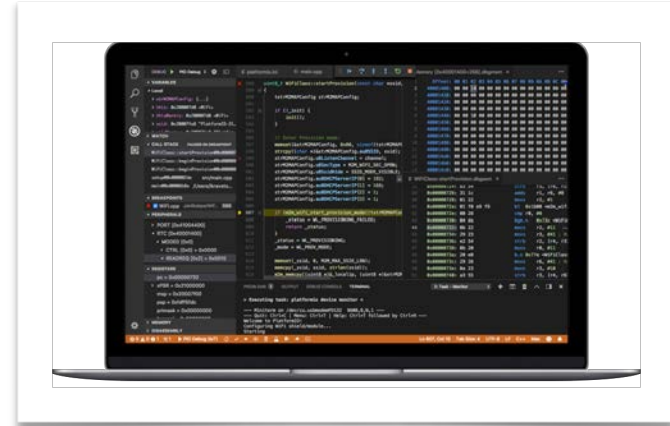
Better tools and methods for secure software development

- New development environments
- New programming languages
- New operating systems
- Static-analysis tools
- Dynamic testing tools
- Verification tools
- ...

Root cause: Cognitive complexity



Cognitive complexity



Better tools for secure software development



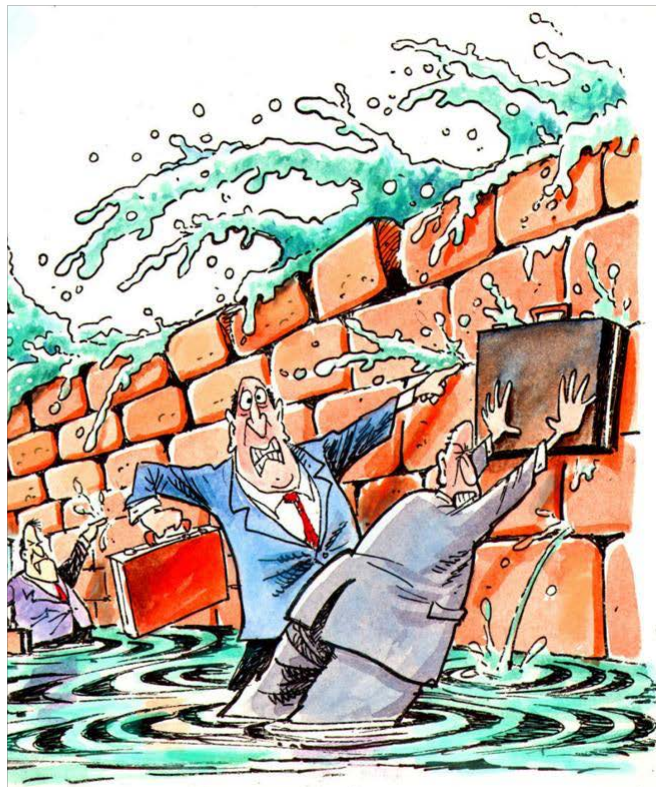
Research and innovation

```

XQ0gaMgC9g9c21libQ0gdG8g
aW5Z2M5G0i9c2d2x1z1G1h1
Y2pbpmU0gd2hp2r2g2P2a1GJ1
IvN5iWQ0gdG9g2r2c2S2S2b
bnkgY29Zc2V0bWUuIS2z21W0
Z5J545Z5Wg2d2c2S2z2P2a1
aw5111111111111111111111
d21021111111111111111111
IGU1111111111111111111111
cApCpYbJ3c1Od0vU1R00zSBT
LK0g2YqC29z1S2S1z2L2dXKp
becgbcYga1u01z2S2bL2C80aG
VuifU0g2Y21abCb2j2d2wXk
11R0R0zS2S2z1W1111
N1cKv1bm1IG
FzR0u0g

```

Insecure systems require many defenders



The Cybersecurity Workforce Gap 2024

FIGURE 2

2024 Global Cybersecurity Workforce Estimate

5,457,173 +0.1% YoY

REGIONS

NORTH AMERICA

1,454,868
-2.7%

EUROPE

1,300,023
-0.7%

LATIN AMERICA

1,273,868
-0.9%

FIGURE 3

2024 Global Cybersecurity Workforce Gap

4,762,963 +19.1% YoY

REGIONS

NORTH AMERICA

542,687
+4.0%

EUROPE

392,320
+12.8%

LATIN AMERICA

328,397
-5.7%

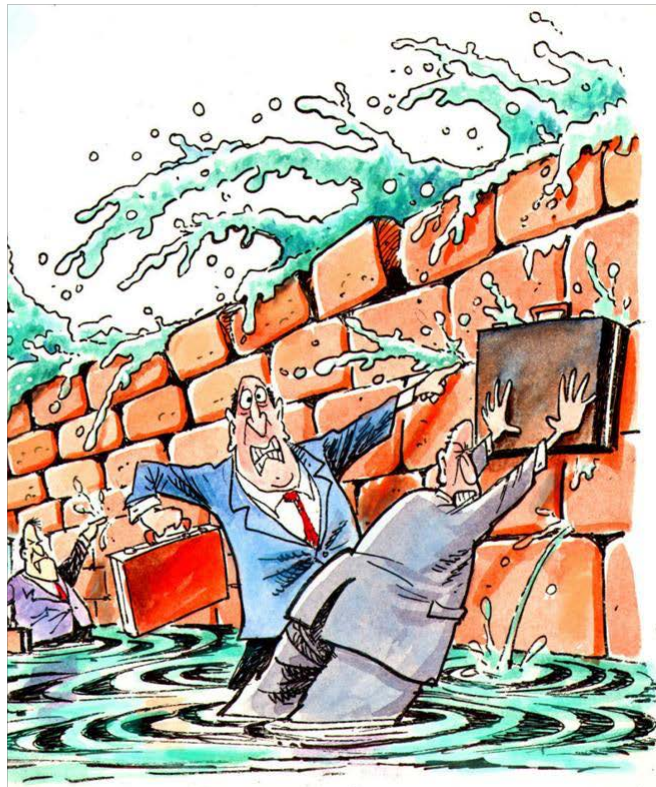
MIDDLE EAST & AFRICA

124,978
+11.8%

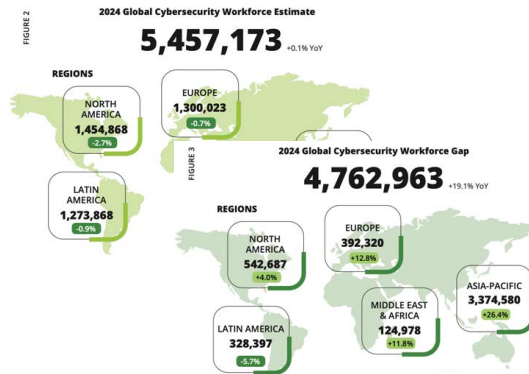
ASIA-PACIFIC

3,374,580
+26.4%

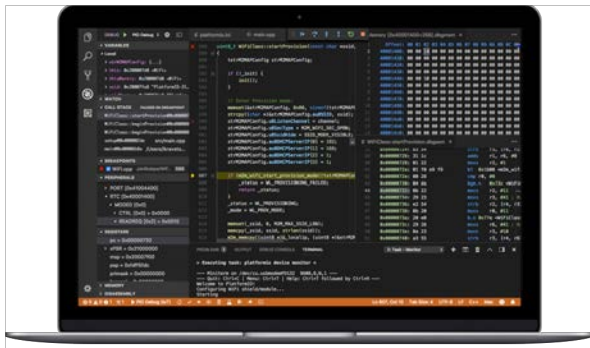
Insecure systems require many defenders



The Cybersecurity Workforce Gap 2024



Education



Better tools and methods



More defenders

Research Innovation

Education

SX0gaXMcG9zc21libGUGdG8g
 aW52ZW50IGBgGc21uz2x1IG1h
 Y2hpbmUGd2hpY2g9y2FIuGJ
 IHVzZWQ6dG8yZ29tcHV0ZSBh
 bnkgY29tcHV0YWJsZSBzZXF1
 ZW5jZS4gSWVmdGhpcyBtYWNo
 aW51IHR5aGVuc3wudG9wZWQ6
 d210aGhIRhG9zZWQ6dGhl
 IGVJZ29tcHV0Y29tcHV0aGJj
 aCBpcyB3cm10dGVuIHROZSBT
 LkQ6Y2Yc29tZSBjb21wdXRp
 bmcgbWFiagJlZSBnLNCB0aG
 VuIFUGd21sbCBjb21wdX
 RIHROZSBzYWllIH
 NlcXVlbmNlIG
 FzIE0uClG

**CENTER FOR CYBER DEFENCE
AND INFORMATION SECURITY**

SXQgaXMcG9s211bGUGdG
 aW52W501G2h21u2a1IG
 Y2hpbmUdG2hp2JggY2FzIG
 HWZuWqGdG9G2F9tcwW0S
 bknqY29kZG92bW92bW92
 W5Z2S4G5WYQ2Gpcy2S
 aS51Y29kZG92bW92bW92
 d2101G2h21u2a1IG
 IQX1Y29kZG92bW92bW92
 ACBpcyB3Cm10dG9uWlRoZS
 LKqbb2Ygc2F92S38J2lWdX
 bncqY2FzIG92bW92bW92
 VuIFUgd219bC8J2lWdX
 R1IHRO2VlbnZlWl1H
 N1cKVlbnZlIG
 Fz1Z0eGc